Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise 4.0.5 with AT&T IP Flexible Reach SIP Trunk Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Session Border Controller for Enterprise 4.0.5, with the AT&T IP Flexible Reach SIP Trunk service using either **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 6.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Communication Server 1000E 7.5 is a telephony server, and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Session Border Controller for Enterprise 4.0.5 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service, and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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

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

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5 (Avaya CS1000E), Avaya Aura® Session Manager Release 6.1 (Session Manager), and the Avaya Session Border Controller for Enterprise 4.0.5 (Avaya SBCE), with the AT&T IP Flexible Reach SIP trunk service for PSTN access.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. The AT&T IP Flexible Reach service utilizes AVPN[1] or MIS/PNT[2] transport services.

For more information on the, AT&T IP Flexible Reach service visit: http://www.business.att.com/enterprise/Service/voice-services/voip/sip-trunking/.

2. General Test Approach and Test Results

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

2.1. Interoperability Compliance Testing

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

- SIP trunking of inbound and outbound calls.
    - Incoming calls from the PSTN were routed to the DID numbers assigned by the AT&T IP Flexible Reach service to Avaya CS1000E location. These incoming PSTN calls arrived via the SIP trunk and were answered by Avaya IP UNIStim telephones (desk phones and soft phones) and fax machine emulation software (Ventafax). Proper call disconnect was verified.
    - Outgoing calls from the Avaya CS1000E location to the PSTN were routed via the SIP trunk to the AT&T IP Flexible Reach service. These outgoing PSTN calls were originated from Avaya IP UNIStim telephones, and fax machine emulation software (Ventafax). Proper call disconnect was verified.
    - Use of G.729A and G.711mu-law codecs were verified.
- Inbound and outbound T.38 Fax, using combinations of Group 3 (G3) and Super G3 (SG3) modes, were verified.
- Avaya CS1000E stations call coverage to Avaya Call Pilot® for message generation and retrieval (including Message Wait Indicator).

---

[1] AVPN uses compressed RTP (cRTP).

[2] .MIS/PNT does not support cRTP.

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

2.2. Test Results

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

2.2.1 Known Limitations

1. To allow the Avaya CS1000E user to transfer a call from PSTN user A to PSTN user B, before user B has answered the call (unattended transfer), Avaya CS1000E plug-in 501 must be enabled as shown in **Section 5.8**. While plug-in 501 will allow the Avaya CS1000E user to complete the transfer operation, user A may not hear ring back tone while user B is ringing in all cases. PSTN users A and B will have two-way talk path once user B answers.

2. G.711 fax is not supported in the reference configuration. T.38 faxing is supported, as is Group 3 and Super Group 3 fax. Fax speeds up to 14400 bps are supported in the configuration tested. In addition, Fax Error Correction Mode (ECM) is supported in the reference configuration.

3. The AT&T IP Flexible Reach service does not support SIP History-Info headers. However, the AT&T IP Flexible Reach service requires that SIP Diversion Header be sent for certain redirected calls (e.g. Call Forward). Session Manager will convert the History Info header into the Diversion Header by the use of the adaptation "*DiversionTypeAdapter*" for these types of calls (see **Section 6.3.2)**. For all other calls, Avaya SBCE will strip off History-Info headers (see **Section 7.4.9**).

4. 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 7.4.9**).

5. 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-e164-clid, and RFC2833 Telephone Event Type 111 (see **Section 7.4.9**).

6. 1140E SIP telephones (v4.03.09) were tested, but due to loss of audio issues found during conference and transfer scenarios, these endpoints are not supported in the reference configuration. Work Items have been opened with Avaya CS1000E support. In addition, the 1140E SIP telephones use a hard coded value of 111 for their RFC2833 Telephone Event Type.

7. **Emergency 911/E911 Services Limitations and Restrictions** - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor. While AT&T IP Flexible Reach services support 911/E911 calling capabilities under certain Calling Plans, there are circumstances when that 911/E911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

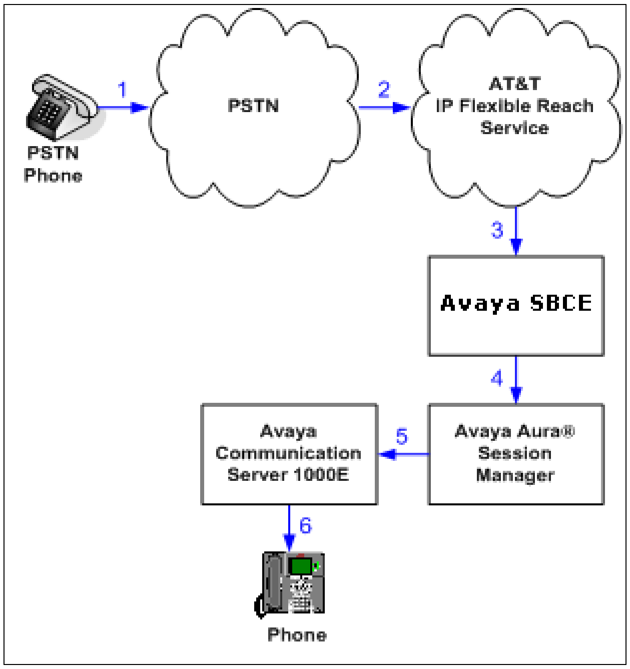
2.3. Call Flows

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

2.3.1 Inbound

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

1. A PSTN phone originates a call to an AT&T IP Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service routes the call to 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 necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Avaya CS1000E.
6. Depending on the called number, Avaya CS1000E routes the call to a phone or fax.

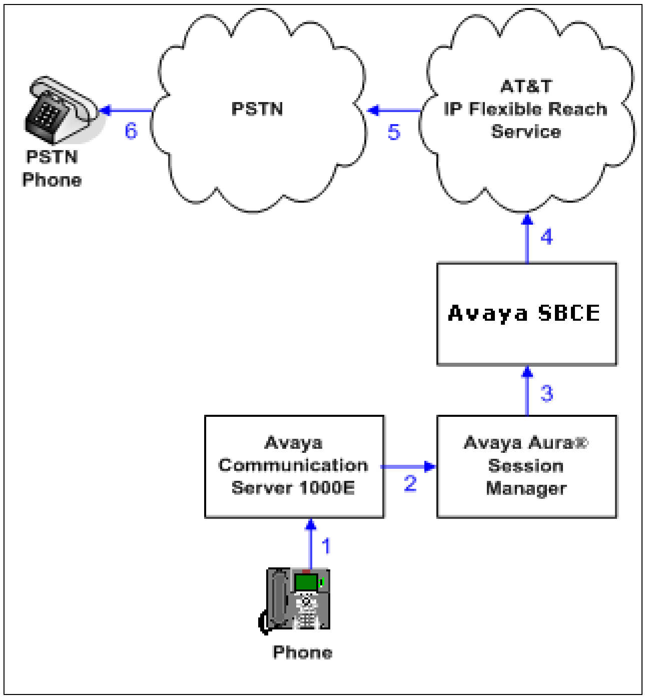

PSTN Phone
1
PSTN
2
AT&T IP Flexible Reach Service
3
Avaya SBCE
4
Avaya Aura® Session Manager
5
Avaya Communication Server 1000E
6
Phone

Inbound AT&T IP Flexible Reach Call

2.3.2 Outbound

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

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


PSTN Phone
6
PSTN
5
AT&T IP Flexible Reach Service
4
Avaya SBCE
3
Avaya Communication Server 1000E
2
Avaya Aura® Session Manager
1
Phone

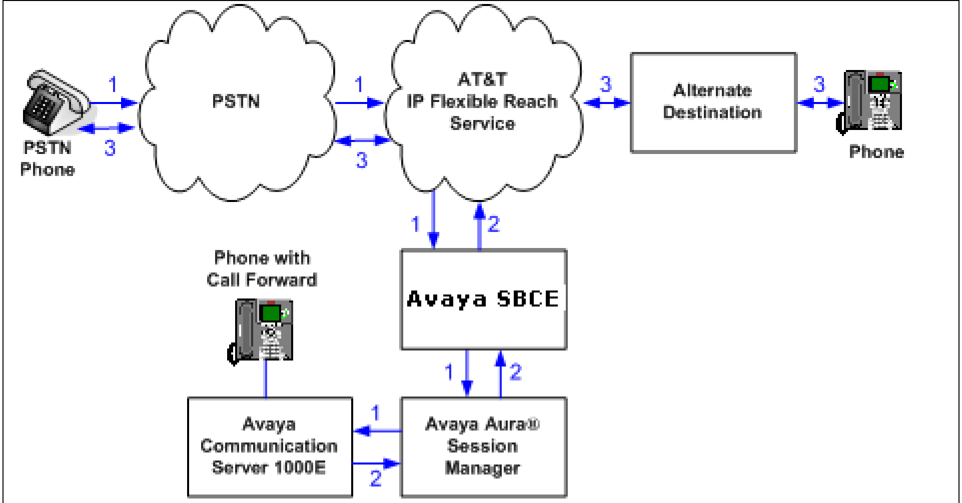
Outbound AT&T IP Flexible Reach Call

2.3.3 Call Forward Re-direction

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

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

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

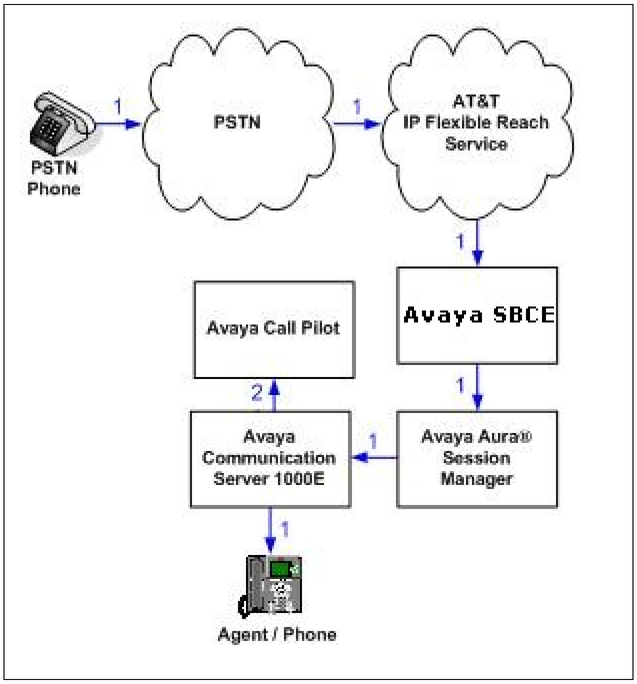

PSTN Phone
1
3
PSTN
1
3
AT&T IP Flexible Reach Service
3
Alternate Destination
3
Phone
1
2
Phone with Call Forward
Avaya SBCE
1
2
Avaya Communication Server 1000E
1
2
Avaya Aura® Session Manager

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

2.3.4 Coverage to Voicemail

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

1. Same as the first call scenario in **Section 2.3.1**.
2. The called Avaya CS1000E 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.



Coverage to Voicemail

2.4. Support

2.4.1 Avaya

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

2.4.2 AT&T

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

3. Reference Configuration

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

- The 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)

  Note – Only Avaya CS1000E system provisioning providing SIP trunk functionality is described in these application notes. For additional Avaya CS1000E system provisioning documentation, see **Section 11.**

- Avaya "desk" phones are represented with Avaya 1140E UNIStim IP and Digital M3904 telephones. 2050 UNIStim soft phones were also tested.

- Avaya SBCE provides address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network. TCP transport protocol is used between Avaya SBCE and Session Manager. UDP transport protocol is used between Avaya SBCE and the AT&T IP Flexible Reach service.

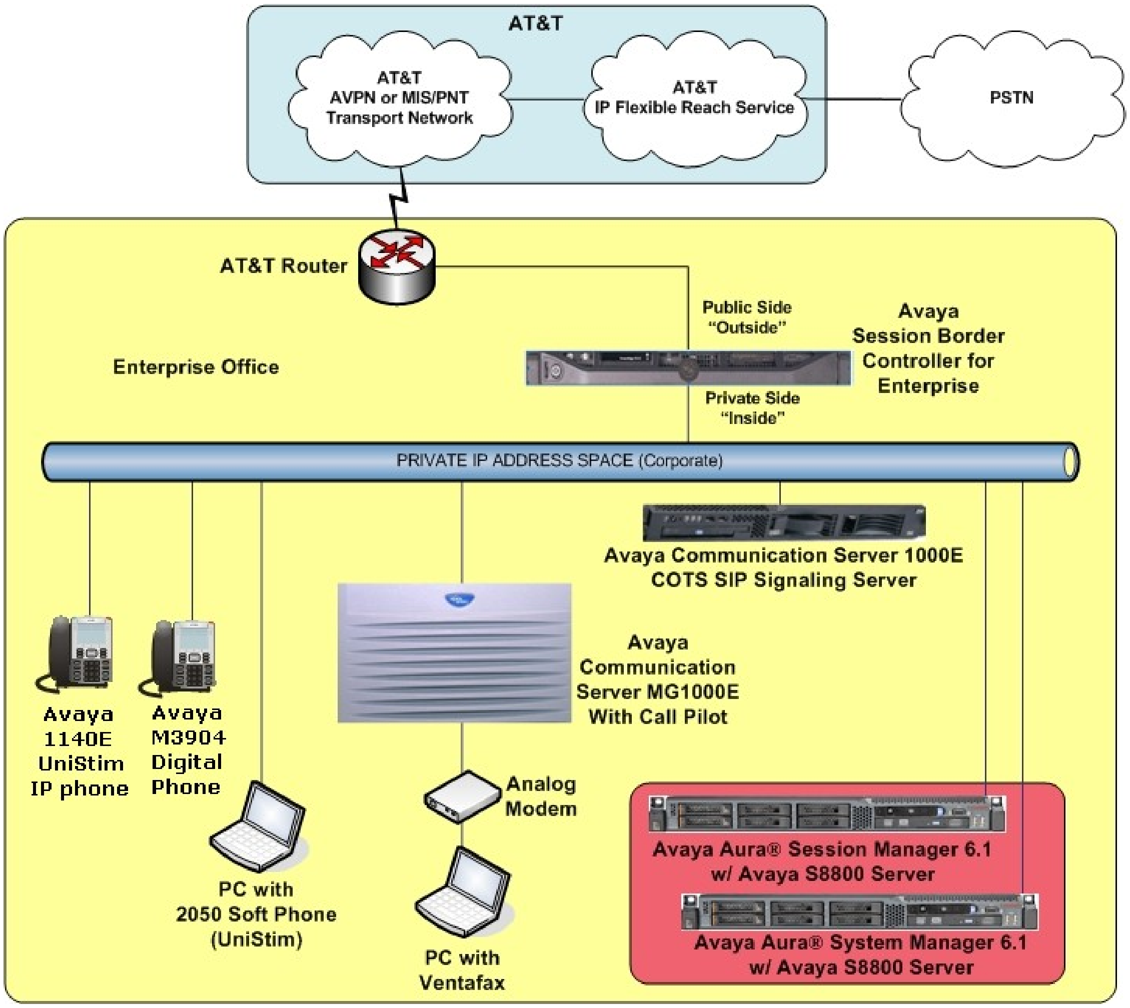
- An existing Avaya Call Pilot® system provides the corporate voice messaging capabilities in the reference configuration. **Note** - The provisioning of Avaya Call Pilot® is beyond the scope of this document (see [11] for more information).

- Outbound calls were originated from a phone or fax provisioned on the Avaya CS1000E system. SIP signaling is passed from Avaya CS1000E system to Session Manager, and to Avaya SBCE, before being sent to the AT&T network for termination. Media was sent from the calling IP phone directly to Avaya SBCE. Legacy devices such as analog fax send their audio from the MGC to Avaya SBCE. Avaya SBCE then directs the media to the AT&T network.

- Inbound calls were sent from PSTN/AT&T, through Avaya SBCE to Session Manager, and on to Avaya CS1000E system. Avaya CS1000E system terminates the calls to the appropriate phone or fax extensions.

Note – In the reference configuration TCP (port 5060) is used as the transport protocol between the Avaya CS1000E, 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 Flexible Reach service for the connection between Avaya SBCE and the AT&T T IP Flexible Reach border element.



AT&T
AT&T AVPN or MIS/PNT Transport Network
AT&T IP Flexible Reach Service
PSTN
AT&T Router
Enterprise Office
Public Side "Outside"
Avaya Session Border Controller for Enterprise
Private Side "Inside"
PRIVATE IP ADDRESS SPACE (Corporate)
Avaya Communication Server 1000E COTS SIP Signaling Server
Avaya Communication Server MG1000E With Call Pilot
Avaya 1140E UniStim IP phone
Avaya M3904 Digital Phone
Analog Modem
PC with 2050 Soft Phone (UniStim)
PC with Ventafax
Avaya Aura® Session Manager 6.1 w/ Avaya S8800 Server
Avaya Aura® System Manager 6.1 w/ Avaya S8800 Server

Figure 5: Avaya Interoperability 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 Flexible Reach service border element IP address shown in this document is an example. AT&T Customer Care will provide the actual IP addressing as part of the IP Flexible Reach provisioning process.

Component	Illustrative Value in these Application Notes
Avaya CS1000E	
SIP Signaling Server IP Address (TLAN)	172.16.6.110
MGC Media (DSP) IP Address (TLAN)	172.16.6.115
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 Flexible Reach Service)	192.168.64.130
IP Address of "Inside" (Private) Interface (connected to Session Manager)	192.168.67.120
AT&T IP Flexible Reach 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 were used in the sample configuration.

Equipment/Software	Release/Version
Avaya CS1000E Platform • MG1000E Media Gateway • IBM xSeries 306M (COTS) SIP Signaling server • Call 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 (System Manager)	Avaya Aura® System Manager Release 6.1.0 with SP2 (Build Number 6.1.0.0.7345-6.1.5.106)
Avaya S8800 Server (Session Manager)	Avaya Aura® Session Manager Release 6.1 SP2 (Load 6.1.2.0.612004)
Dell R310	Avaya Session Border Controller for Enterprise 4.0.5.Q02
Avaya 1140E Series IP Deskphones (UNIStim)	FW 625C8L
Avaya 2050 Soft Phone (UNIStim)	4.03.0081
Avaya M3904 Series Digital Deskphones	-
Fax device	Ventafax Home Version 6.3.102.288
AT&T IP Flexible Reach Service via AVPN or MIS/PNT transport service connections.	VNI 21

Table 2: Equipment and Software Used in the Sample Configuration

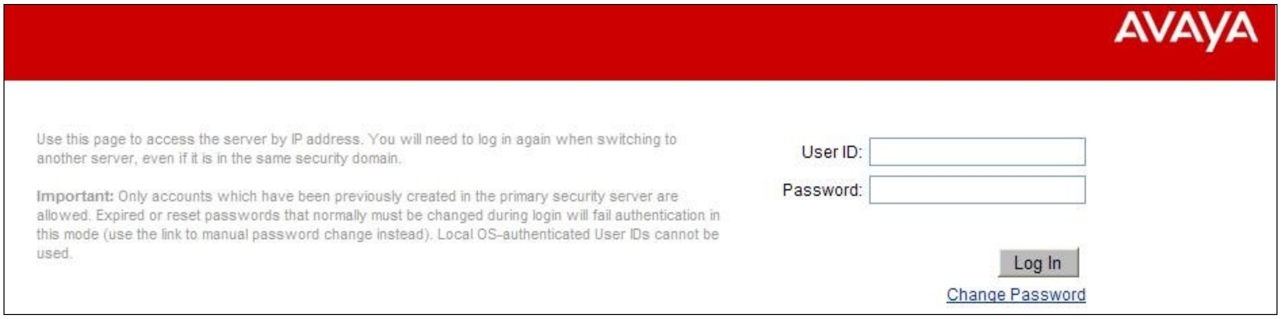
5. Configure Avaya CS1000E

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 (although supported by the CS1000E platform, SIP telephones are not supported in the reference configuration, see **Section 2.2.1**). For references on how to administer these functions of Avaya CS1000E, see **Section 11**

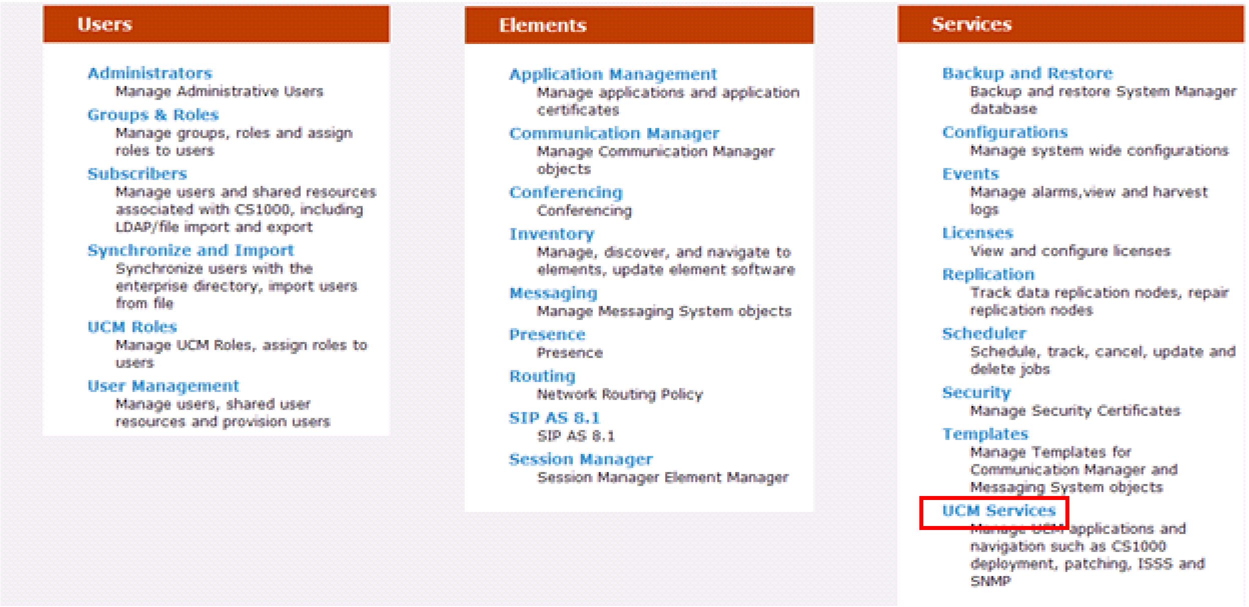
Step 1 - Unless otherwise noted, all Avaya CS1000E provisioning was performed via the Avaya Unified Communication Management (AUCM) web interface. The **AUCM** web interface may be launched directly via **https://<ip address>** where the relevant <ip address> in the sample configuration is 172.16.6.111.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



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

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

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



Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Subscribers
Manage users and shared resources associated with CS1000, including LDAP/file import and export

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

SIP AS 8.1
SIP AS 8.1

Session Manager
Session Manager Element Manager

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

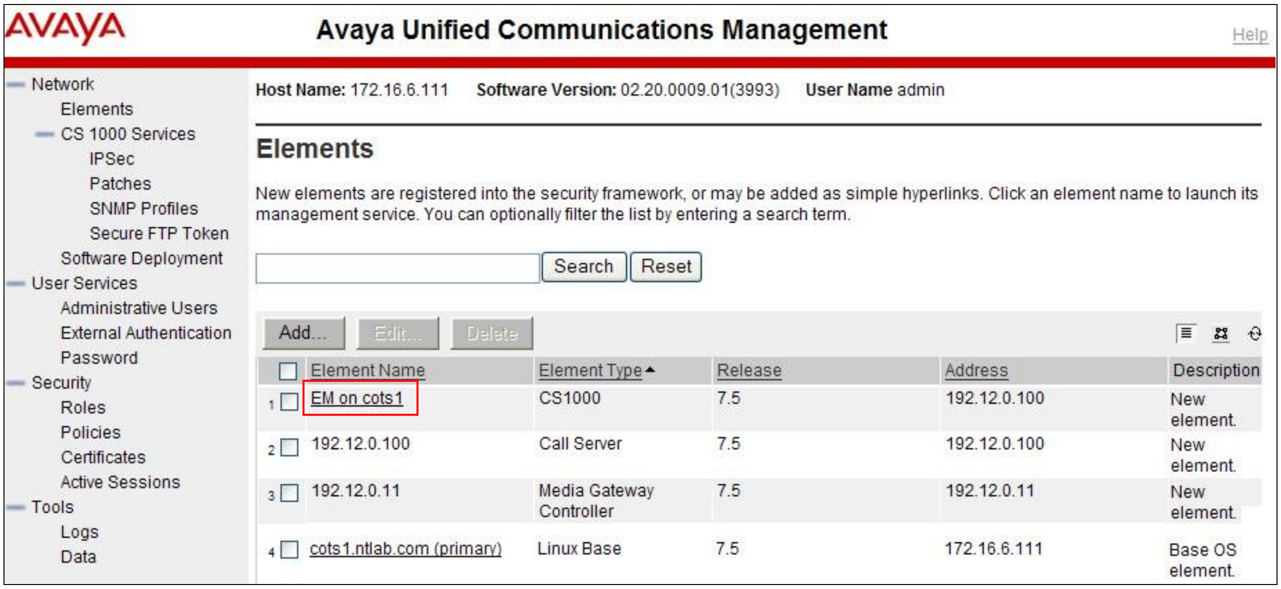
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

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

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



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

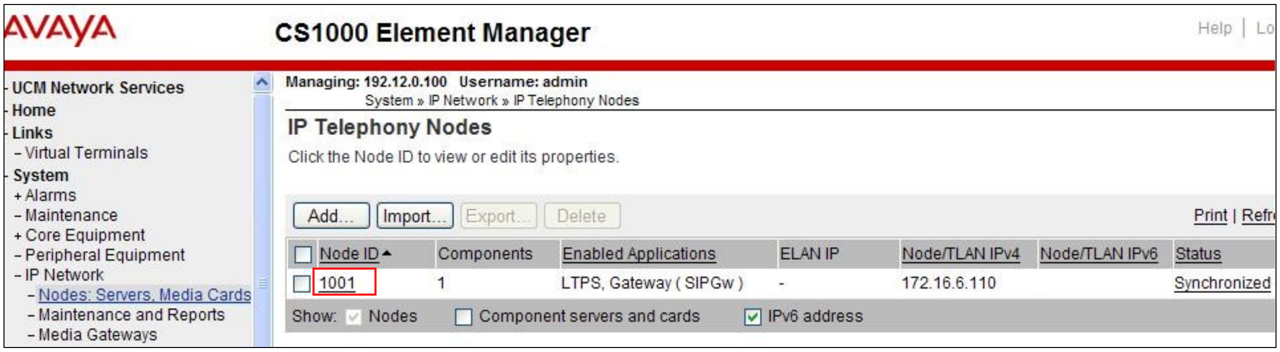
Elements

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.

	Element Name	Element Type ▲	Release	Address	Description
1 ☐	EM on cots1	CS1000	7.5	192.12.0.100	New element.
2 ☐	192.12.0.100	Call Server	7.5	192.12.0.100	New element.
3 ☐	192.12.0.11	Media Gateway Controller	7.5	192.12.0.11	New element.
4 ☐	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.



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

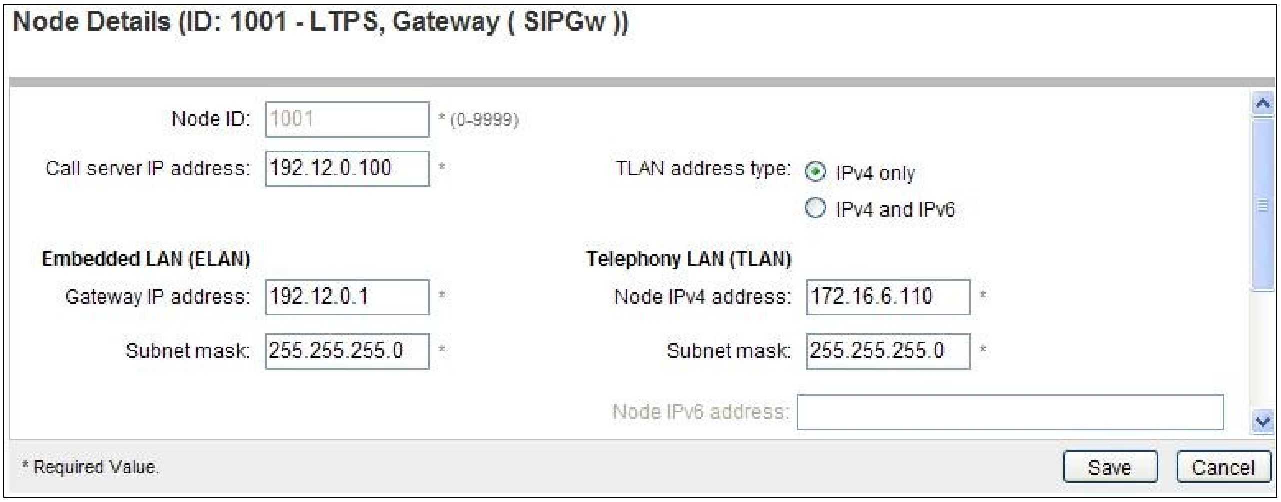
IP Telephony Nodes

Click the Node ID to view or edit its properties.

☐ Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
☐ 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: 1001 * (0-9999)

Call server IP address: 192.12.0.100 *

TLAN address type: ● IPv4 only ○ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 192.12.0.1 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

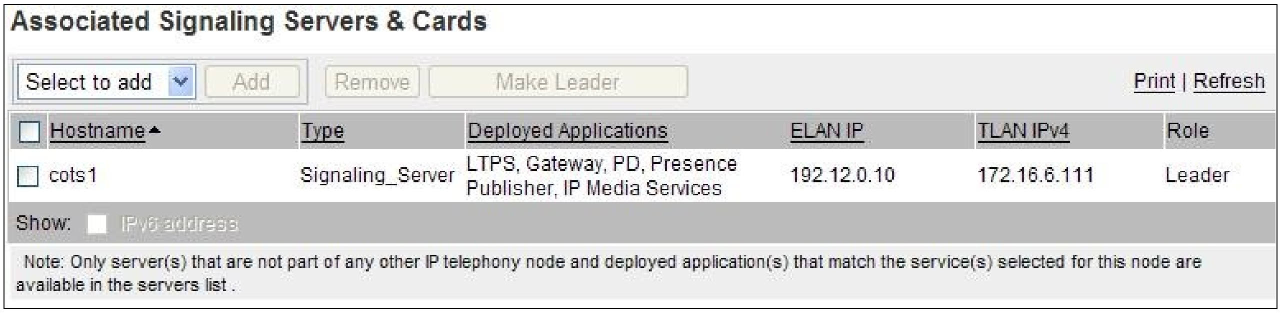
Node IPv4 address: 172.16.6.110 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

* Required Value.

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



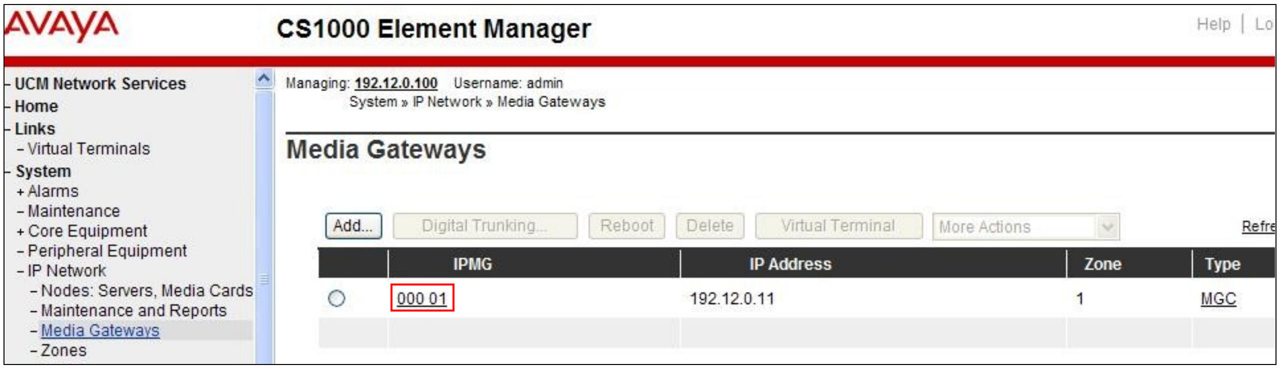
Associated Signaling Servers & Cards

☐ Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
☐ 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**).



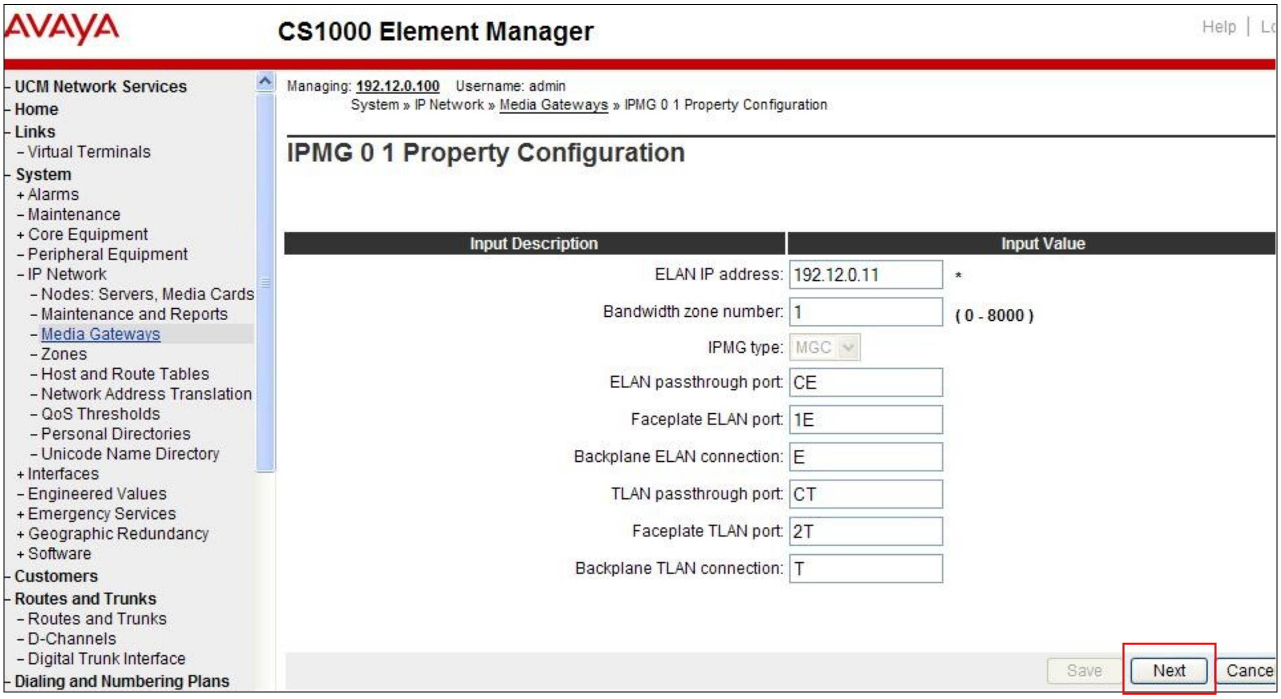
Managing: 192.12.0.100 Username: admin
System » IP Network » Media Gateways

Media Gateways

	IPMG	IP Address	Zone	Type
○	000 01	192.12.0.11	1	MGC

This will open the Property Configuration screen.

Step 3 – Click on the Next button.

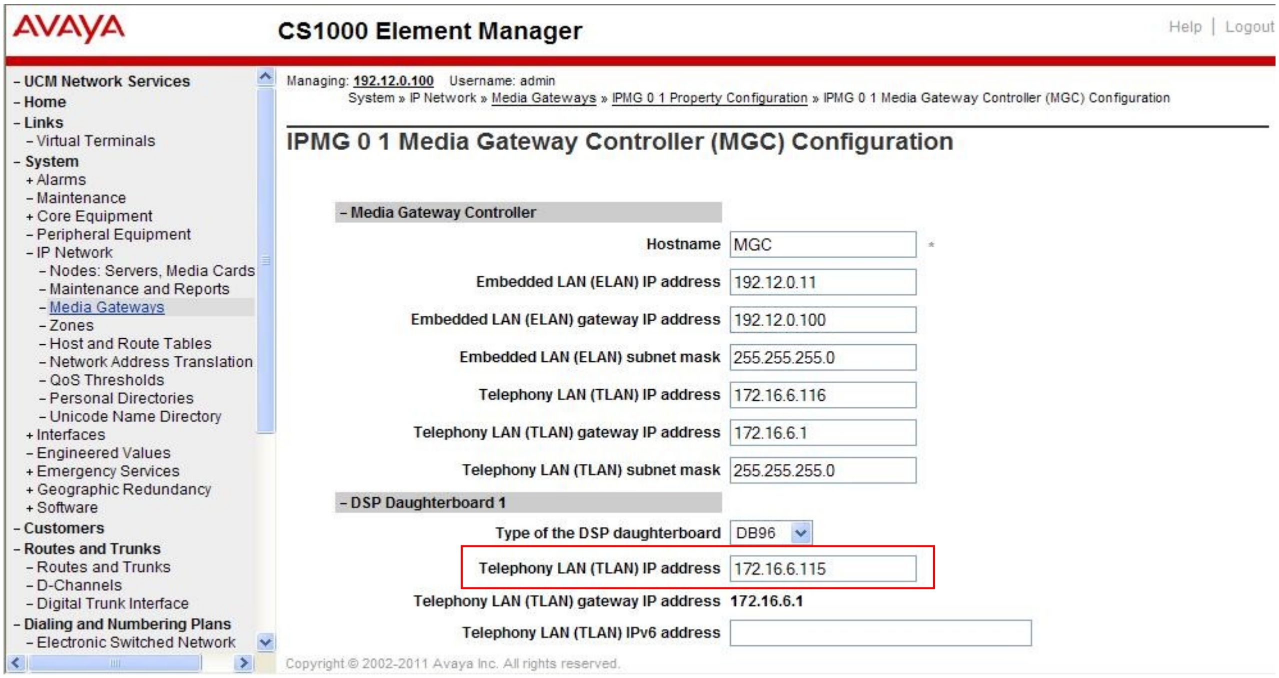


Managing: 192.12.0.100 Username: admin
System » IP Network » Media Gateways » IPMG 0 1 Property Configuration

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 the Avaya SBCE "outside" IP address before sending the INVITE on to the AT&T IP Flexible Reach service.



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

IPMG 0 1 Media Gateway Controller (MGC) Configuration

- Media Gateway Controller

Hostname: MGC *
Embedded LAN (ELAN) IP address: 192.12.0.11
Embedded LAN (ELAN) gateway IP address: 192.12.0.100
Embedded LAN (ELAN) subnet mask: 255.255.255.0
Telephony LAN (TLAN) IP address: 172.16.6.116
Telephony LAN (TLAN) gateway IP address: 172.16.6.1
Telephony LAN (TLAN) subnet mask: 255.255.255.0

- DSP Daughterboard 1

Type of the DSP daughterboard: DB96
Telephony LAN (TLAN) IP address: 172.16.6.115
Telephony LAN (TLAN) gateway IP address: 172.16.6.1
Telephony LAN (TLAN) IPv6 address:

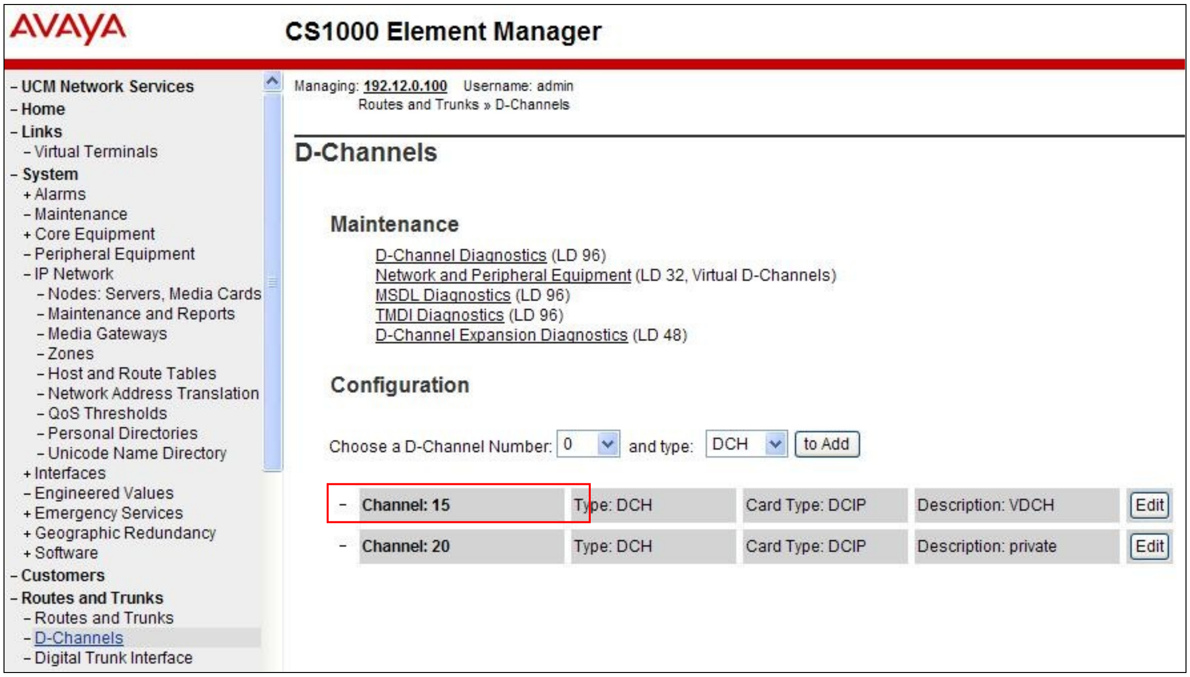
Copyright © 2002-2011 Avaya Inc. All rights reserved.

5.2. Virtual D-Channel, Routes and Trunks

Avaya 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.



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

D-Channels

Maintenance

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

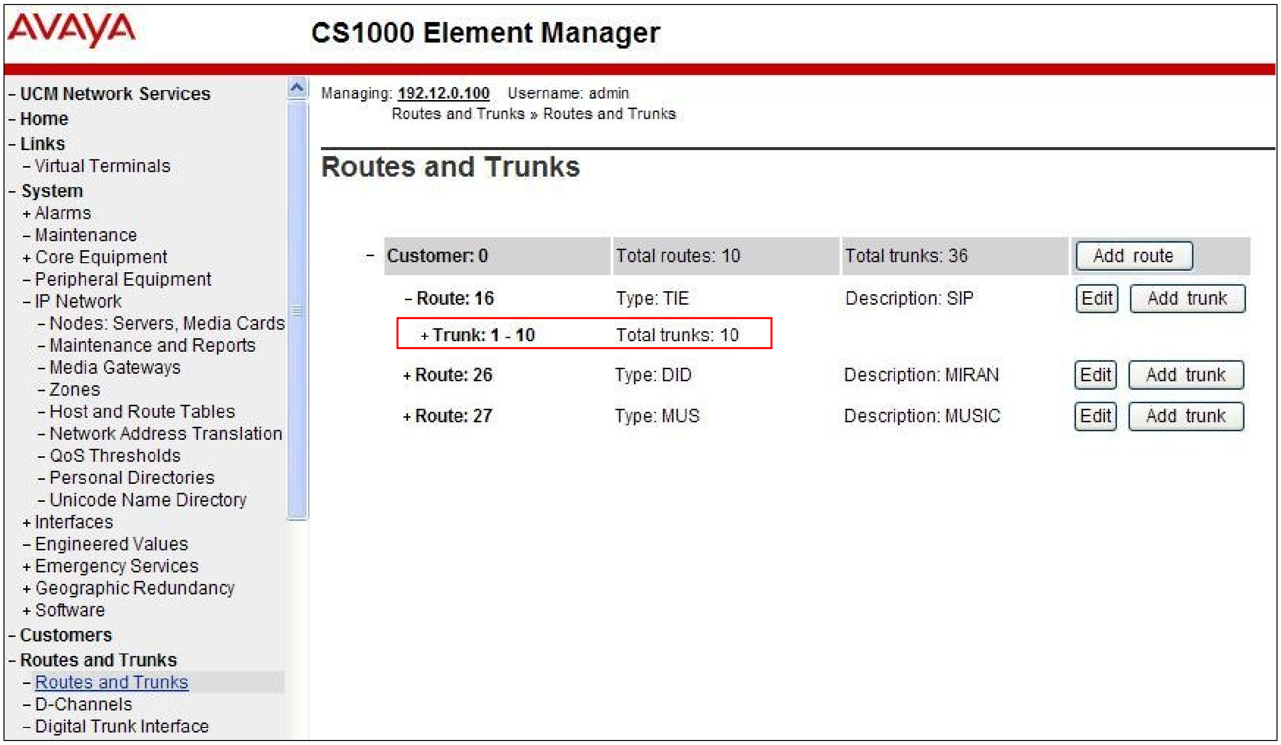
Configuration

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

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

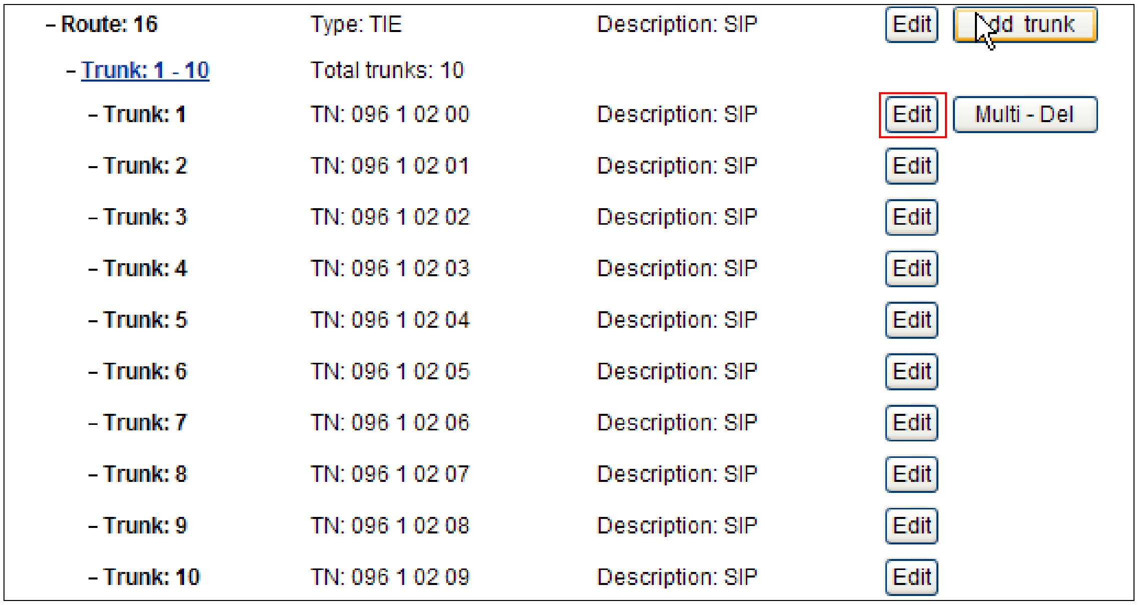
5.2.2 Routes and Trunks Configuration

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**).



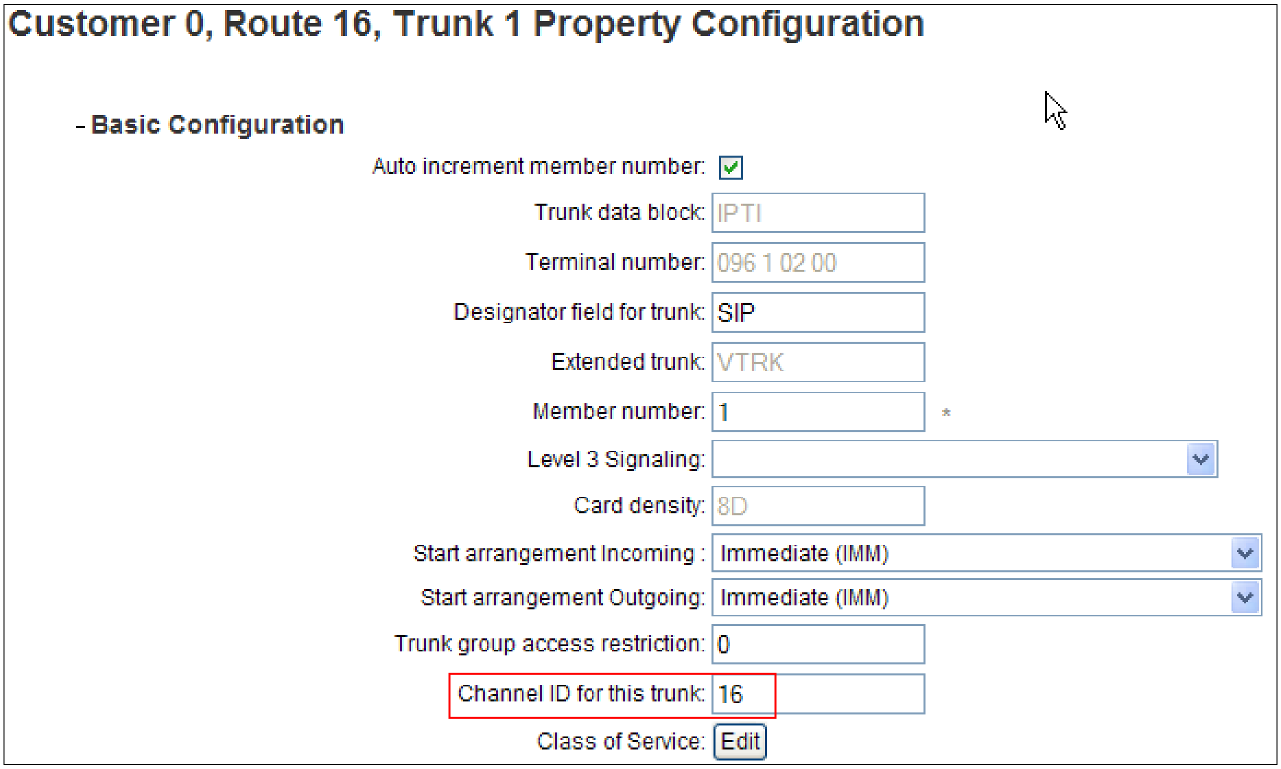
- Customer: 0	Total routes: 10	Total trunks: 36	Add route
- Route: 16	Type: TIE	Description: SIP	Edit Add trunk
+ Trunk: 1 - 10	Total trunks: 10		
+ Route: 26	Type: DID	Description: MIRAN	Edit Add trunk
+ Route: 27	Type: MUS	Description: MUSIC	Edit Add trunk

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



- Route: 16	Type: TIE	Description: SIP	Edit Add trunk
- 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

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+(n-1), where n is the trunk number. For example, Trunk 9 will use channel 24.

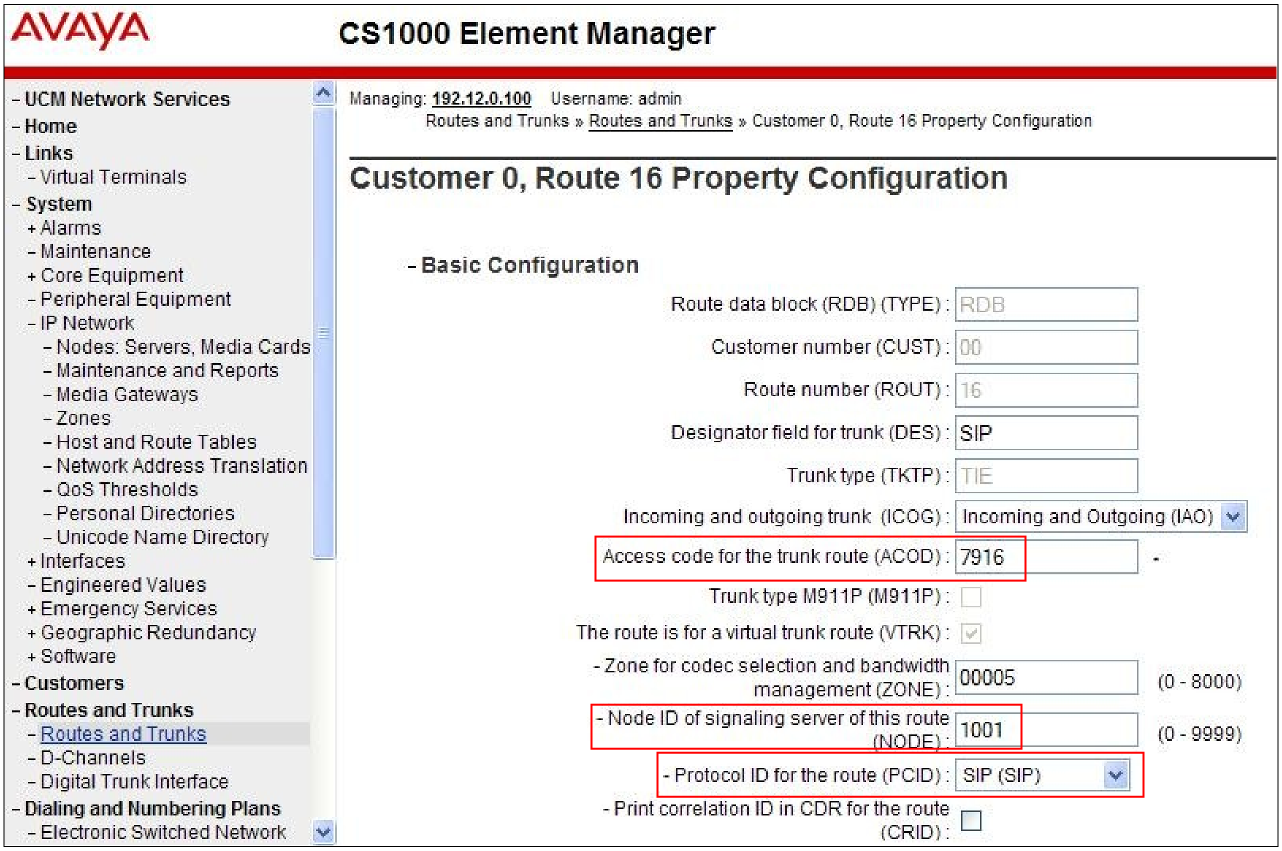


Customer 0, Route 16, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☑
Trunk data block: IPTI
Terminal number: 096 1 02 00
Designator field for trunk: SIP
Extended trunk: VTRK
Member number: 1 *
Level 3 Signaling:
Card density: 8D
Start arrangement Incoming : Immediate (IMM)
Start arrangement Outgoing: Immediate (IMM)
Trunk group access restriction: 0
Channel ID for this trunk: 16
Class of Service: Edit

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

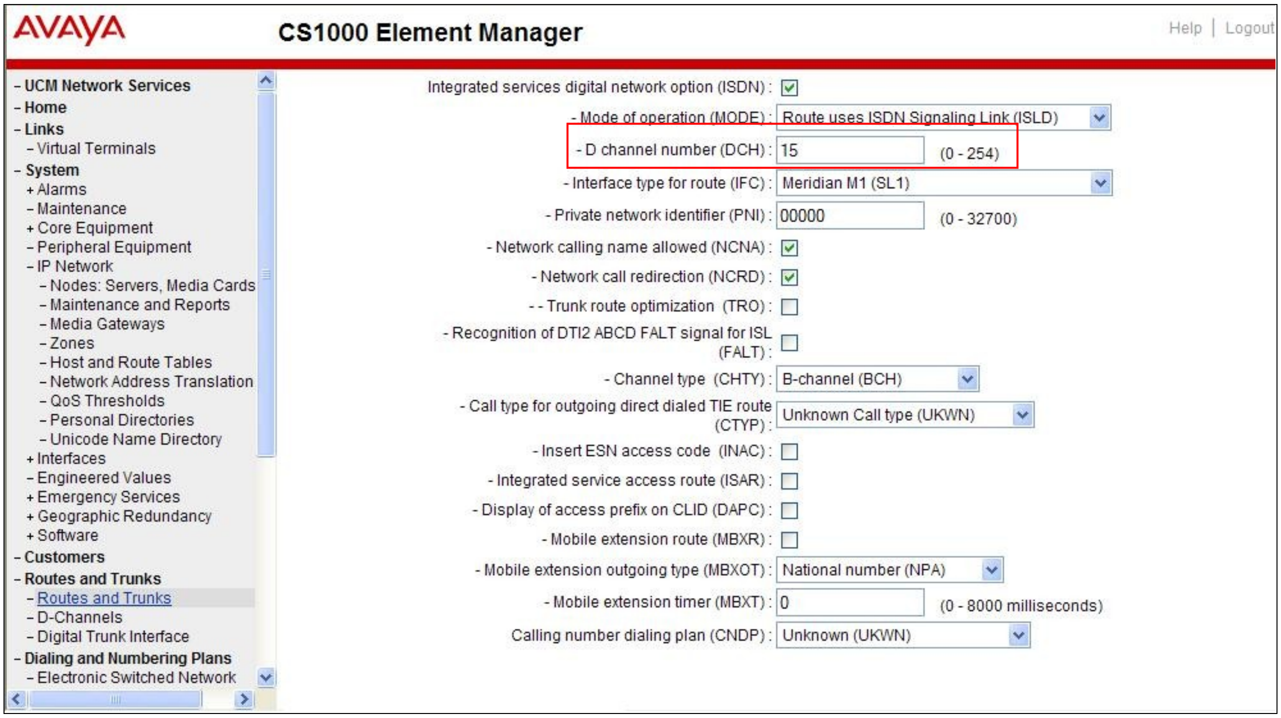


Customer 0, Route 16 Property Configuration

- Basic Configuration

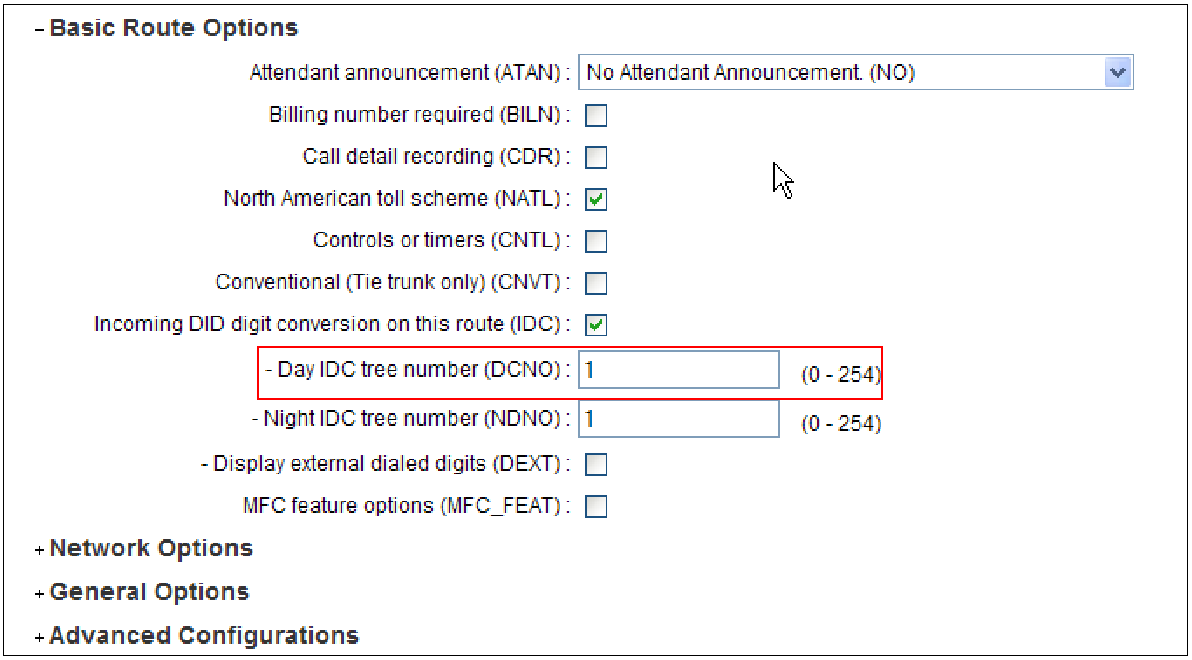
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 00
Route number (ROUT) : 16
Designator field for trunk (DES) : SIP
Trunk type (TKTP) : TIE
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 7916
Trunk type M911P (M911P) : ☐
The route is for a virtual trunk route (VTRK) : ☑
- Zone for codec selection and bandwidth management (ZONE) : 00005 (0 - 8000)
- Node ID of signaling server of this route (NODE) : 1001 (0 - 9999)
- Protocol ID for the route (PCID) : SIP (SIP)
- Print correlation ID in CDR for the route (CRID) : ☐

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



Integrated services digital network option (ISDN) : ☑
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) : 15 (0 - 254)
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 00000 (0 - 32700)
- Network calling name allowed (NCNA) : ☑
- Network call redirection (NCRD) : ☑
- - Trunk route optimization (TRO) : ☐
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) : ☐
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Unknown Call type (UKWN)
- Insert ESN access code (INAC) : ☐
- Integrated service access route (ISAR) : ☐
- Display of access prefix on CLID (DAPC) : ☐
- Mobile extension route (MBXR) : ☐
- Mobile extension outgoing type (MBXOT) : National number (NPA)
- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) : Unknown (UKWN)

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



- Basic Route Options

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

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

North American toll scheme (NATL) : ☑

Controls or timers (CNTL) : ☐

Conventional (Tie trunk only) (CNVT) : ☐

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

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

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

- Display external dialed digits (DEXT) : ☐

MFC feature options (MFC_FEAT) : ☐

+ Network Options

+ General Options

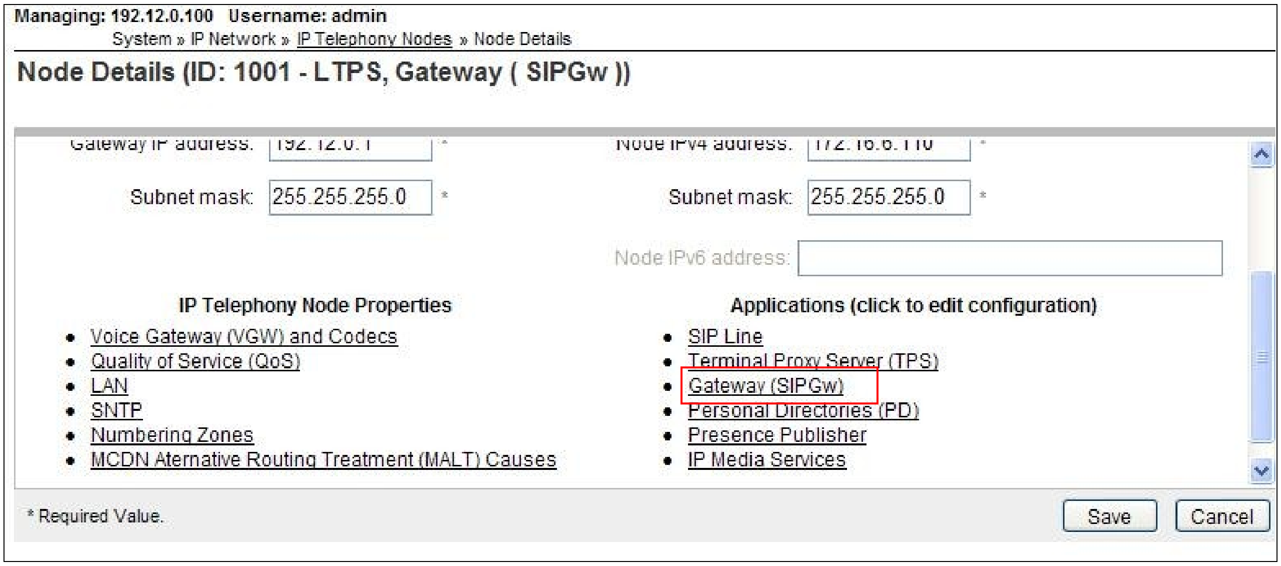
+ Advanced Configurations

5.3. SIP Trunk to Session Manager

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

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

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



Managing: 192.12.0.100 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

Gateway IP address: 192.12.0.1 *

Subnet mask: 255.255.255.0 *

Node IPv4 address: 172.16.6.110 *

Subnet mask: 255.255.255.0 *

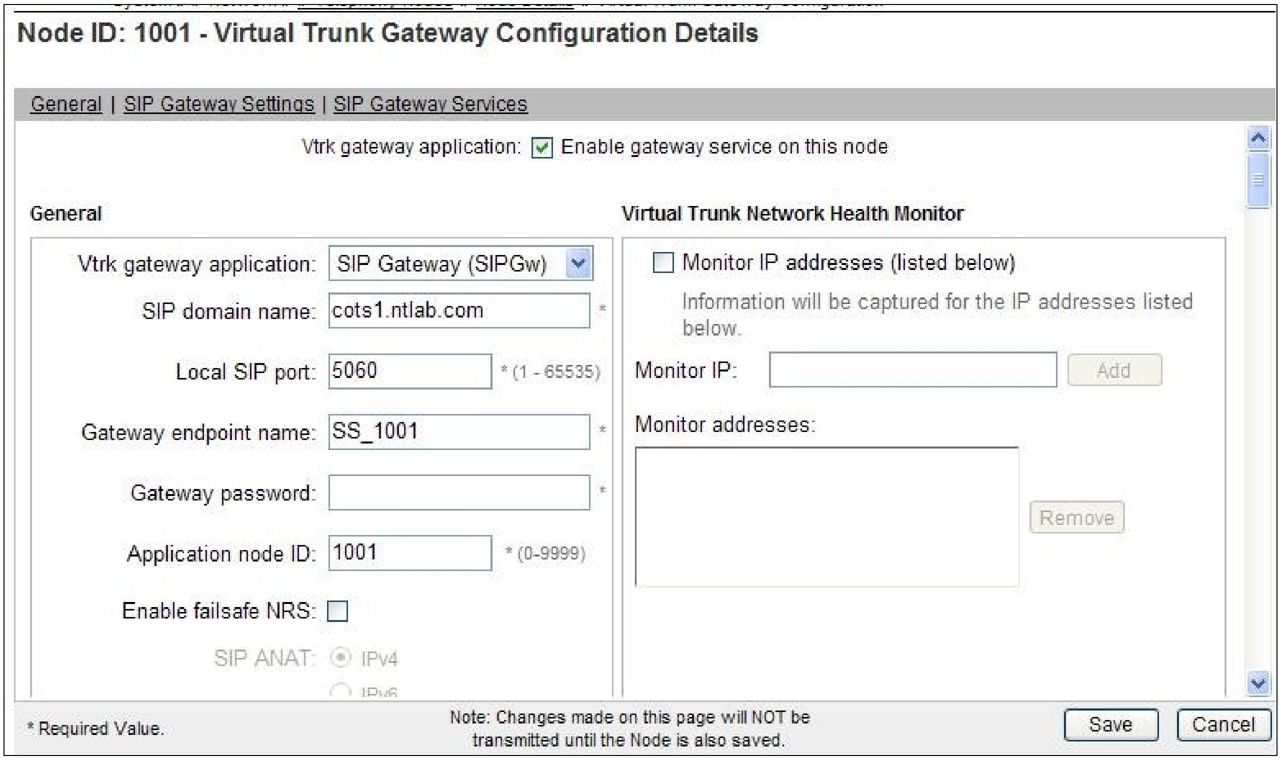
Node IPv6 address:

IP Telephony Node Properties
Voice Gateway (VGW) and Codecs
Quality of Service (QoS)
LAN
SNTP
Numbering Zones
MCDN Alternative Routing Treatment (MALT) Causes
Applications (click to edit configuration)
SIP Line
Terminal Proxy Server (TPS)
Gateway (SIPGw)
Personal Directories (PD)
Presence Publisher
IP Media Services
* Required Value.
Save
Cancel

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

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

The values defined for the sample configuration are shown below.



Node ID: 1001 - Virtual Trunk Gateway Configuration Details

Vtrk gateway application: ☑ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: cots1.ntlab.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: SS_1001 *

Gateway password: *

Application node ID: 1001 * (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ● IPv4 ○ IPv6

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

* Required Value.

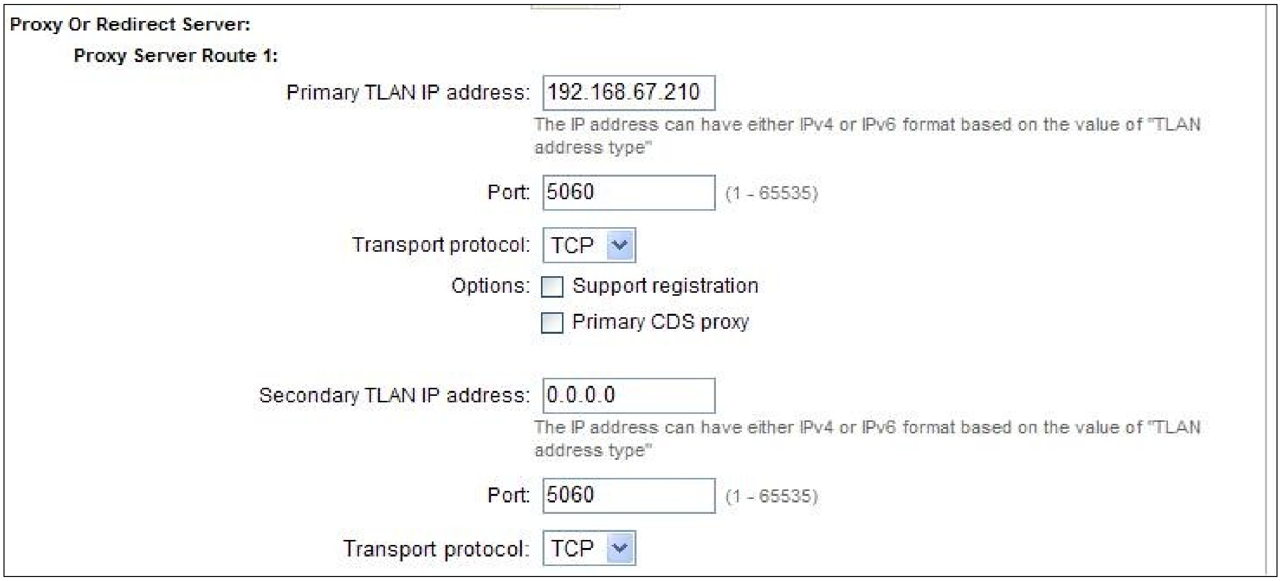
Note: Changes made on this page will NOT be transmitted until the Node is also saved.

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.



Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 192.168.67.210

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

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration

☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0

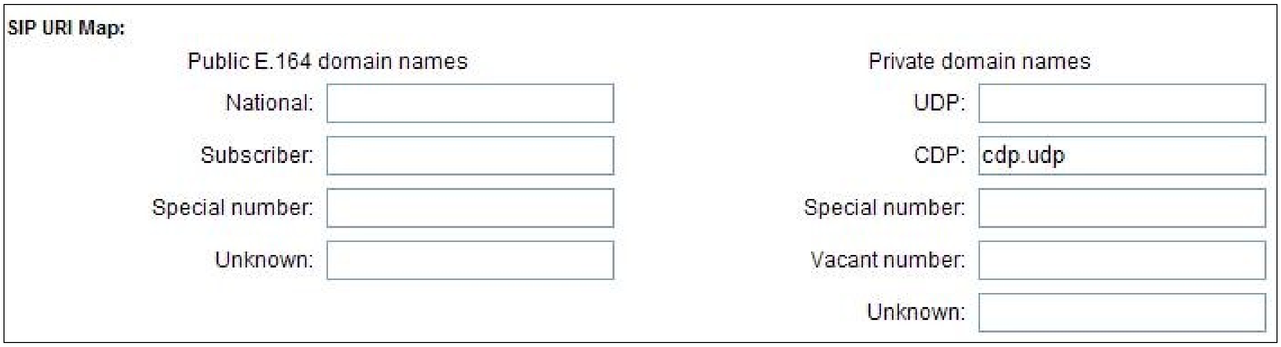
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: 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 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, the Avaya CS1000E will omit the "phone-context=" in the SIP header altogether.



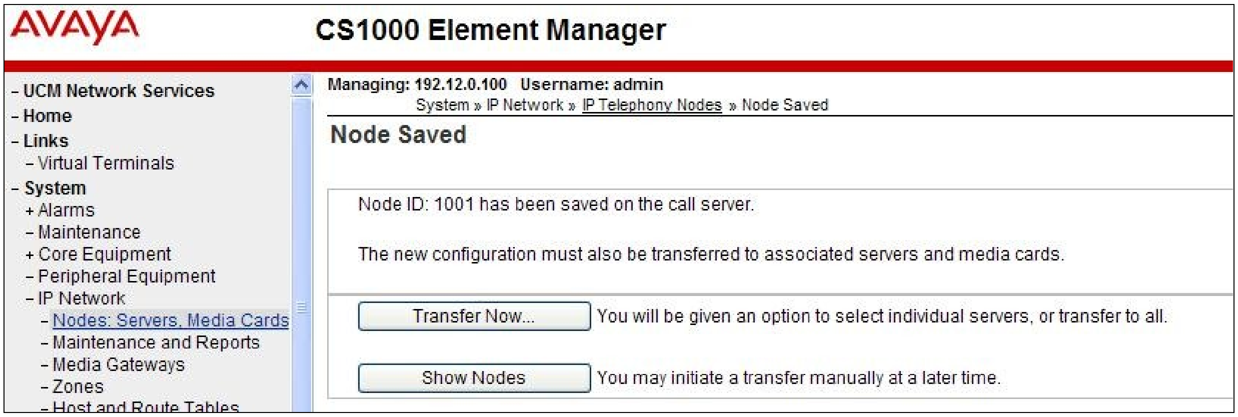
SIP URI Map:

Public E.164 domain names		Private domain names	
National:		UDP:	
Subscriber:		CDP:	cdp.udp
Special number:		Special number:	
Unknown:		Vacant number:	
		Unknown:	

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.



Node Saved

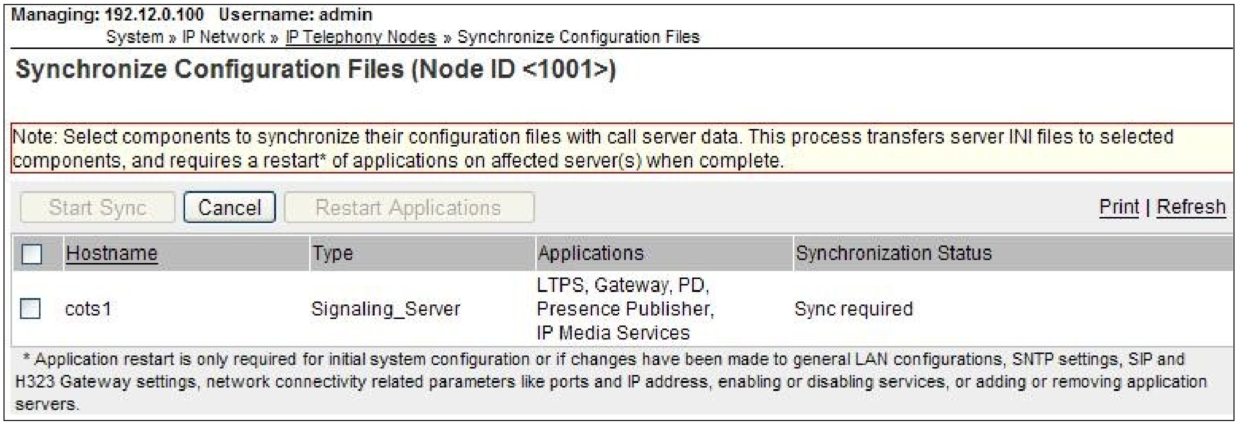
Node ID: 1001 has been saved on the call server.

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

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

Show Nodes 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
Start Sync
Cancel
Restart Applications
Print | Refresh

Synchronize Configuration Files (Node ID <1001>)

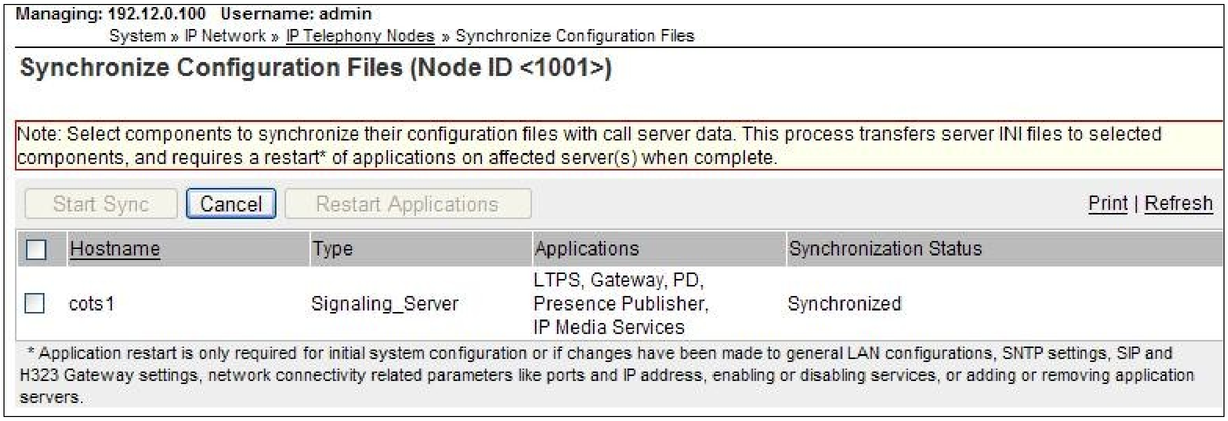
Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

☐	Hostname	Type	Applications	Synchronization Status
☐	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
Start Sync
Cancel
Restart Applications
Print | Refresh

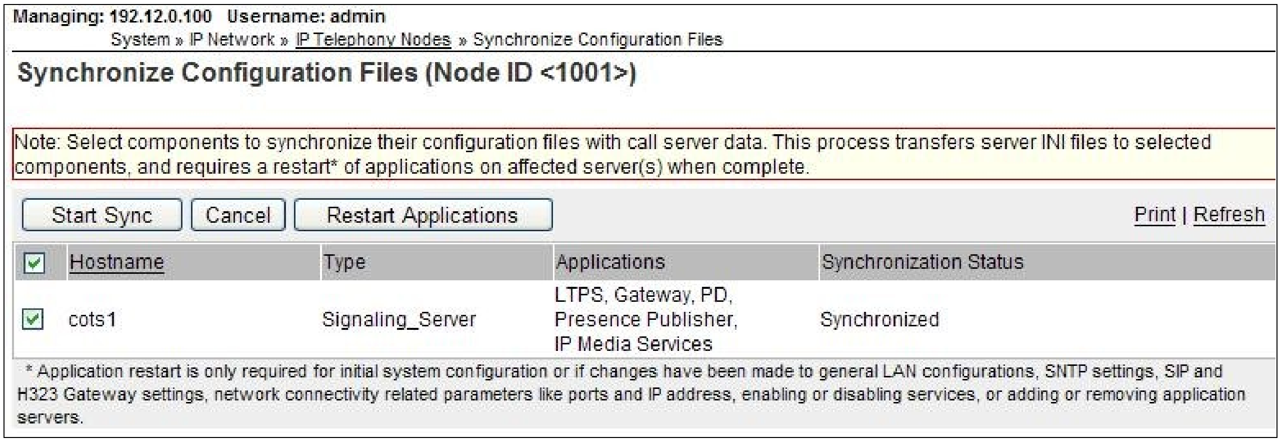
Synchronize Configuration Files (Node ID <1001>)

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.

☐	Hostname	Type	Applications	Synchronization Status
☐	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
Start Sync
Cancel
Restart Applications
Print | Refresh

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.

☑	Hostname	Type	Applications	Synchronization Status
☑	cots1	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

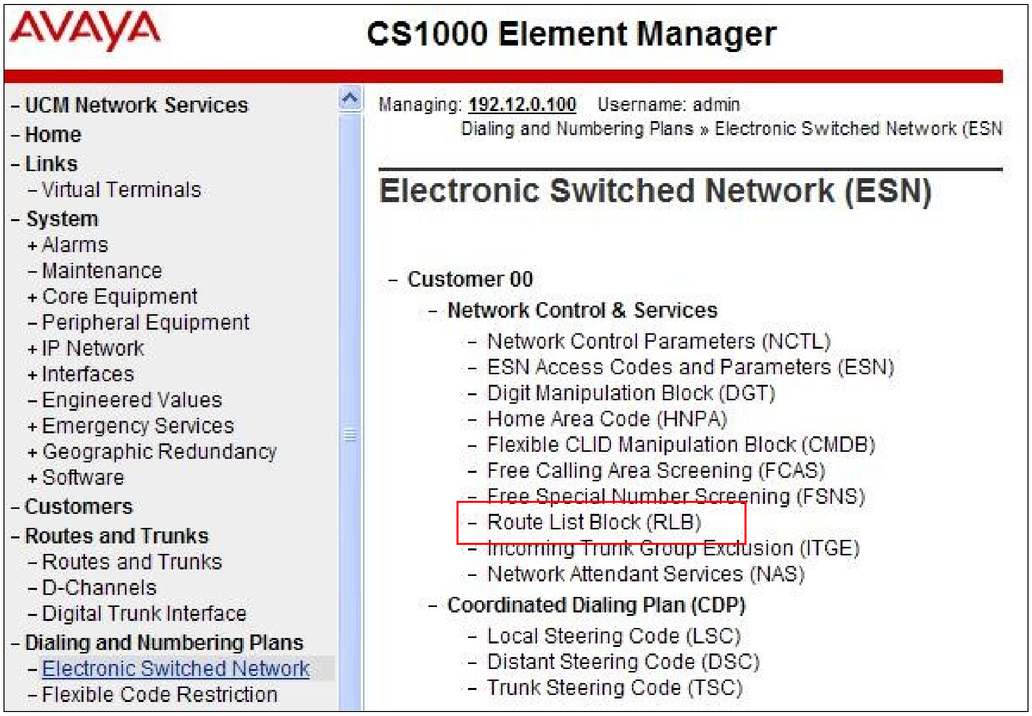
* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application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

5.4. Routing of Outbound Dialed Numbers to Session Manager

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

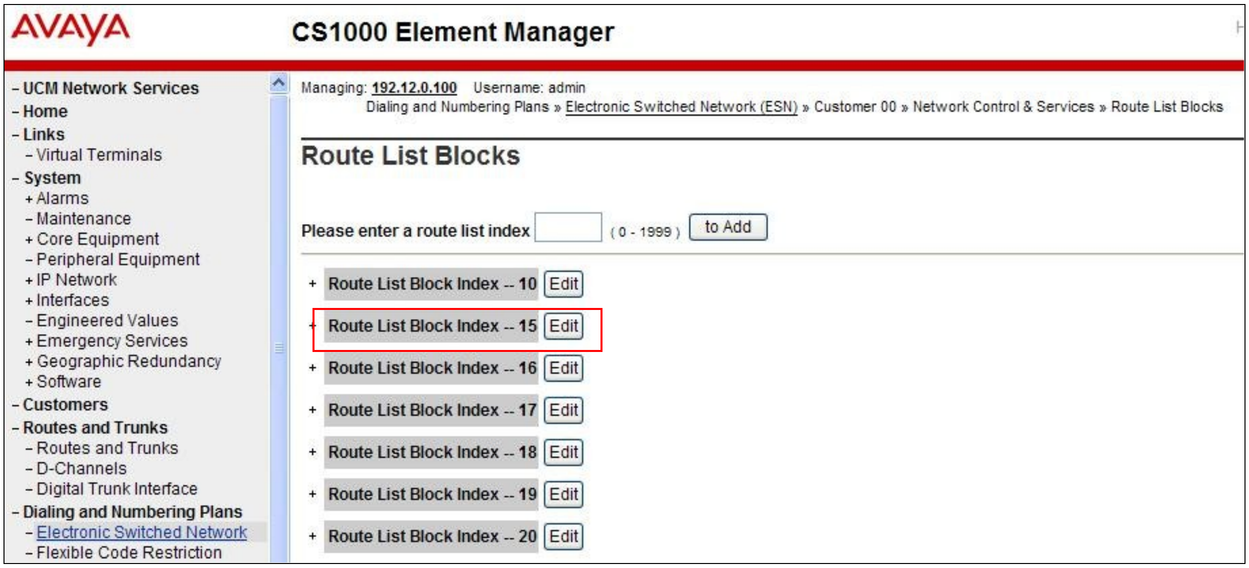
5.4.1 Route List Block

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


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN
Electronic Switched Network (ESN)
- Customer 00
- Network Control & Services
- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)
- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)

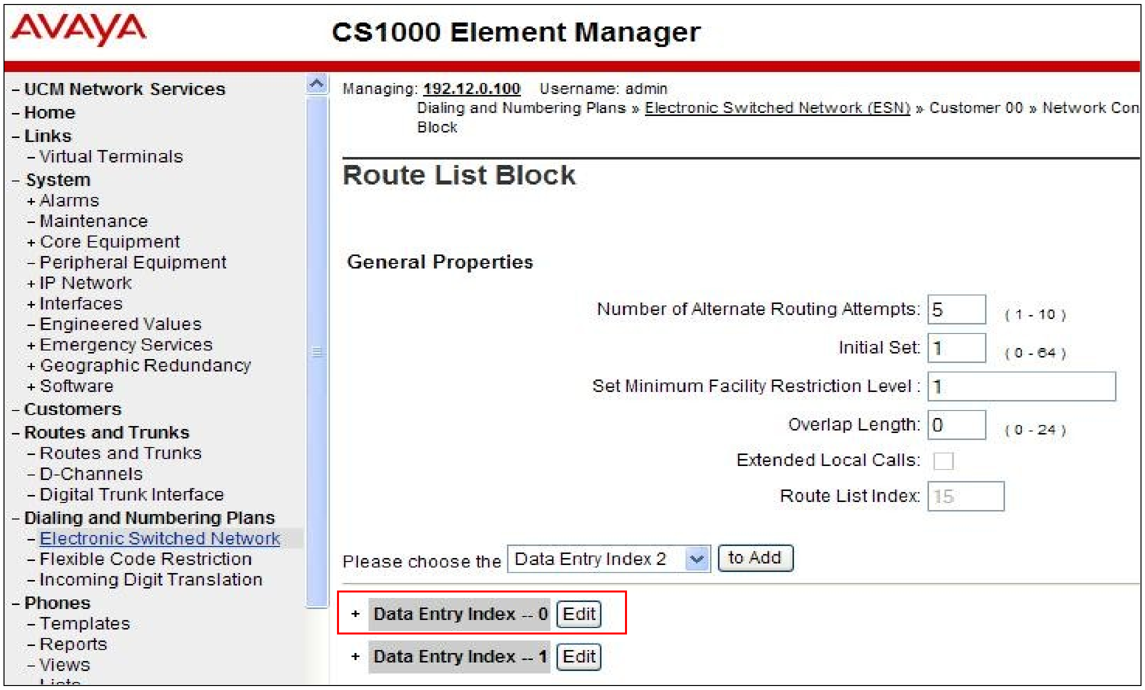
The **Route List Blocks** screen is displayed.

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


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks
Route List Blocks
Please enter a route list index (0 - 1999) to Add
+ Route List Block Index -- 10 Edit
+ Route List Block Index -- 15 Edit
+ Route List Block Index -- 16 Edit
+ Route List Block Index -- 17 Edit
+ Route List Block Index -- 18 Edit
+ Route List Block Index -- 19 Edit
+ Route List Block Index -- 20 Edit

The Route List Block screen will open.

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

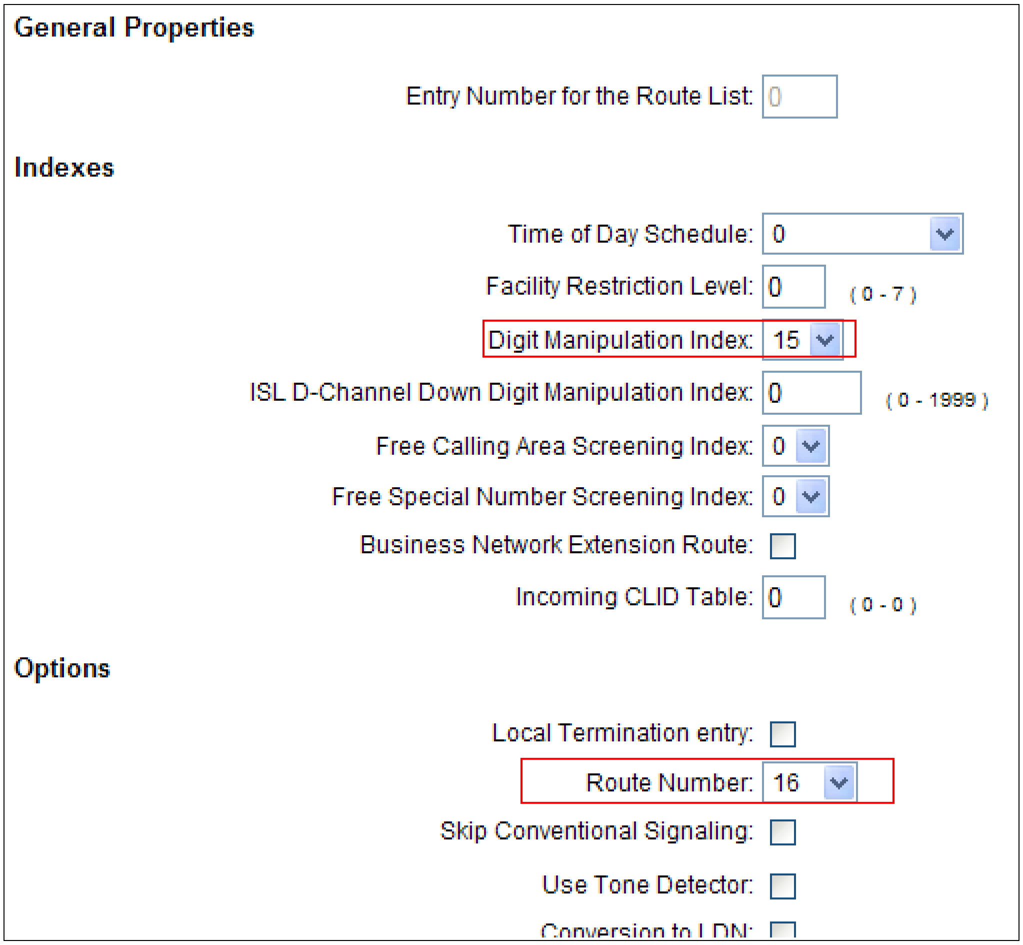


Number of Alternate Routing Attempts: 5 (1 - 10)
Initial Set: 1 (0 - 64)
Set Minimum Facility Restriction Level : 1
Overlap Length: 0 (0 - 24)
Extended Local Calls: ☐
Route List Index: 15
Please choose the Data Entry Index 2 to Add

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

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

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



General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 15

ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: ☐

Incoming CLID Table: 0 (0 - 0)

Options

Local Termination entry: ☐

Route Number: 16

Skip Conventional Signaling: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

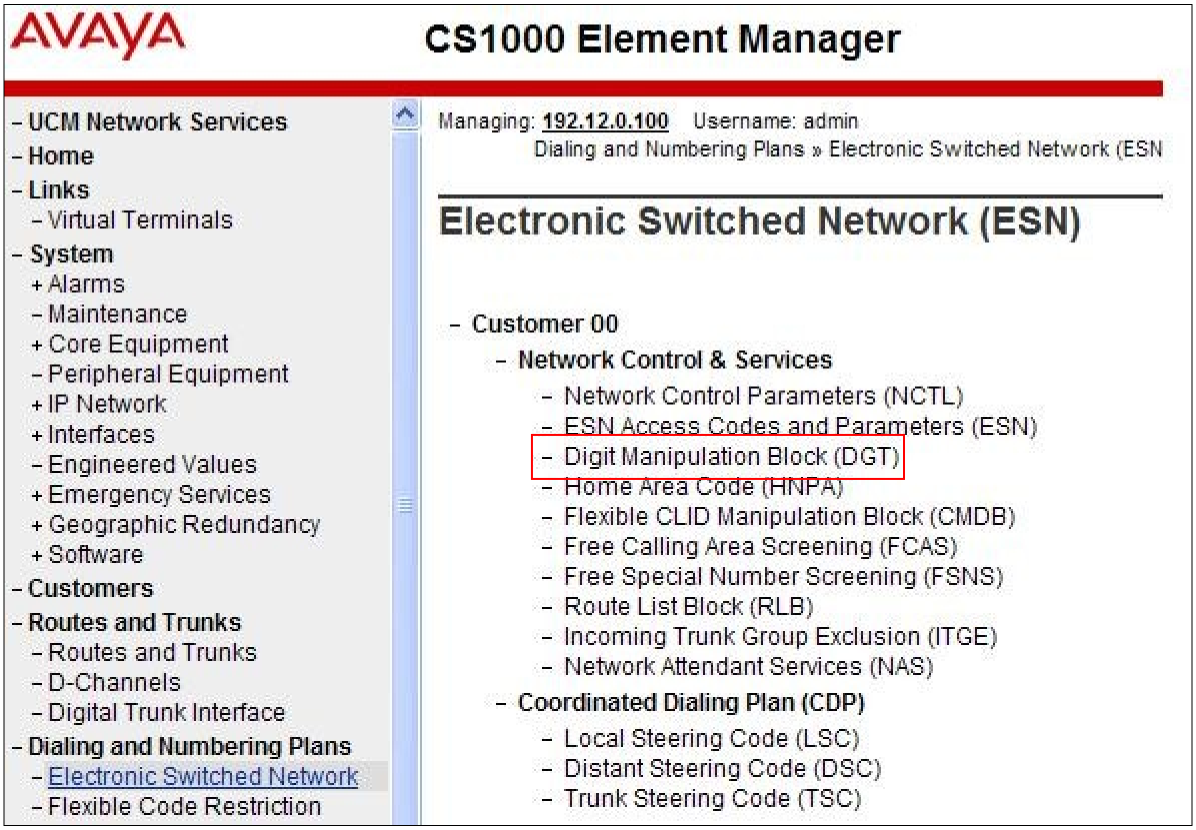
Step 6 - Click **Submit** (not shown) to save the Route List Block definitions.

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

5.4.2 Digit Manipulation Block

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

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

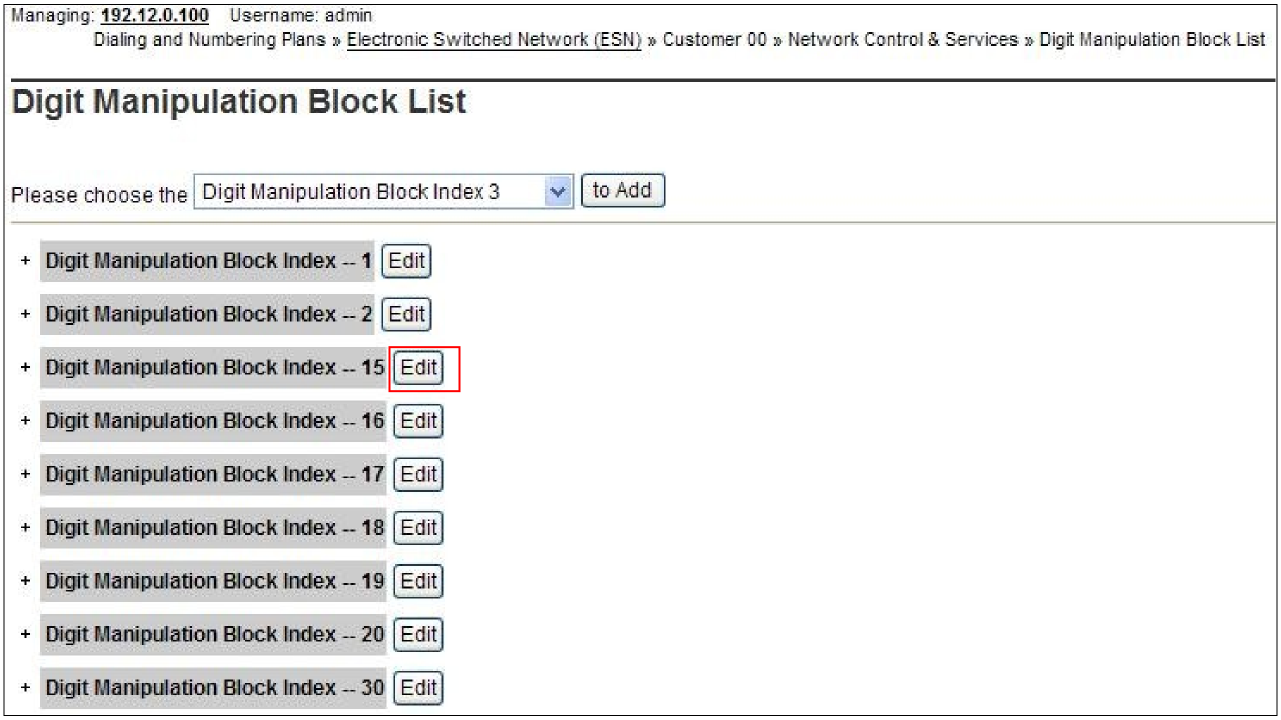


Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN

Electronic Switched Network (ESN)

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

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

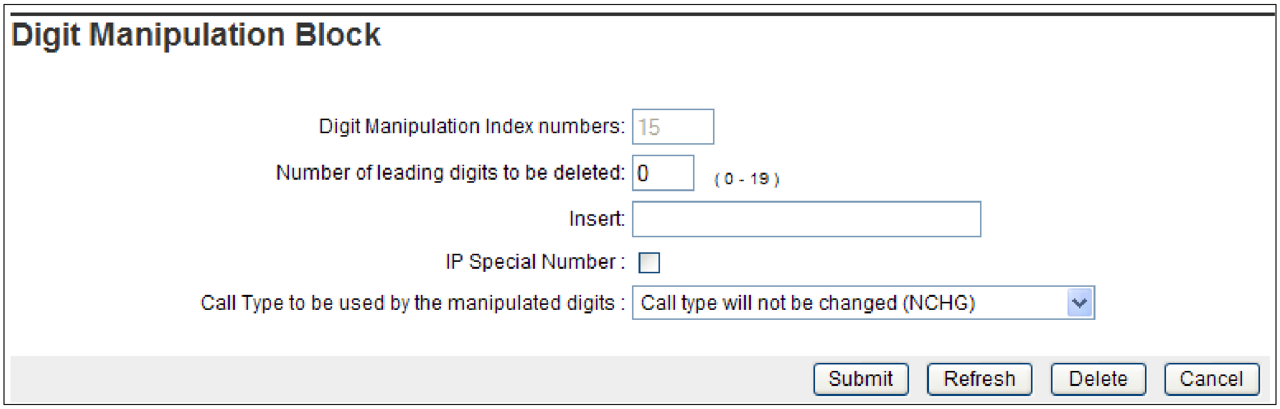

Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List

Digit Manipulation Block List

Please choose the Digit Manipulation Block Index 3 to Add

+ Digit Manipulation Block Index -- 1 Edit
+ Digit Manipulation Block Index -- 2 Edit
+ Digit Manipulation Block Index -- 15 Edit
+ Digit Manipulation Block Index -- 16 Edit
+ Digit Manipulation Block Index -- 17 Edit
+ Digit Manipulation Block Index -- 18 Edit
+ Digit Manipulation Block Index -- 19 Edit
+ Digit Manipulation Block Index -- 20 Edit
+ Digit Manipulation Block Index -- 30 Edit

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



Digit Manipulation Block

Digit Manipulation Index numbers: 15

Number of leading digits to be deleted: 0 (0 - 19)

Insert:

IP Special Number : ☐

Call Type to be used by the manipulated digits : Call type will not be changed (NCHG)

Step 4 – Click on **Submit**.

5.4.3 NARS Access Code

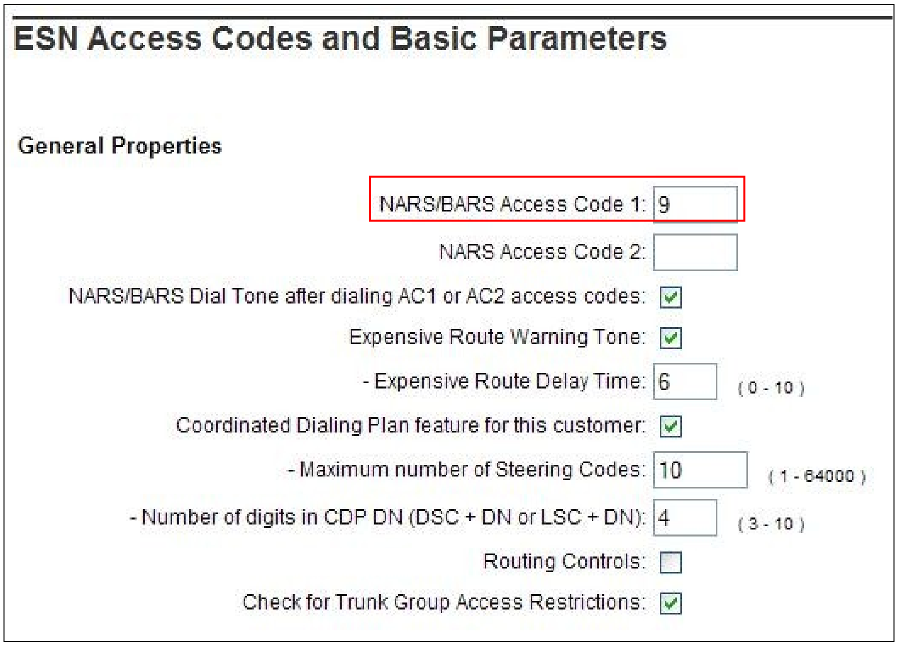
This section defines the access code for off-net dialing (e.g. calls to PSTN).

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

Step 2 - Select **ESN Access Codes and Parameters (ESN).** Although not repeated below, the option can be seen on the screenshot shown in **Section 5.4.1**, **Step 1**.

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

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



ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 9

NARS Access Code 2:

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

Expensive Route Warning Tone: ☑

- Expensive Route Delay Time: 6 (0 - 10)

Coordinated Dialing Plan feature for this customer: ☑

- Maximum number of Steering Codes: 10 (1 - 64000)

- Number of digits in CDP DN (DSC + DN or LSC + DN): 4 (3 - 10)

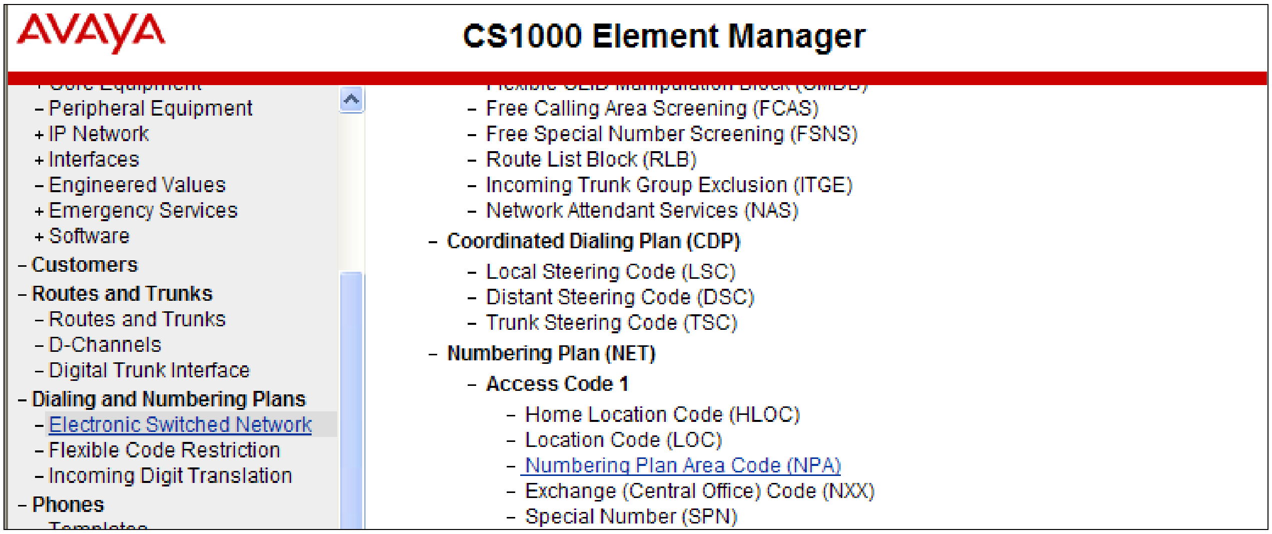
Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☑

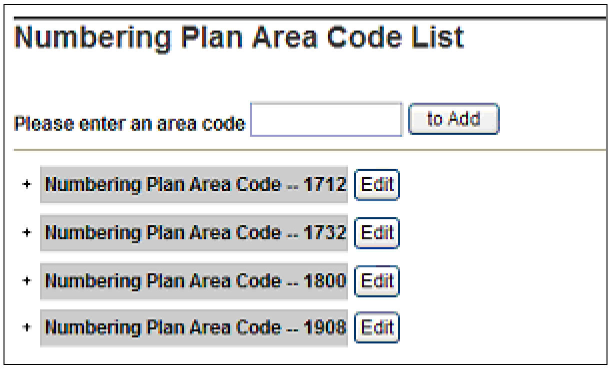
5.4.4 Numbering Plan Area Codes

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

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

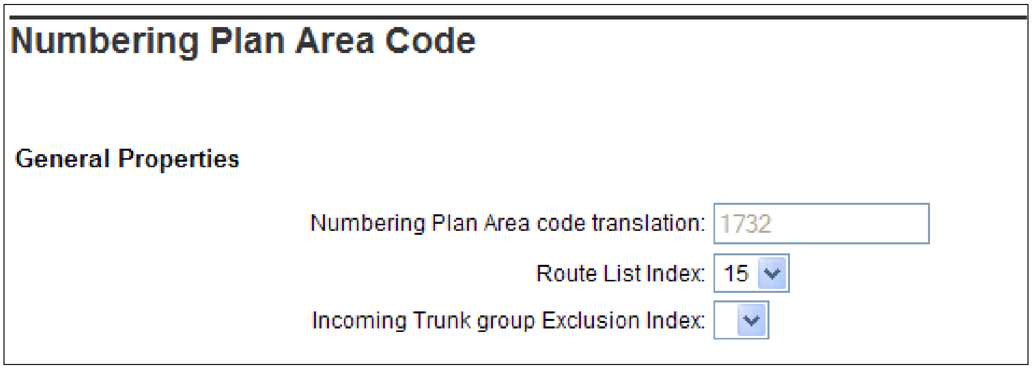

AVAYA
CS1000 Element Manager
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)
- Numbering Plan (NET)
- Access Code 1
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)

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



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

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



Numbering Plan Area Code

General Properties

Numbering Plan Area code translation: 1732

Route List Index: 15

Incoming Trunk group Exclusion Index:

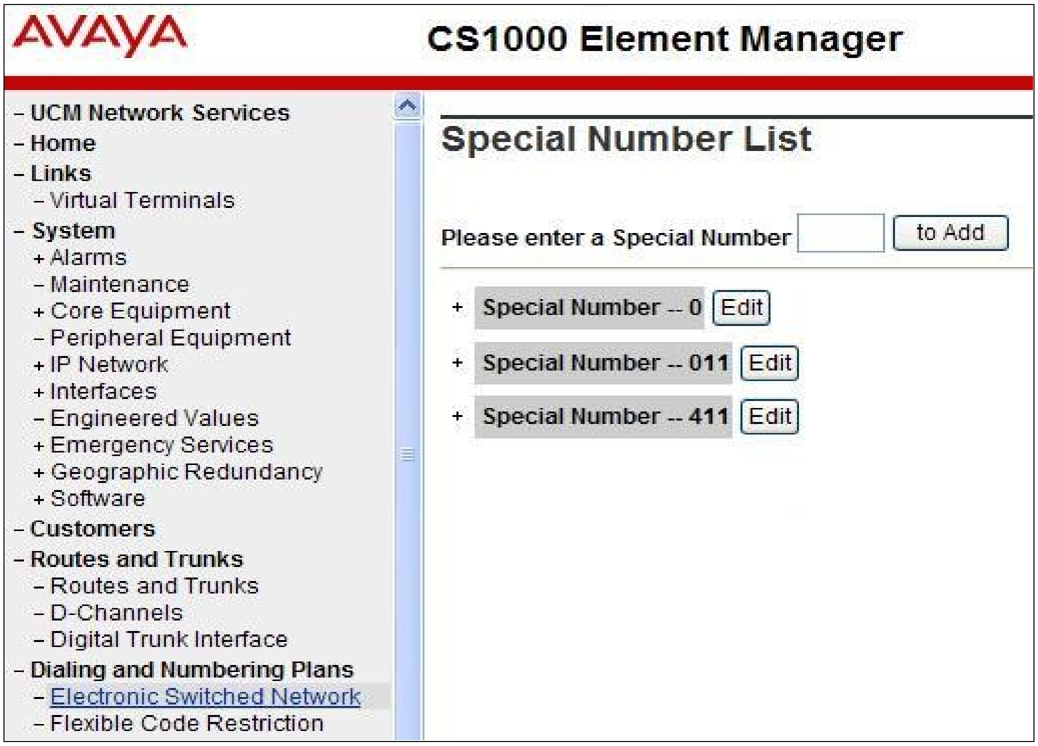
5.4.5 Other Special Numbers to Route to Session Manager

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

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

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

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

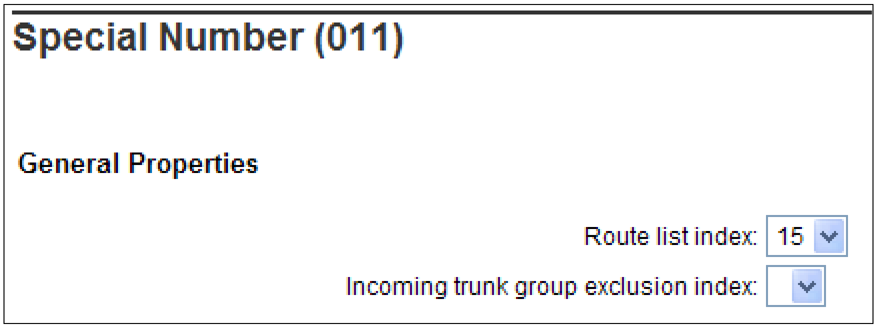


Special Number List

Please enter a Special Number

+ Special Number -- 0
+ Special Number -- 011
+ Special Number -- 411

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



Special Number (011)

General Properties

Route list index: 15

Incoming trunk group exclusion index:

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

5.4.6 Summary

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

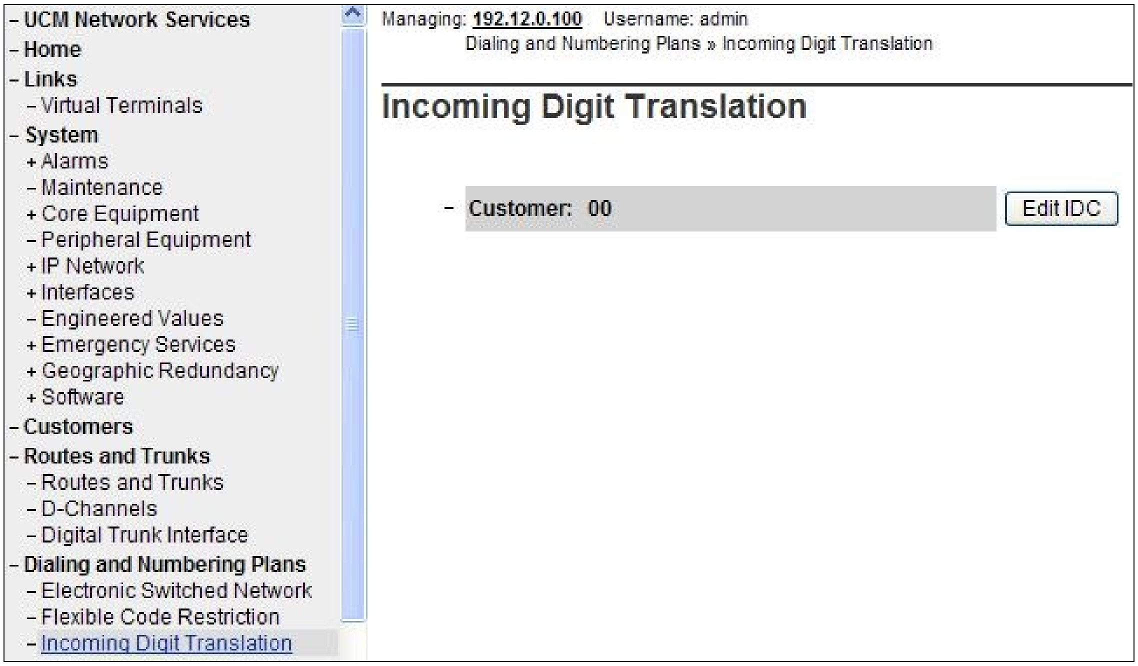
- Routes & Trunks (**Section 5.2.2**)
    - Customer 0
    - Route 16 = SIP trunk
- Route List Block (**Section 5.4.1**)
    - Data 0
        - Route = 16
        - Digit Manipulation = 15
- Digit Manipulation Block 15 (**Section 5.4.2**)
    - Delete = 0
    - Type = NCHG
- ESN Access Codes and Parameters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

5.5. Routing of Inbound Numbers to Avaya CS1000E

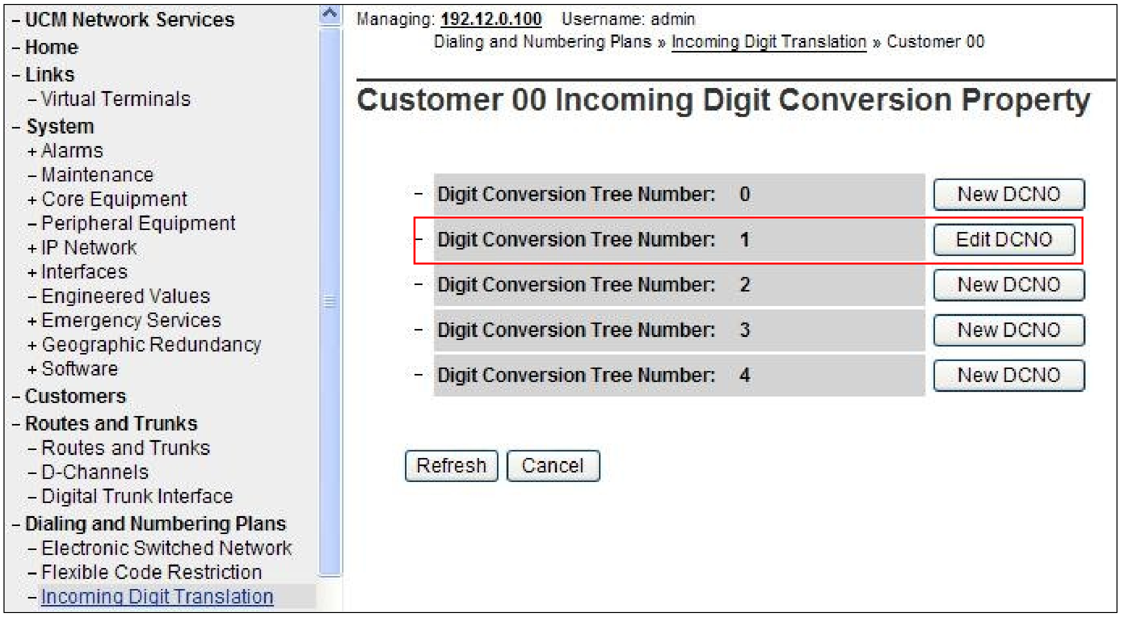
Calls from PSTN will dial AT&T IP Flexible Reach DID numbers to reach stations on Avaya CS1000E. These DID numbers are converted to the associated extensions by the Avaya CS1000E Incoming Digit Translation (IDT) table.

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

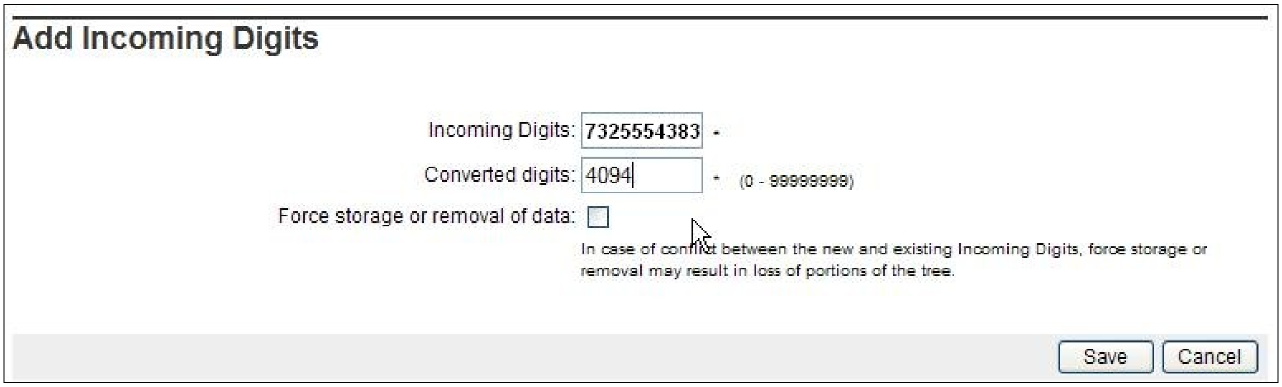
Step 2 – Select the appropriate **Customer ID** (**00** in the reference configuration) and click on **Edit IDC**.



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**.


- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00
Customer 00 Incoming Digit Conversion Property
- Digit Conversion Tree Number: 0
New DCNO
- Digit Conversion Tree Number: 1
Edit DCNO
- Digit Conversion Tree Number: 2
New DCNO
- Digit Conversion Tree Number: 3
New DCNO
- Digit Conversion Tree Number: 4
New DCNO
Refresh
Cancel

Step 4 – The IDC Tree form will open. Click on the **Add** button. In the **Incoming Digits** field, enter an AT&T IP Flexible Reach DID (e.g. **7325554383**). In the **Converted Digits** field, enter the associated Avaya CS1000E extension (e.g. **4094**). Click on **Save**.



Add Incoming Digits

Incoming Digits: 7325554383 *

Converted digits: 4094 * (0 - 99999999)

Force storage or removal of data: ☐

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

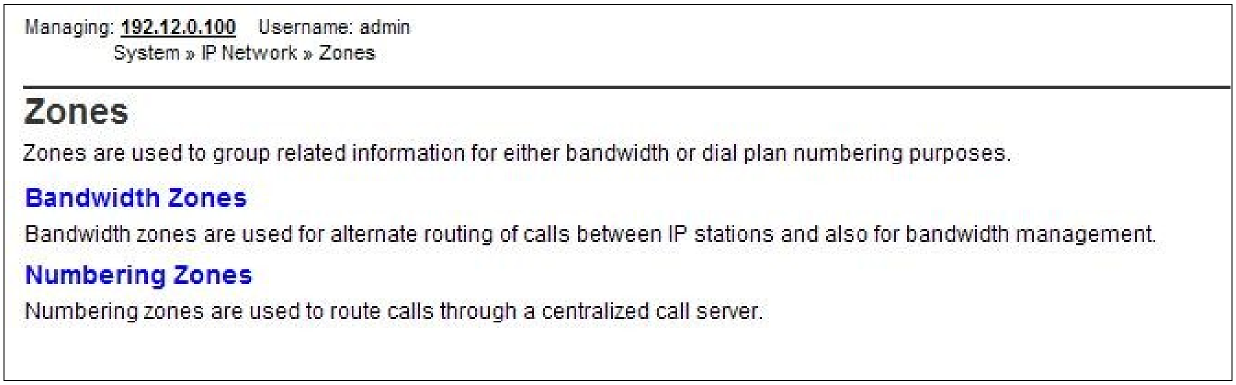
Step 5 – Repeat **Step 4** for all associated AT&T IP Flexible Reach DIDs and extensions.

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

5.6. Zones

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

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



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

Zones

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

Bandwidth Zones

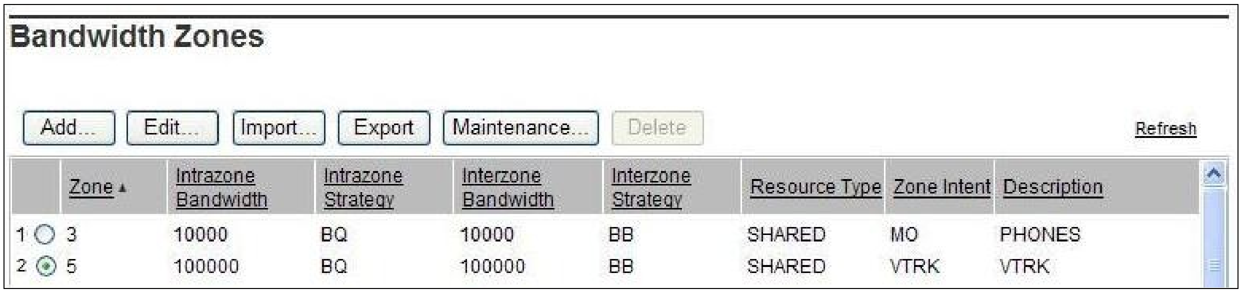
Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones

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

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

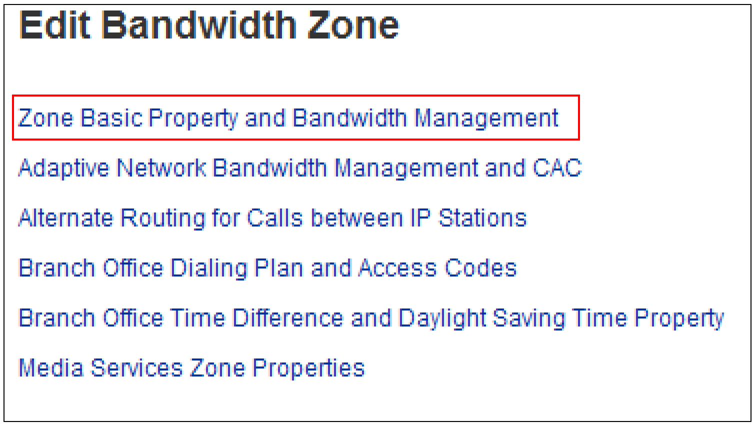
Step 3 - Select the zone associated with the virtual trunk to Session Manager (e.g. item **2**, zone **5**) and click **Edit** as shown below.



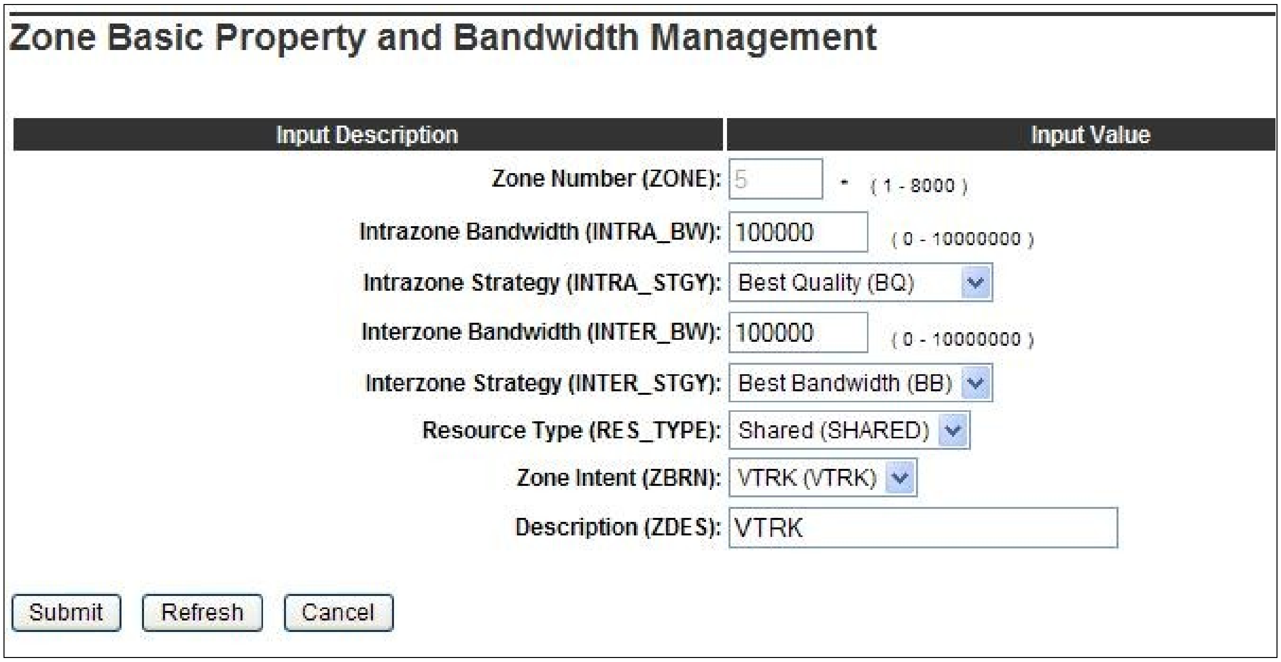
Bandwidth Zones

	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-law for calls with the AT&T IP Flexible Reach service.



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

5.7. Codec Parameters.

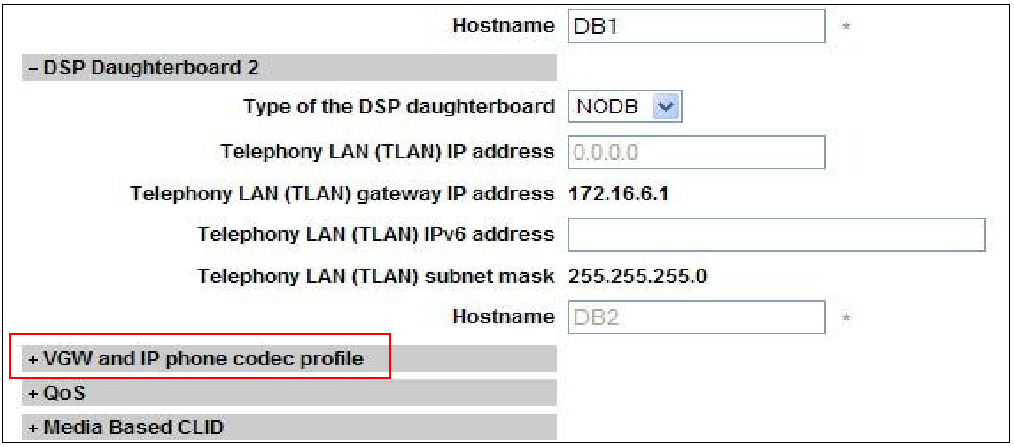
The following section describes how to set codec preferences as well as setting Packet Interval (PTIME) values. Note that the Avaya CS1000E always specifies G.711mu-law regardless of the additional selected codes. Codecs are defined in the **Media Gateway** (for analog and digital phones) and in the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

5.7.1 Media Gateway Codec Configuration

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

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

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



Hostname DB1 *

- DSP Daughterboard 2

Type of the DSP daughterboard NODB

Telephony LAN (TLAN) IP address 0.0.0.0

Telephony LAN (TLAN) gateway IP address 172.16.6.1

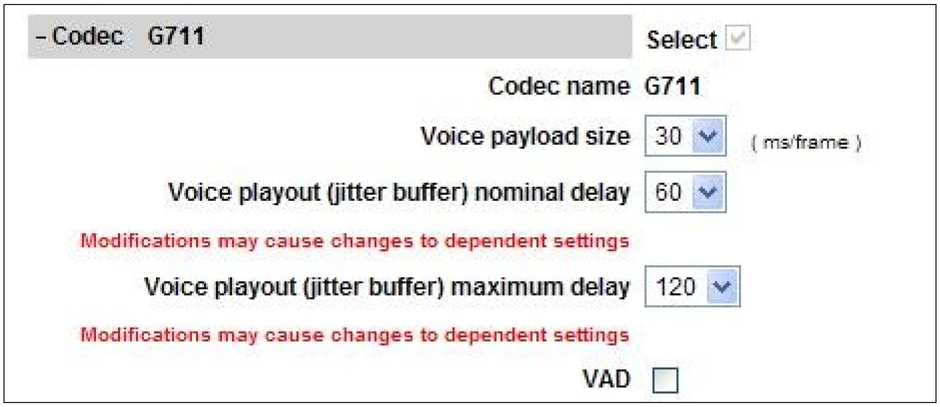
Telephony LAN (TLAN) IPv6 address

Telephony LAN (TLAN) subnet mask 255.255.255.0

Hostname DB2 *

.

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 (ms/frame)

Voice playout (jitter buffer) nominal delay 60

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 120

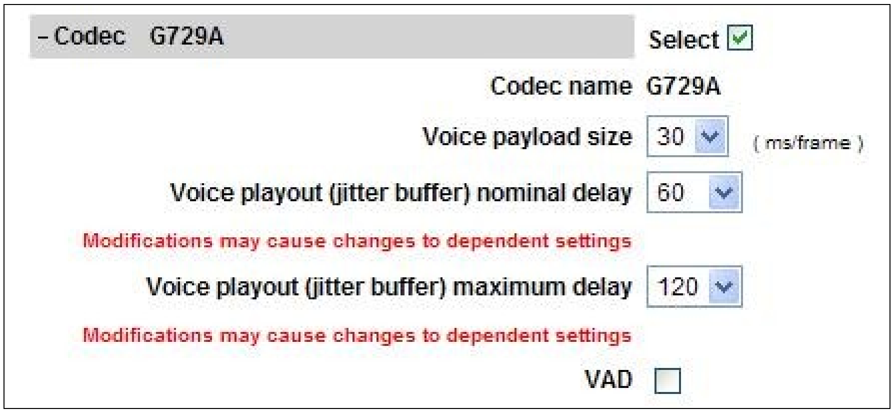
Modifications may cause changes to dependent settings

VAD ☐

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

Note – Although not 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 5.7.2**.

.



- Codec G729A Select ☑

Codec name G729A

Voice payload size 30 (ms/frame)

Voice playout (jitter buffer) nominal delay 60

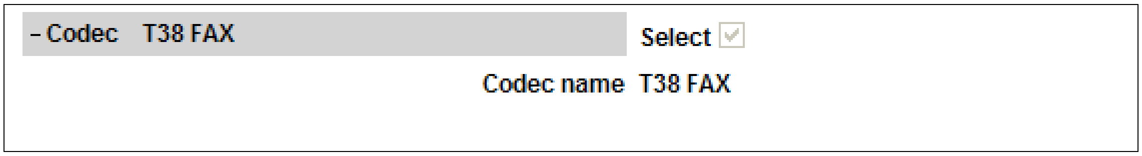
Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 120

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.

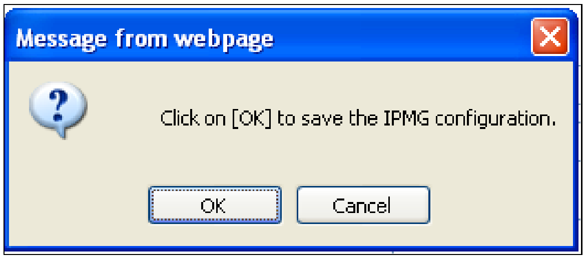


- Codec T38 FAX Select ☑

Codec name T38 FAX

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

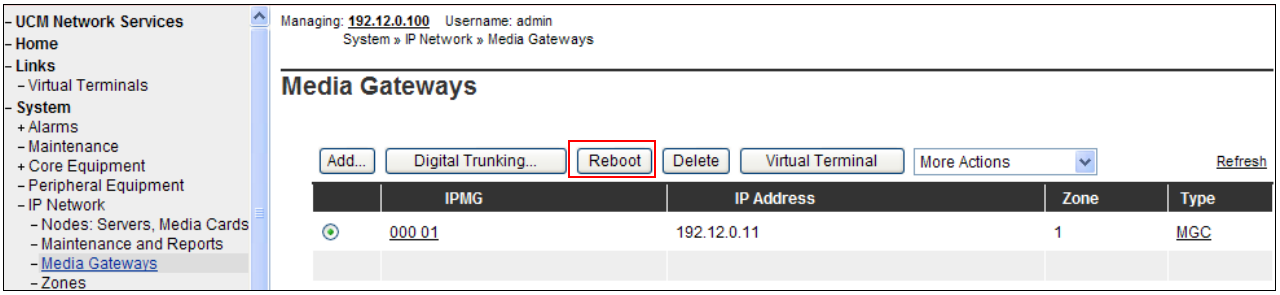
Step 8 – A dialog box will open. Click on **Ok**.



Message from webpage

Click on [OK] to save the IPMG configuration.

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.



Managing: 192.12.0.100 Username: admin

System » IP Network » Media Gateways

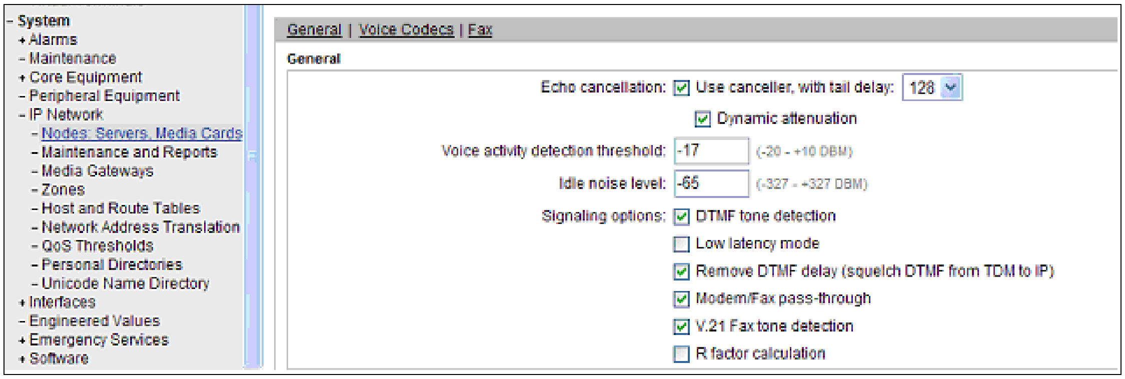
Media Gateways

	IPMG	IP Address	Zone	Type
◉	000 01	192.12.0.11	1	MGC

5.7.2 IP Telephony Node Codec Configuration

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

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



General

Echo cancellation: ☑ Use canceller, with tail delay: 128

☑ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☑ DTMF tone detection

☐ Low latency mode

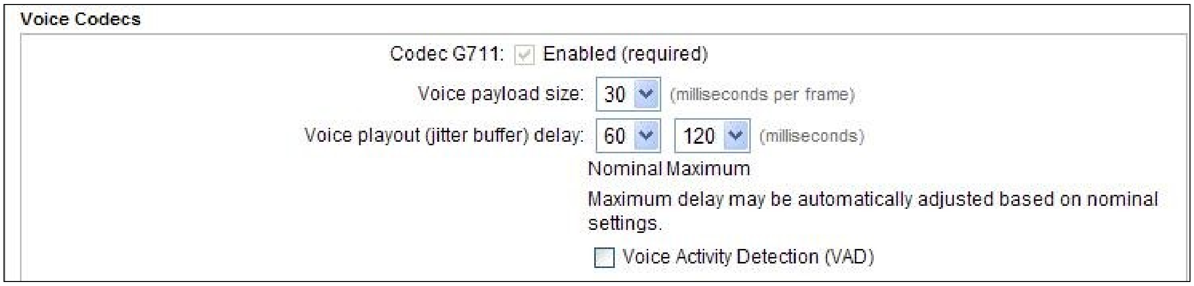
☑ Remove DTMF delay (squelch DTMF from TDM to IP)

☑ Modem/Fax pass-through

☑ V.21 Fax tone detection

☐ R factor calculation

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)

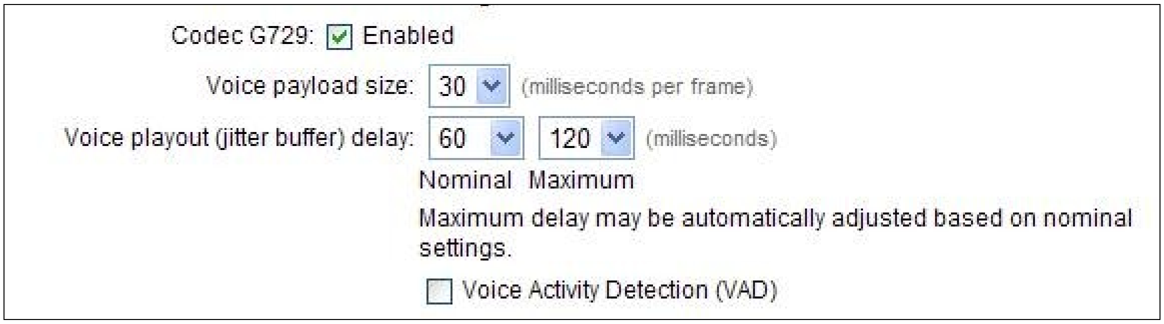
Nominal Maximum

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 5.7.1**.



Codec G729: ☑ Enabled

Voice payload size: 30 (milliseconds per frame)

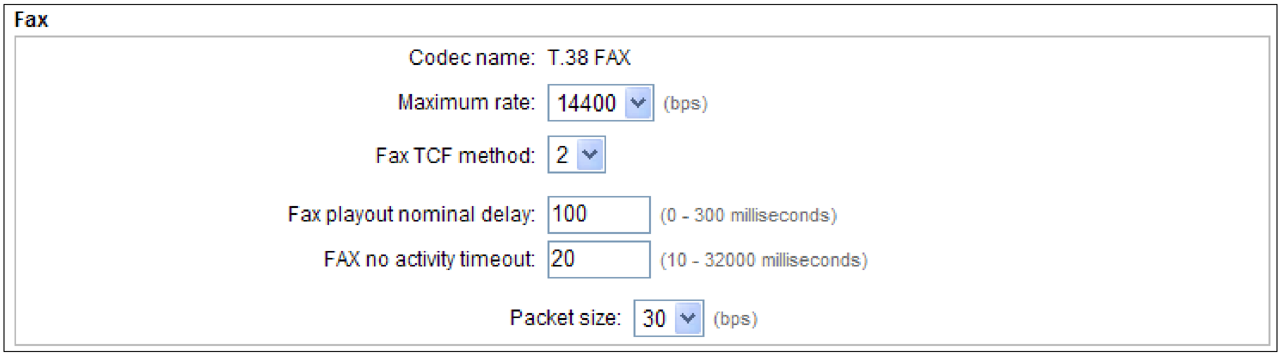
Voice playout (jitter buffer) delay: 60 120 (milliseconds)

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**.



Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

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

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

Packet size: 30 (bps)

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

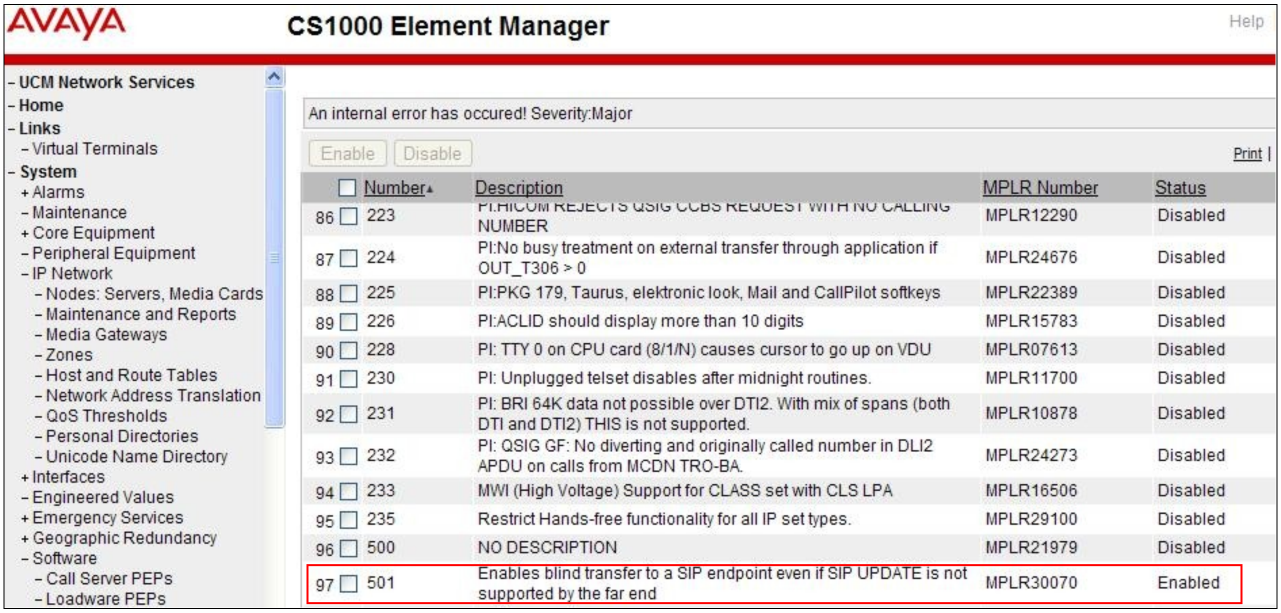
5.8. Enabling Plug-Ins for Call Transfer Scenarios

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

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

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

Note - Enabling plug-in 501 will allow the user to complete the transfer while the call is in a ringing state, but no audible ring back tone will be heard after the transfer is completed.



An internal error has occured! Severity:Major

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

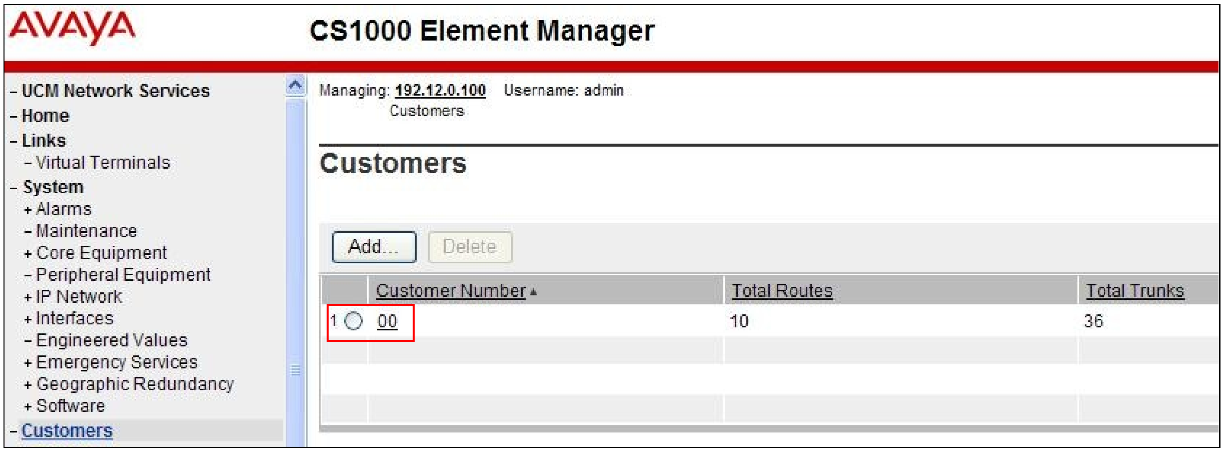
5.9. Customer Information

In the reference configuration, specific calling number information is required based on the destination of the call. For Calls to the AT&T IP Flexible Reach service, AT&T assigned DIDs are required.

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

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

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

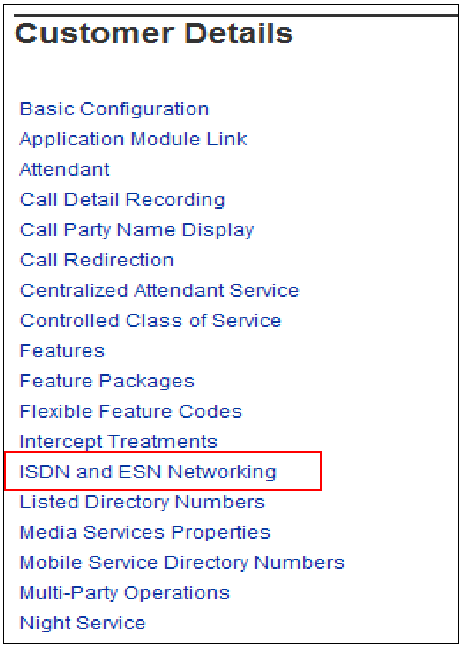


Managing: 192.12.0.100 Username: admin
Customers

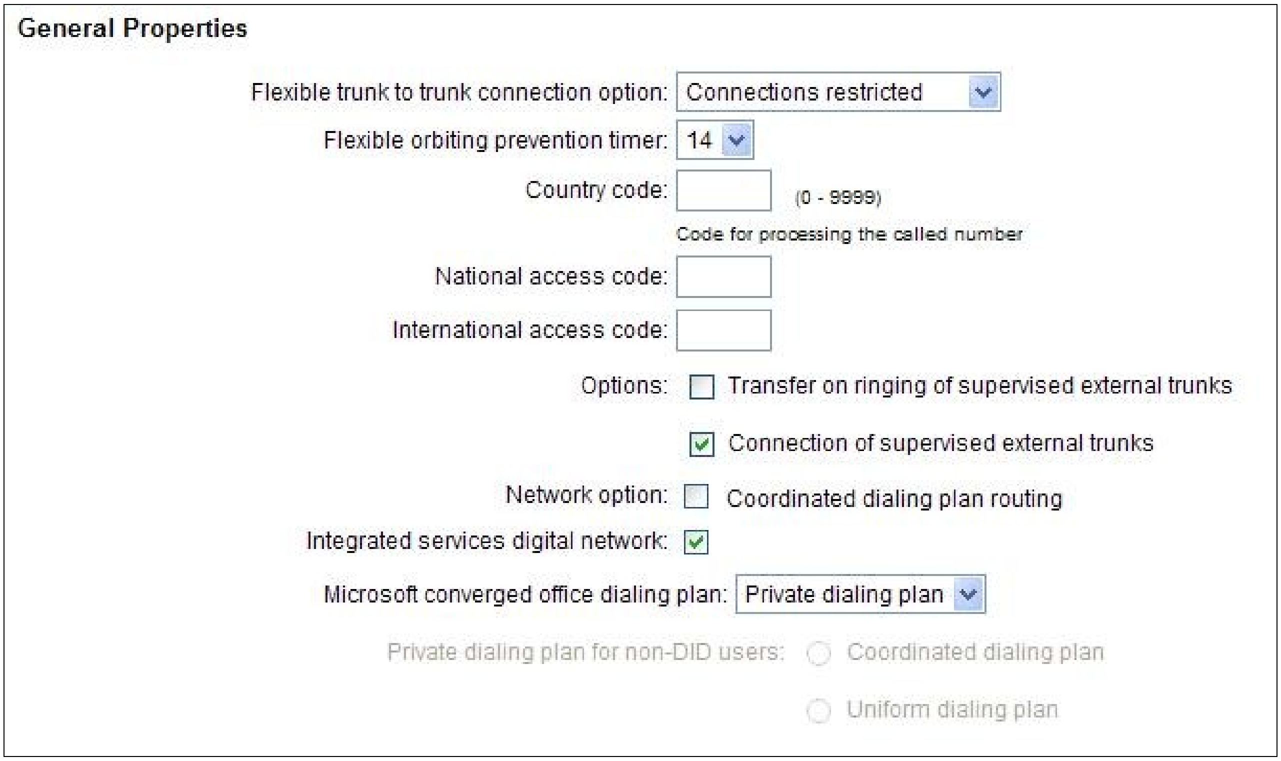
Customers

	Customer Number ▴	Total Routes	Total Trunks
1 ○	00	10	36

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



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



General Properties

Flexible trunk to trunk connection option: Connections restricted

Flexible orbiting prevention timer: 14

Country code: (0 - 9999)

Code for processing the called number

National access code:

International access code:

Options: ☐ Transfer on ringing of supervised external trunks

☑ Connection of supervised external trunks

Network option: ☐ Coordinated dialing plan routing

Integrated services digital network: ☑

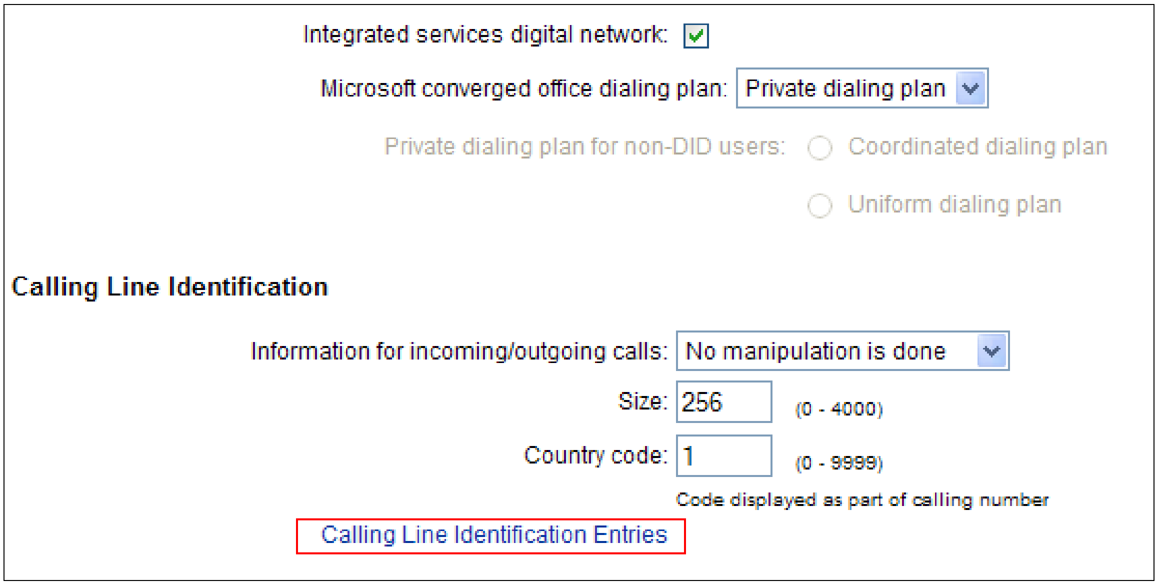
Microsoft converged office dialing plan: Private dialing plan

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

○ Uniform dialing plan

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

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



Integrated services digital network: ☑

Microsoft converged office dialing plan: Private dialing plan

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)

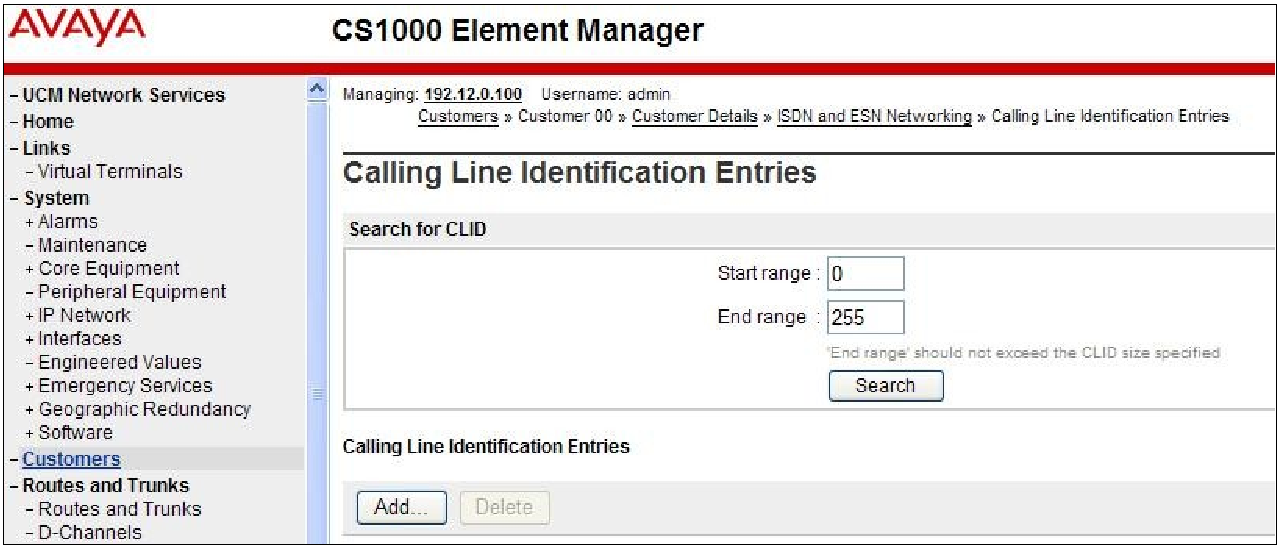
Country code: 1 (0 - 9999)

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**" (zero) in the **Start range** field and in the **End range** field enter one less than the **Size** value from **Step 3** above (e.g. enter **255**). Click on **Search**.



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

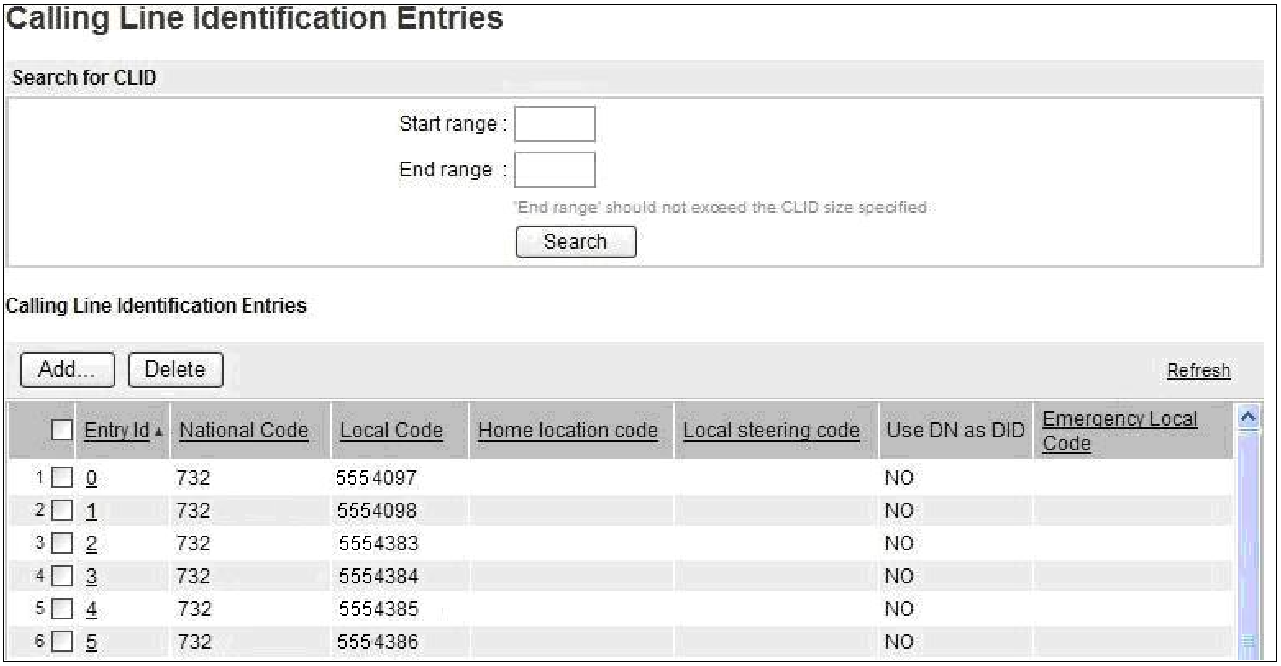
Start range : 0

End range : 255

'End range' should not exceed the CLID size specified

Calling Line Identification Entries

This will display all defined Call Ids. For example, CLID 0 will use 732-555-4097



Calling Line Identification Entries

Search for CLID

Start range :

End range :

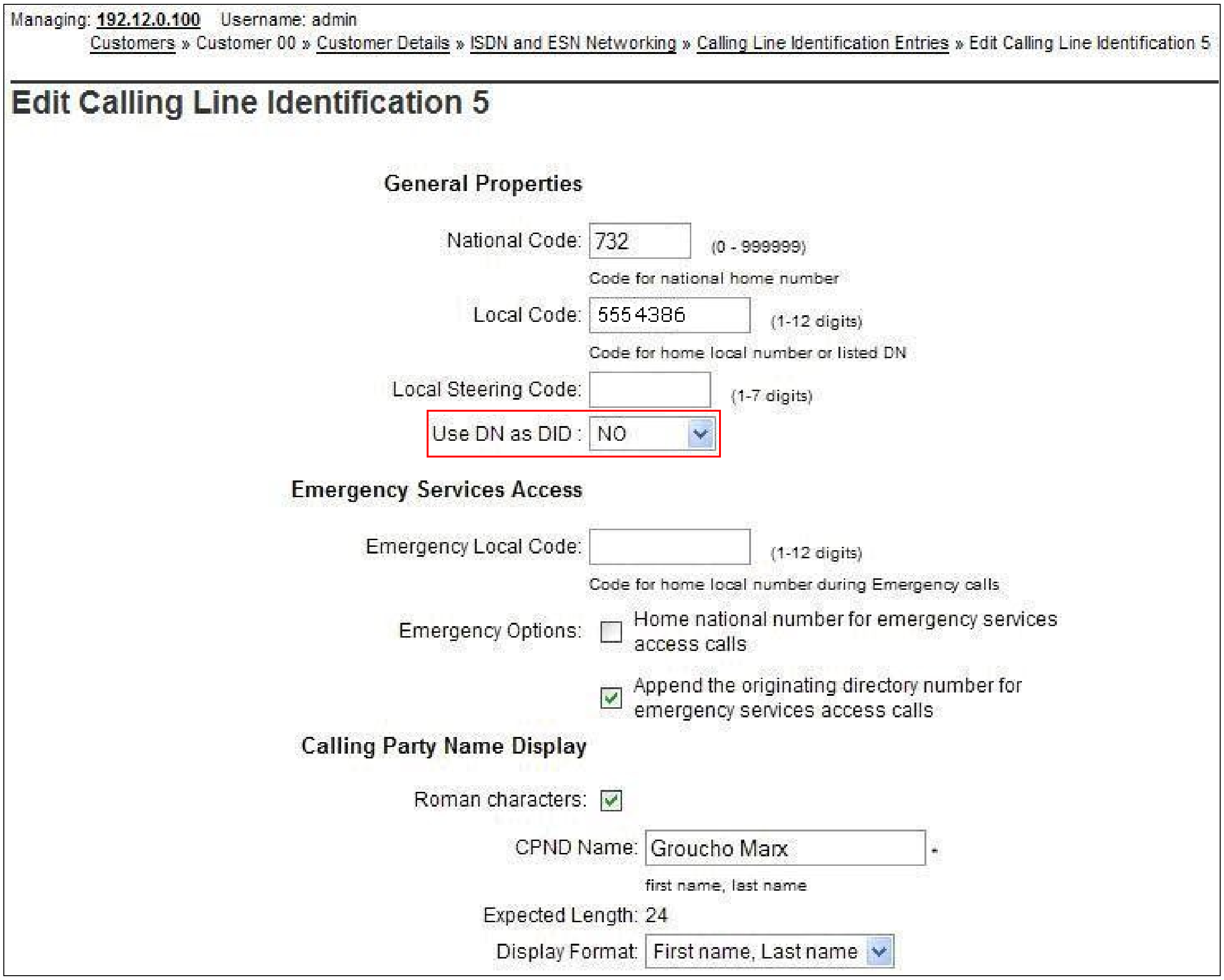
'End range' should not exceed the CLID size specified

Calling Line Identification Entries

	☐	Entry Id ▲	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1	☐	0	732	5554097			NO	
2	☐	1	732	5554098			NO	
3	☐	2	732	5554383			NO	
4	☐	3	732	5554384			NO	
5	☐	4	732	5554385			NO	
6	☐	5	732	5554386			NO	

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

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



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

Edit Calling Line Identification 5

General Properties

National Code: 732 (0 - 999999)
Code for national home number

Local Code: 5554386 (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
☑ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☑

CPND Name: Groucho Marx *
first name, last name

Expected Length: 24

Display Format: First name, Last name

Call IDs are then associated with specific telephone directory numbers (DNs) assigned to stations. See **Section 5.10.**

5.9.1.1 Summary

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

- Customers = 00 (**Section 5.9.1**)
  - ISDN & ESN Networking
    - Calling Line Identification Entries
      - CLID Search
        - Start = 1
        - End = 255
          - Entry ID 5
            - National code = 732
            - Local code - 5554386
            - Use DN as DID = NO
- Phones (**Section 5.10.1**)

- DN 4094 (select TN)
    - Key 0
        - CLID = 5

5.10. Avaya CS1000E Stations

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

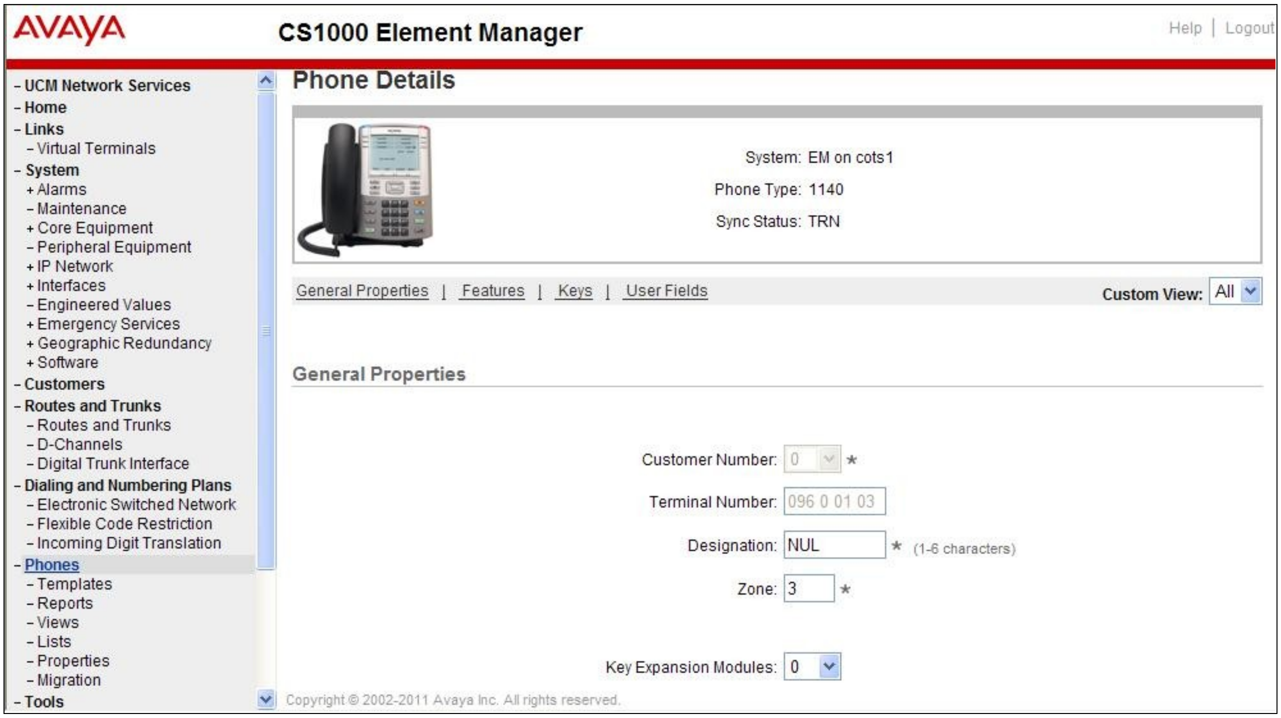
5.10.1 Example IP UNIStim Phone DN 4094,

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

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

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

Step 3 – Click on the TN value (e.g. **096 0 01 03**). The **Phone Details** form will open. Note that the telephone type is an 1140 and that it is defined in Zone 3. A call between this telephone and another telephone in Zone 3 will use a "best quality" strategy (see **Section 5.6**) and therefore can use G.711mu-law. If this same telephone calls out to the PSTN via the SIP trunk, the call would use a "best bandwidth" strategy, and the call would use G.729A.



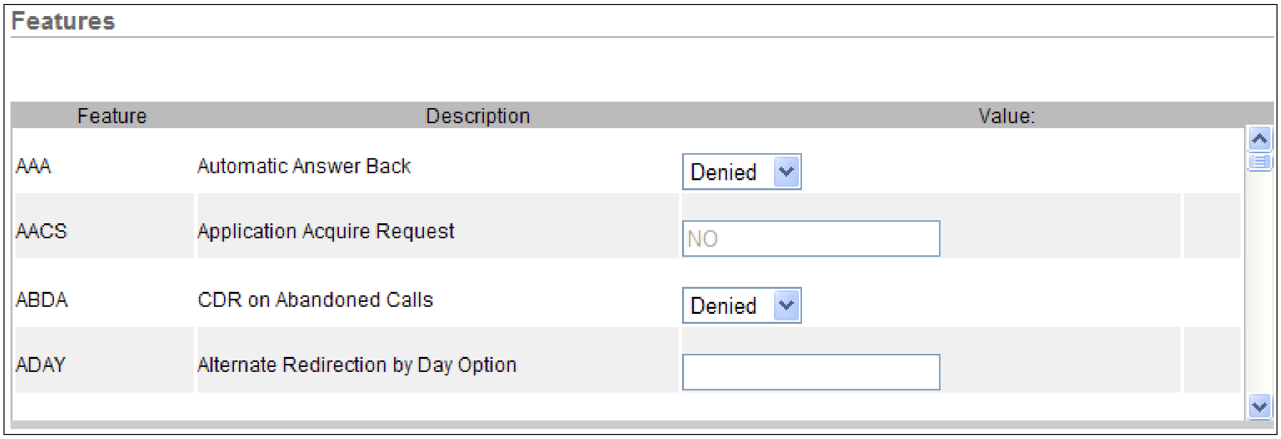
System: EM on cots1
Phone Type: 1140
Sync Status: TRN

Custom View: All

Customer Number: 0 *
Terminal Number: 096 0 01 03
Designation: NUL * (1-6 characters)
Zone: 3 *
Key Expansion Modules: 0

5.10.1.1 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. All of the features described below are found by scrolling through this section.

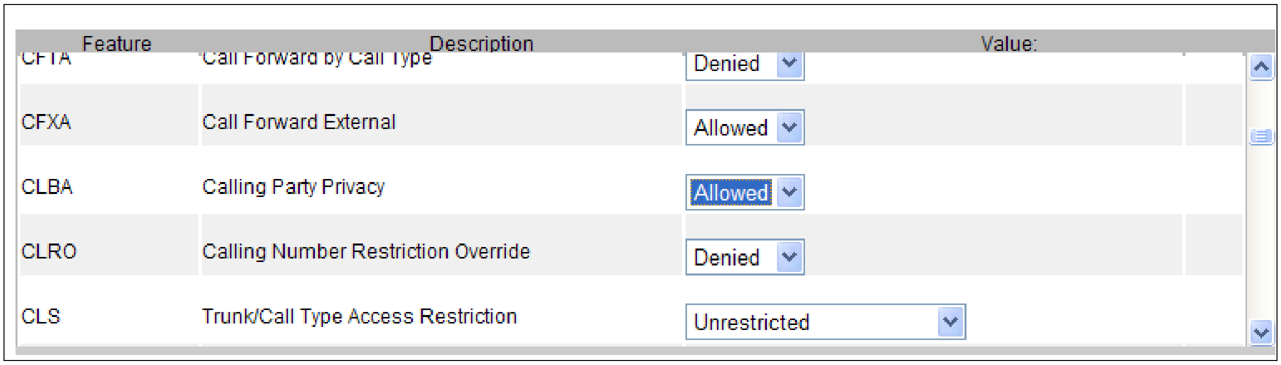


Features

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

5.10.1.1.1 Requesting Privacy

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



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

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

5.10.1.1.2 Call coverage to Call Pilot

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

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

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

Note - The phone Key **MWK** (Message Waiting) is also required (see **Section 5.10.1.2.3** below).

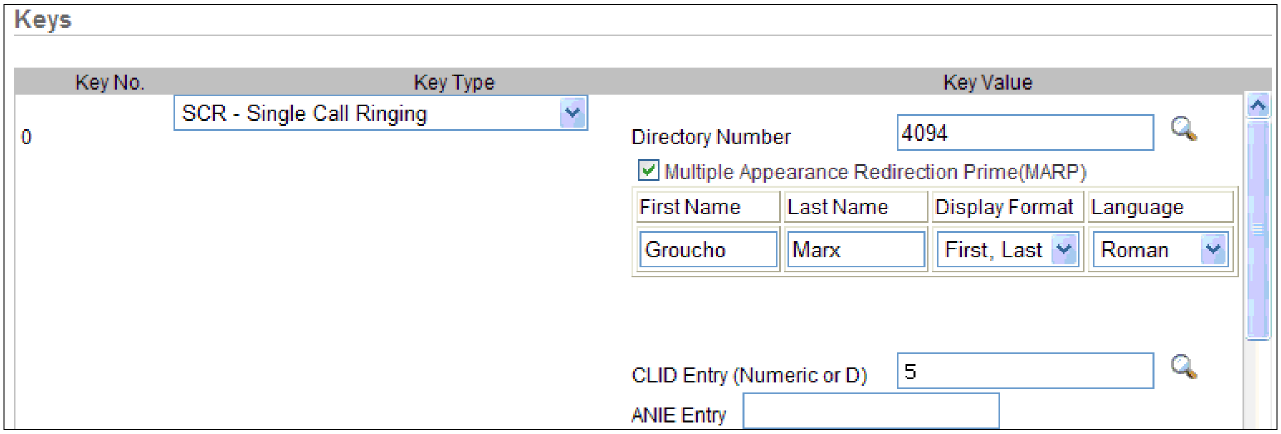
5.10.1.2 Keys

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

5.10.1.2.1 Key 0 - Single Call Appearance

This key defines the first call appearance on the telephone.

Note – The **CLID Entry (Numeric or D)** field is where the CLID defined in **Section 5.9** is associated with this station. In the reference configuration, telephone station 4094 was assigned CLID 5 and therefore will use 7325554386 as its calling number.


Keys

Key No.	Key Type	Key Value
0	SCR - Single Call Ringing	Directory Number 4094

☑ Multiple Appearance Redirection Prime(MARP)

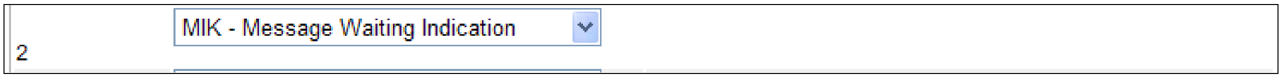
First Name	Last Name	Display Format	Language
Groucho	Marx	First, Last	Roman

CLID Entry (Numeric or D) 5

ANIE Entry

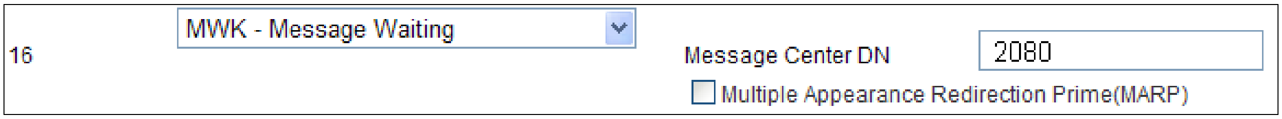
5.10.1.2.2 Key 2 – Message Waiting Indicator

This defines the MWI lamp.


2 MIK - Message Waiting Indication

5.10.1.2.3 Key 16 - Message Waiting

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

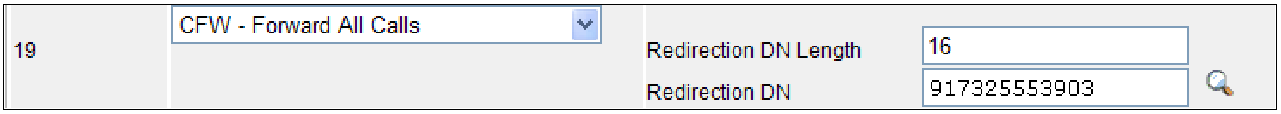

16 MWK - Message Waiting

Message Center DN 2080

☐ Multiple Appearance Redirection Prime(MARP)

5.10.1.2.4 Key 19 - Forward All Calls

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

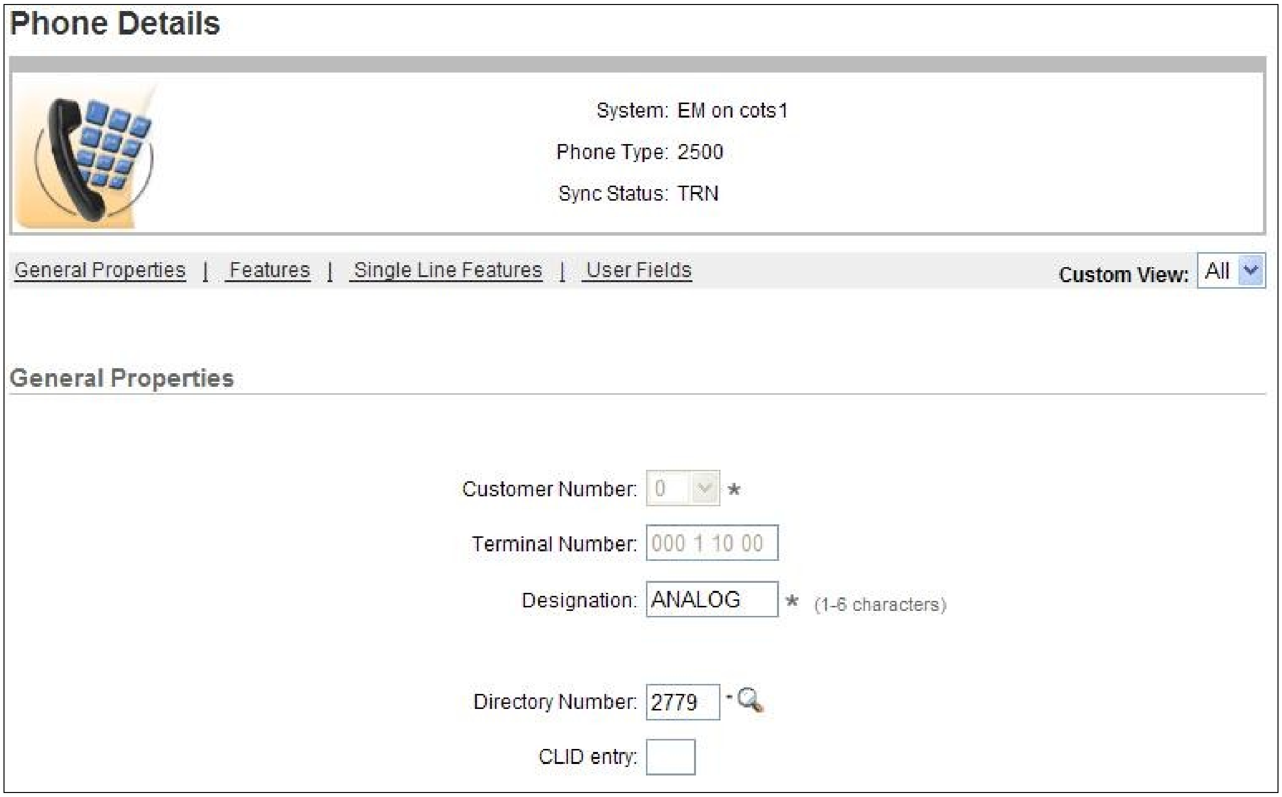

19 CFW - Forward All Calls

Redirection DN Length 16

Redirection DN 917325553903

5.10.2 Analog Fax Line

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


Phone Details
General Properties | Features | Single Line Features | User Fields
Custom View: All
General Properties

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

Customer Number: 0 *
Terminal Number: 000 1 10 00
Designation: ANALOG * (1-6 characters)
Directory Number: 2779 *
CLID entry:

5.11. Changing RFC2833 DTMF Telephone Event Type

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.

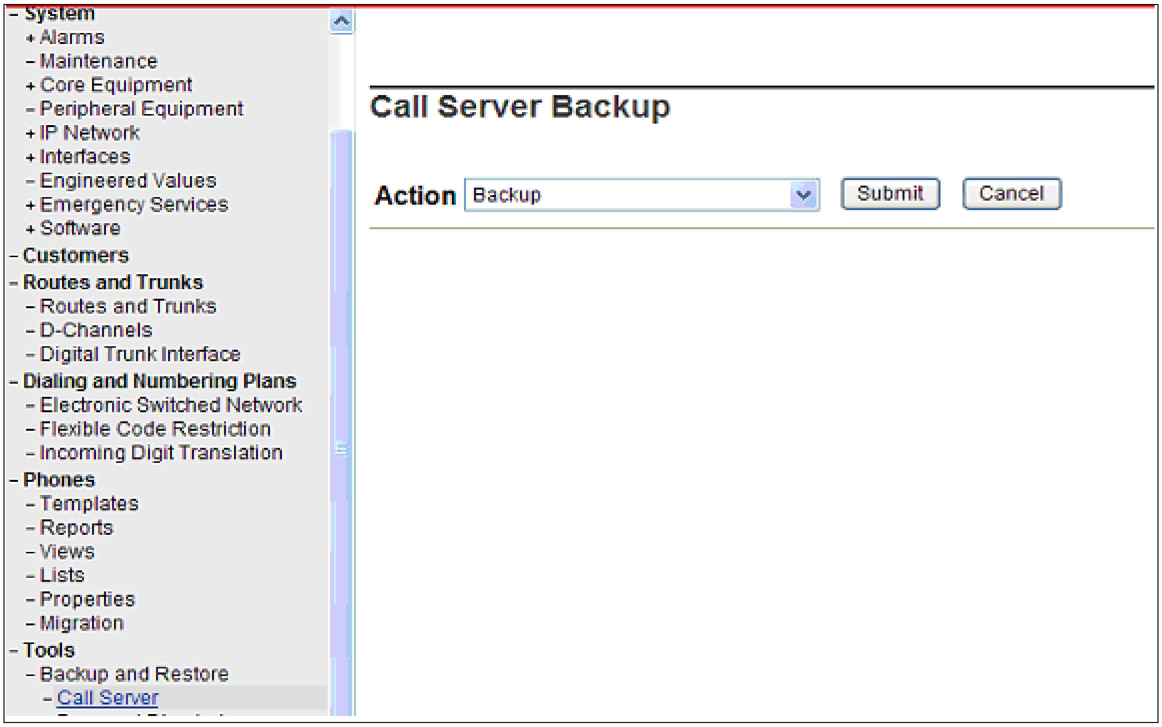
```
pdt>
```

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

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

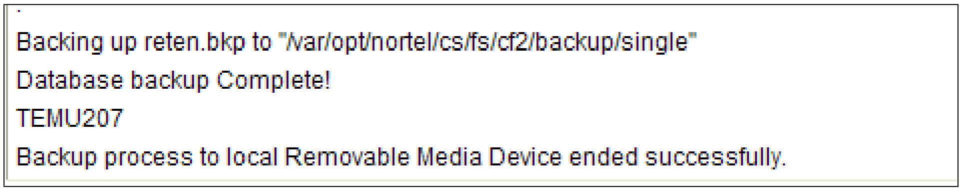
5.12. Configuration Backup

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



Action: Backup

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

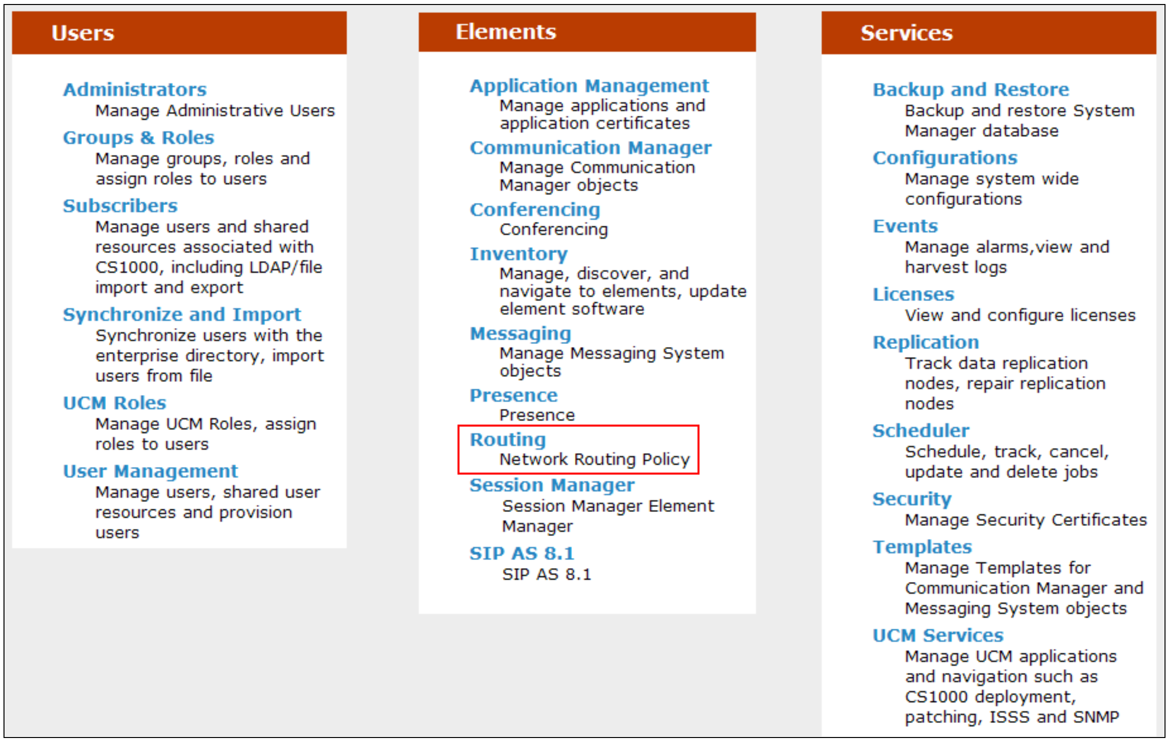
This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Avaya CS1000E and Session Manager, and the SIP trunk between Session Manager and the Avaya Aura® SBC.

The following administration activities will be described:

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

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

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



Users

- **Administrators**
  Manage Administrative Users
- **Groups & Roles**
  Manage groups, roles and assign roles to users
- **Subscribers**
  Manage users and shared resources associated with CS1000, including LDAP/file import and export
- **Synchronize and Import**
  Synchronize users with the enterprise directory, import users from file
- **UCM Roles**
  Manage UCM Roles, assign roles to users
- **User Management**
  Manage users, shared user resources and provision users

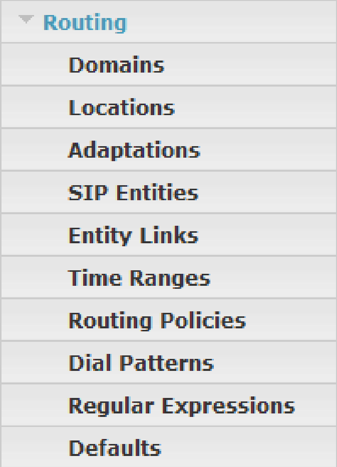
Elements

- **Application Management**
  Manage applications and application certificates
- **Communication Manager**
  Manage Communication Manager objects
- **Conferencing**
  Conferencing
- **Inventory**
  Manage, discover, and navigate to elements, update element software
- **Messaging**
  Manage Messaging System objects
- **Presence**
  Presence
- **Routing**
  Network Routing Policy
- **Session Manager**
  Session Manager Element Manager
- **SIP AS 8.1**
  SIP AS 8.1

Services

- **Backup and Restore**
  Backup and restore System Manager database
- **Configurations**
  Manage system wide configurations
- **Events**
  Manage alarms,view and harvest logs
- **Licenses**
  View and configure licenses
- **Replication**
  Track data replication nodes, repair replication nodes
- **Scheduler**
  Schedule, track, cancel, update and delete jobs
- **Security**
  Manage Security Certificates
- **Templates**
  Manage Templates for Communication Manager and Messaging System objects
- **UCM Services**
  Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

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



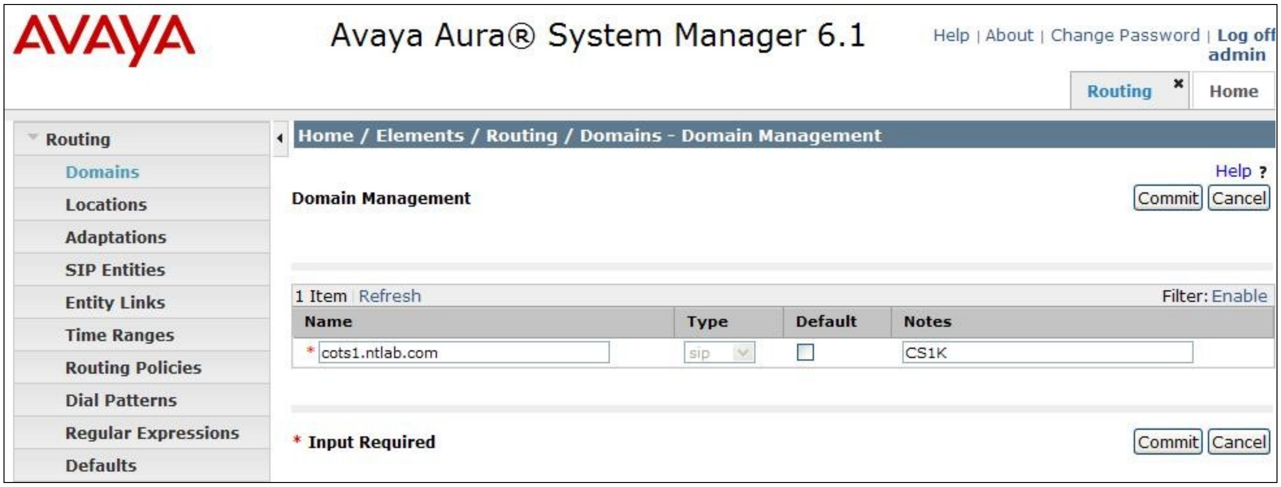
6.1. SIP Domain

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

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

- **Name** Enter the enterprise SIP Domain Name. In the sample screen below, "**cots1.ntlab.com**" is shown.
- **Type** Verify "**SIP**" is selected.

- **Notes** Add a brief description. [Optional]



Domain Management

Name	Type	Default	Notes
* cots1.ntlab.com	sip	☐	CS1K

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**.**

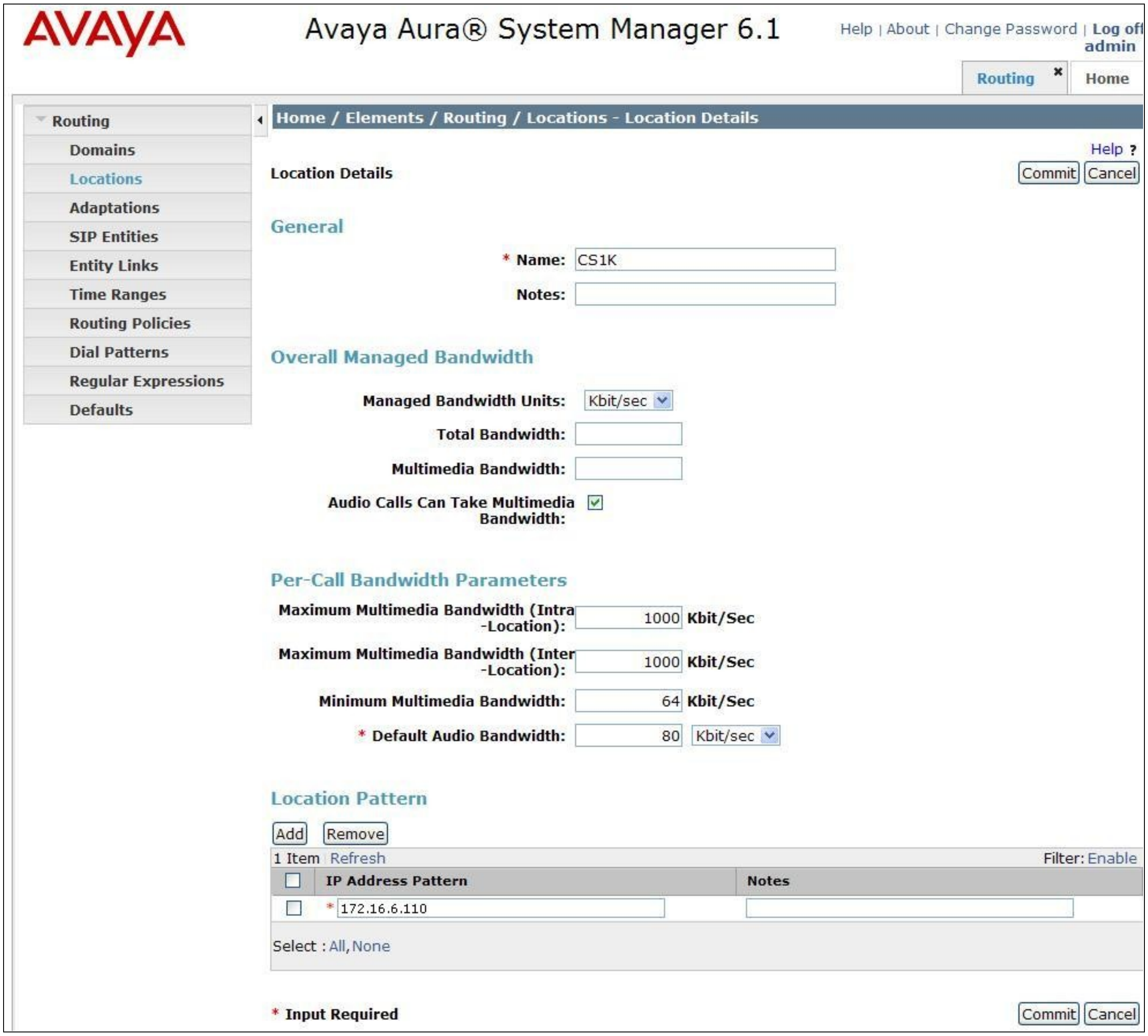
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

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.



Location Details

General

* Name: CS1K

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

☐	IP Address Pattern	Notes
☐	* 172.16.6.110	

* Input Required

6.2.2 Location for the Avaya Session Border Controller

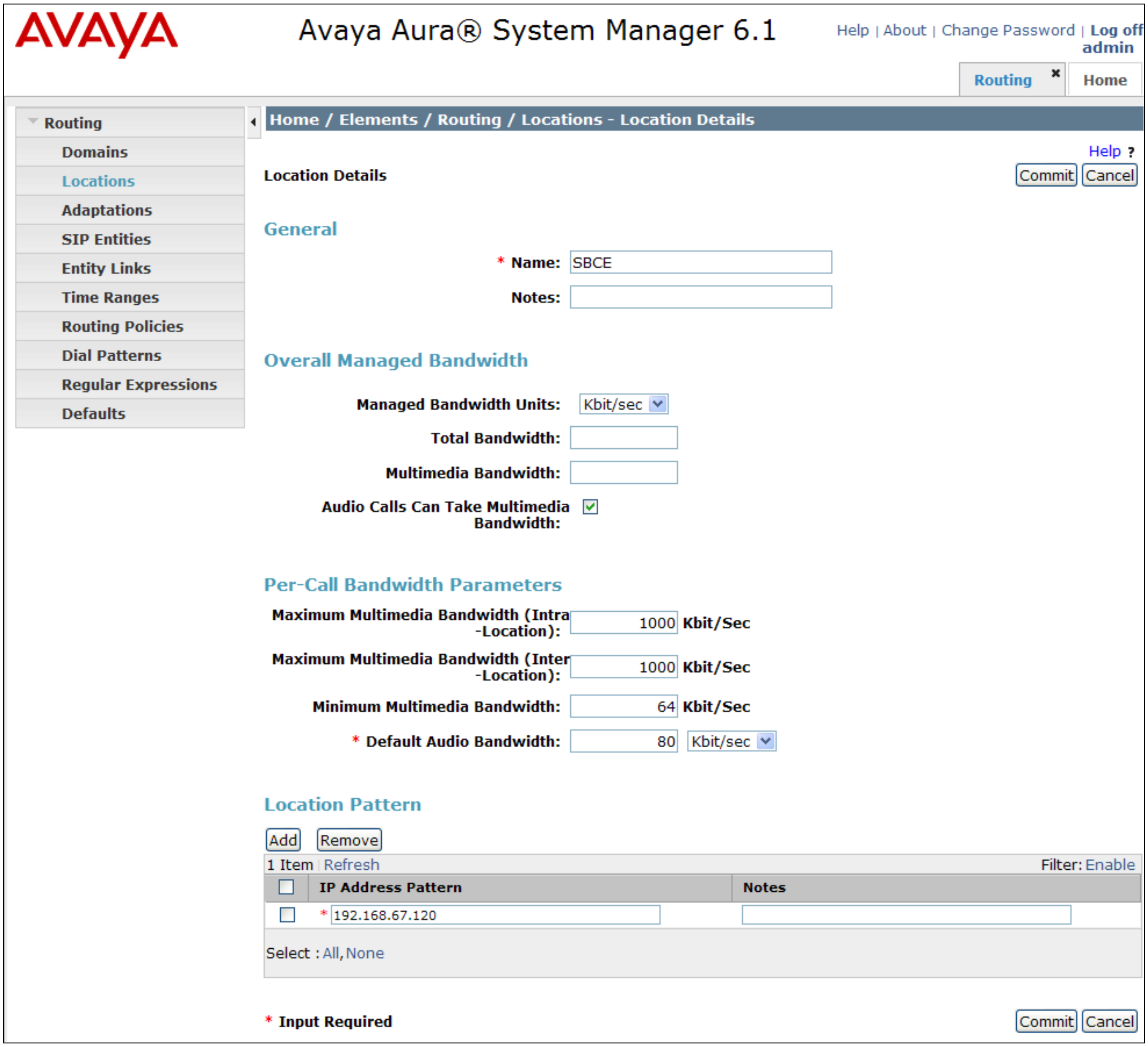
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

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

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

IP Address Pattern	Enter the IP Address or IP Address pattern used to identify the Avaya SBCE location (e.g. **192.168.67.120**).
Notes	Add a brief description. [Optional]

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



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

☐	IP Address Pattern	Notes
☐	* 192.168.67.120	

* Input Required

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 Communication Server to the format used by other Avaya products and endpoints. In the reference configuration the following adaptations was used.

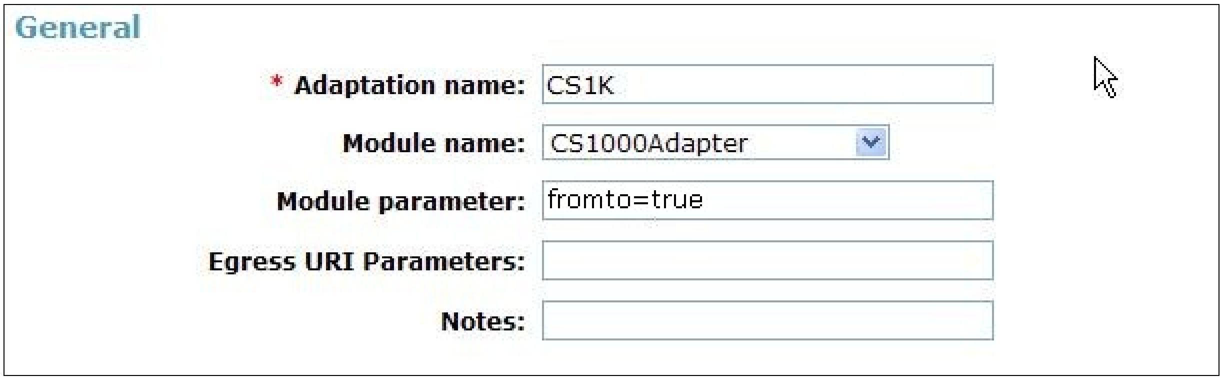
- **DiversionTypeAdapter** – This adaptation is used to convert History-Info headers sent by Avaya CS1000E in certain outbound calls to AT&T (which are not supported by the AT&T IP Flexible Reach service), to Diversion Headers. This is required for call scenarios such as Call Forwarding.
- **CS1000Adapter** – 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 Avaya CS1000E 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., "CS1000")
- **Module Name:** Select "**CS1000Adapter**" from drop-down menu (or add an adapter with name "CS1000Adapter" if not previously defined)
- **Module Parameter:** Enter **fromto=true** (Note – this parameter is set so that destination user information is copied from the R-URI into the To header for inbound calls to Call Pilot).


General

* Adaptation name:	CS1K
Module name:	CS1000Adapter
Module parameter:	fromto=true
Egress URI Parameters:	
Notes:	

Step 2 – In the **Digit Conversion for Outgoing Calls from SM** section, click **Add** to configure entries for calls from AT&T.

Note that incoming AT&T calls to Avaya CS1000E stations have the inbound NDIS digits converted to their associated local extensions in the Avaya CS1000E **Incoming Digit Translation** table (e.g., AT&T DNIS 7325554383 is converted to local extension 4095, see **Section 5.5**), so those digit conversions are not needed here.

However, for direct PSTN/AT&T access to the integrated Call Pilot messaging system, the **fromto=true** Module Parameter needs to be applied to insert the Call Pilot local access extension (2090) into the To header.

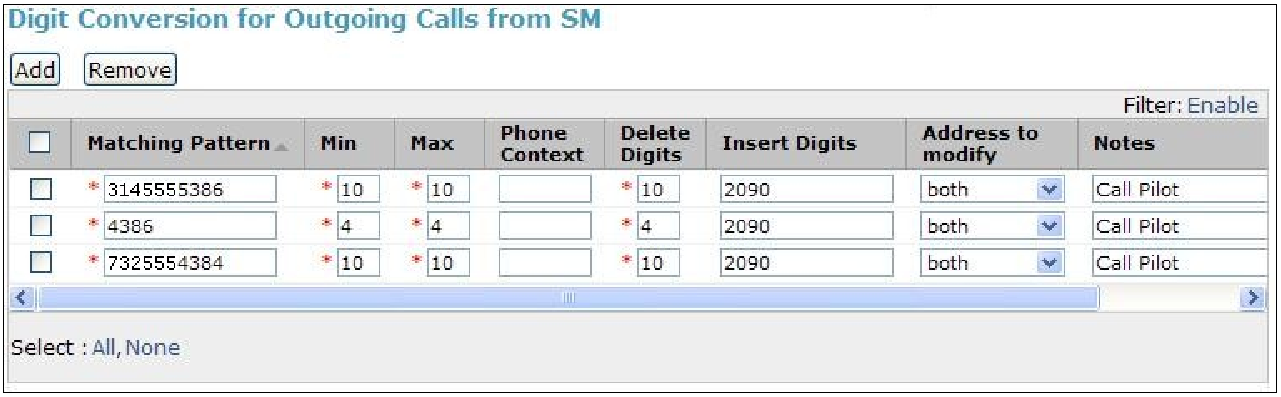
The text below and the screen example that follows explain how to use Session Manager to convert between inbound AT&T IP Flexible Reach DNIS numbers and the Avaya CS1000E Call Pilot extension (2090).

Matching Pattern	Enter AT&T IP Flexible Reach DIDs (e.g. **7325554384**).
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. **2090**).

- **Address to modify** Select **"both".**

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

Step 3 - Click **Commit.**



Digit Conversion for Outgoing Calls from SM

☐	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 3145555386	* 10	* 10		* 10	2090	both	Call Pilot
☐	* 4386	* 4	* 4		* 4	2090	both	Call Pilot
☐	* 7325554384	* 10	* 10		* 10	2090	both	Call Pilot

Note – Avaya CS1000E is used to convert local extensions to AT&T DIDs for outbound calls (see **Section 5.9.1**). Therefore no entries are required in the **Digit Conversion for Incoming Calls to SM** section of this form (calls to AT&T from Avaya CS1000E).

6.3.2 Adaptation for the Avaya CS1000E to Avaya SBCE Entity

The message body of an INVITE message sent from the 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 Flexible Reach service for Call Forward scenarios. Note that the Avaya SBCE is used to remove and/or alter additional Avaya CS1000E SIP headers (see **Section 7.4.9**).

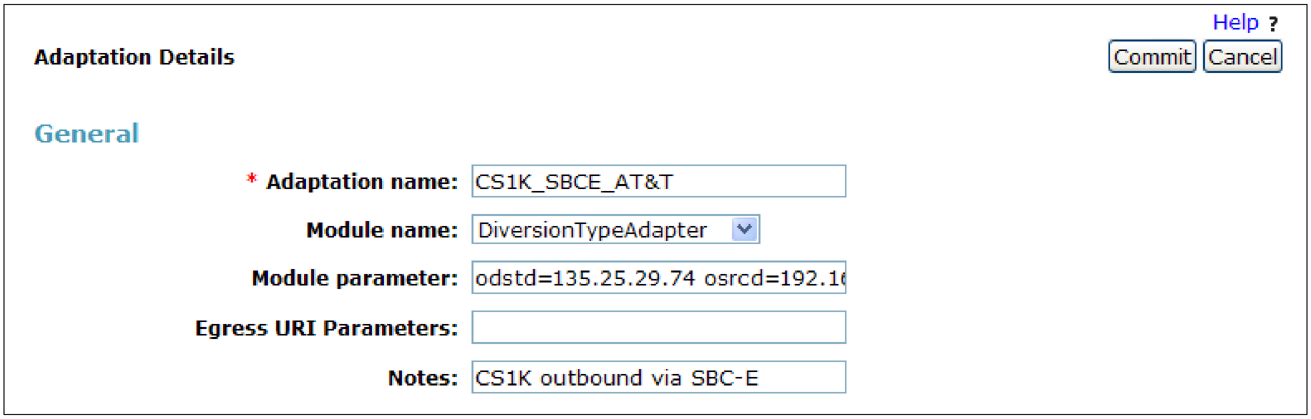
Step 1 - Select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **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 Flexible Reach border element >" (e.g. **odstd=135.25.29.74**).
  - Enter "**osrcd=**< IP address of the public interface of the Avaya SBCE >" (e.g. **osrcd=192.168.64.130**).
  - Enter "**MIME=no**" to remove additional MIME Media Type headers that the 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.



Adaptation Details

General

* Adaptation name: CS1K_SBCE_AT&T

Module name: DiversionTypeAdapter

Module parameter: odstd=135.25.29.74 osrcd=192.16

Egress URI Parameters:

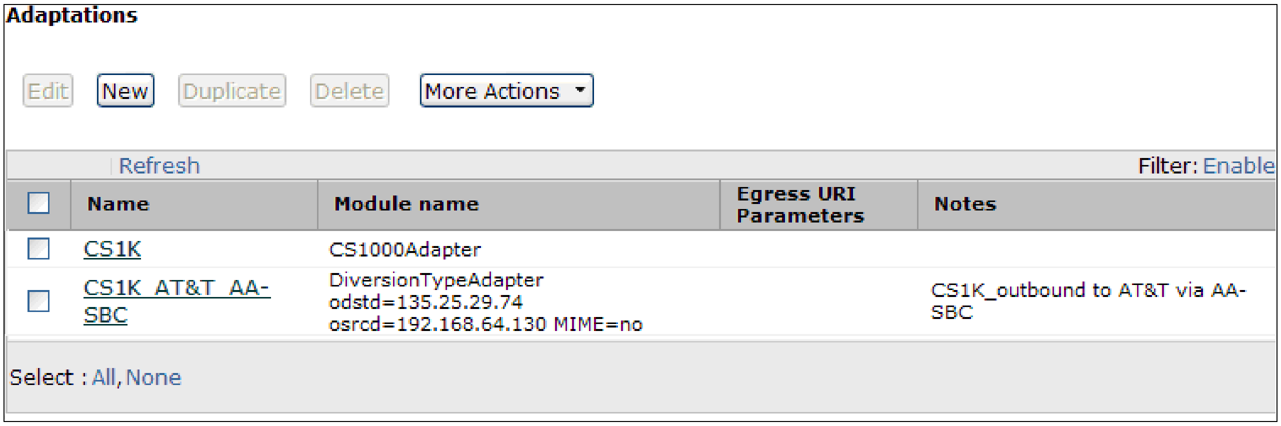
Notes: CS1K outbound via SBC-E

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

Step 2 - Click **Commit.**

6.3.3 List of Adaptations

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



Adaptations

☐	Name	Module name	Egress URI Parameters	Notes
☐	CS1K	CS1000Adapter		
☐	CS1K_AT&T_AA-SBC	DiversionTypeAdapter odstd=135.25.29.74 osrcd=192.168.64.130 MIME=no		CS1K_outbound to AT&T via AA-SBC

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**.**

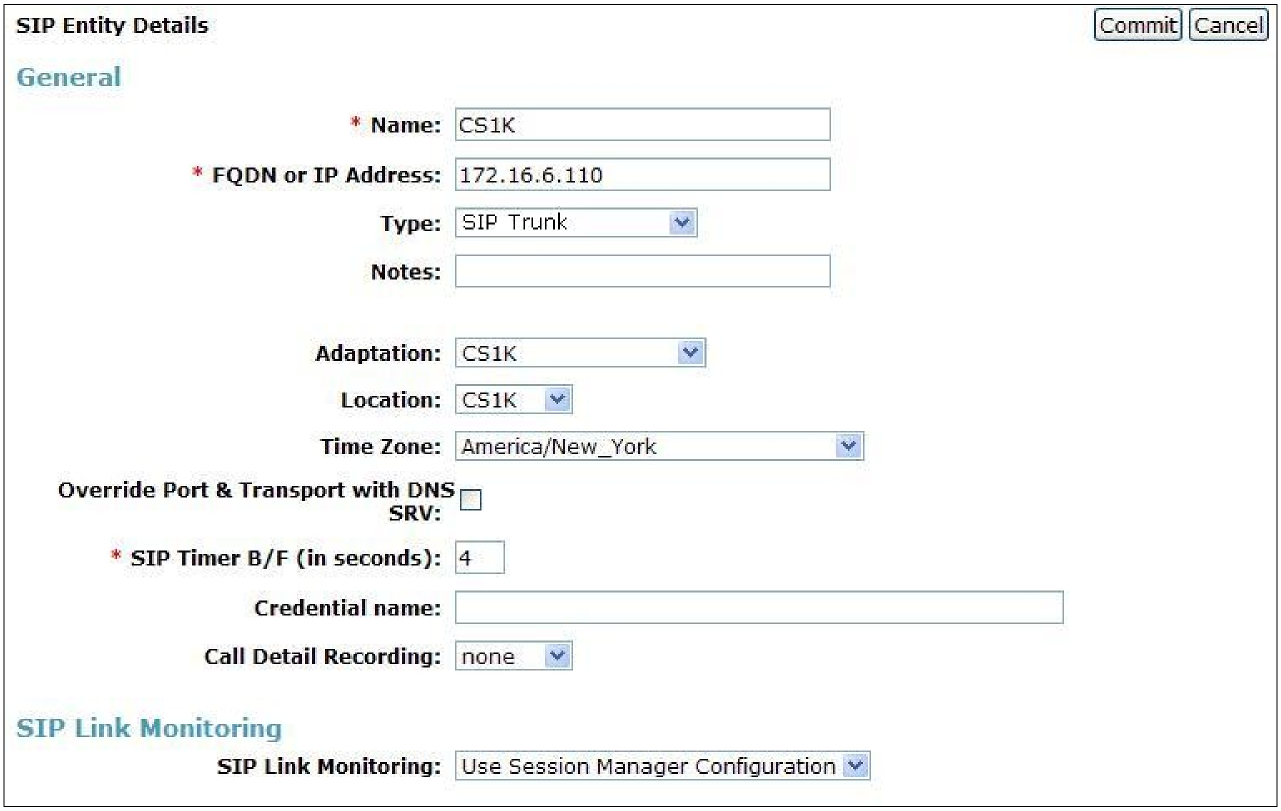
- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter the TLAN IP address of the Avaya CS1000E Node.
- **Type:** Select "**SIP Trunk**"
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined in **Section 6.3.1**.
- **Location:**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



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 the Avaya SBCE

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

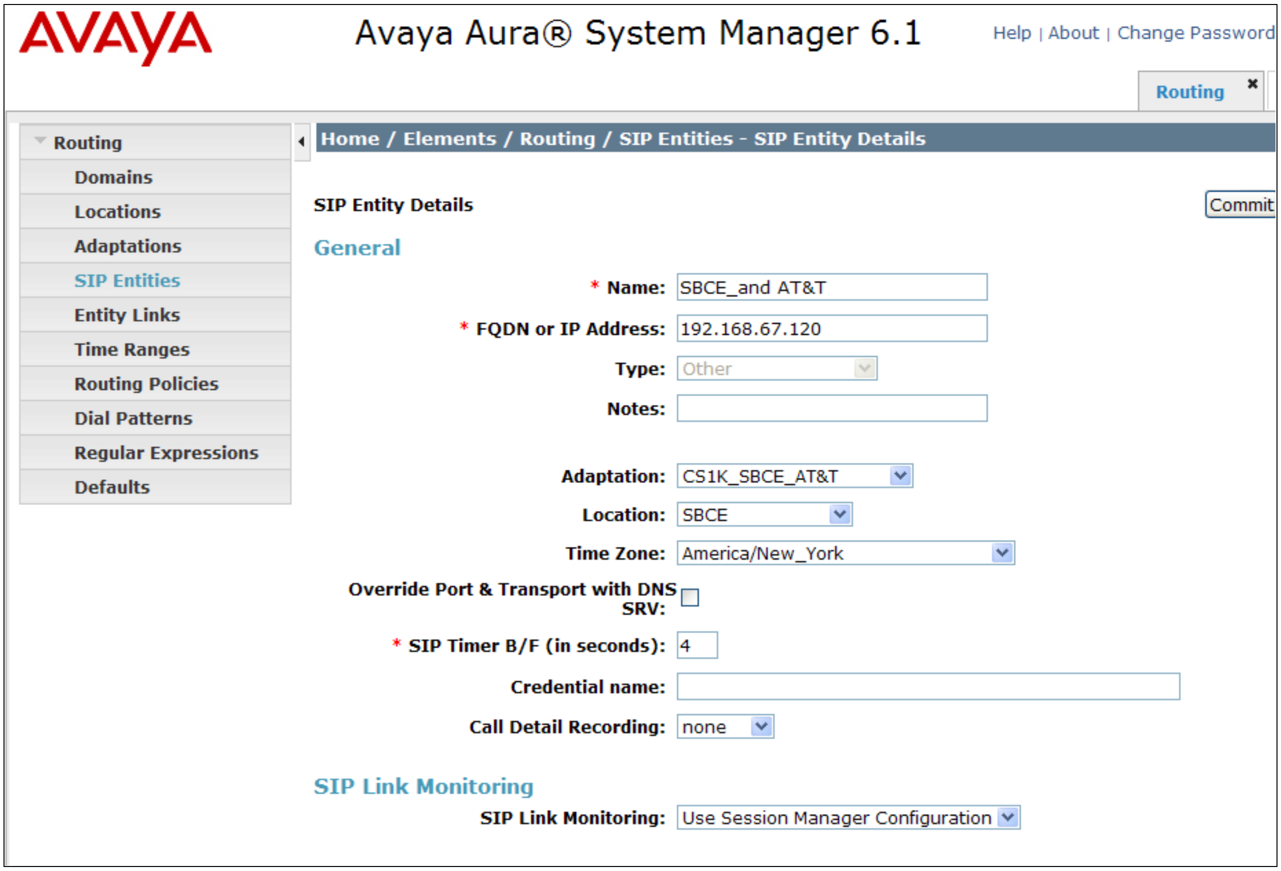
Step 2 - Click **New** (not shown**)**. In the **General** section, enter the following values and use default values for remaining fields**.**

- **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 Avaya SBCE in the sample configuration.



SIP Entity Details

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

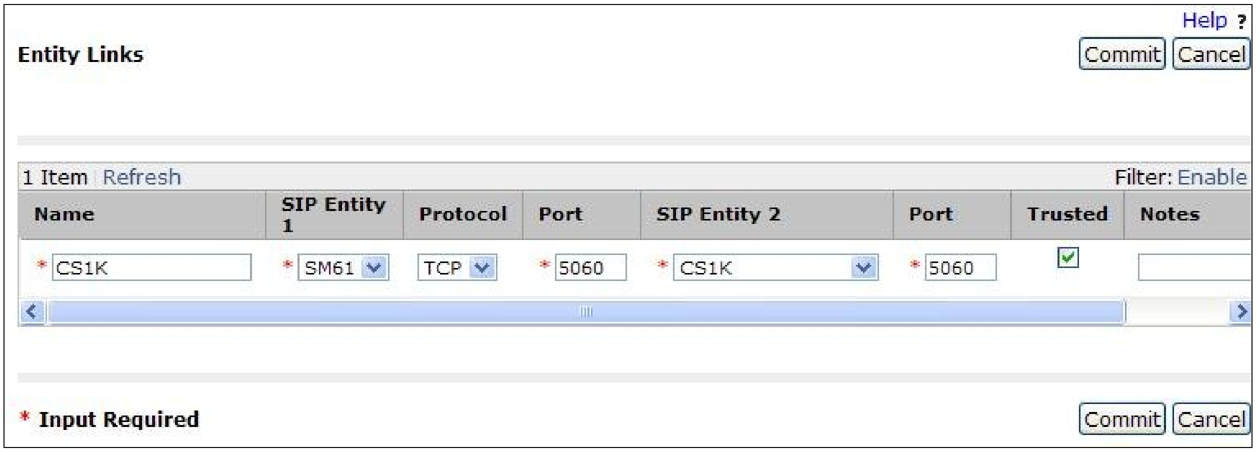
Step 1 - Select **Entity Links** from the left navigation menu.

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	☑	

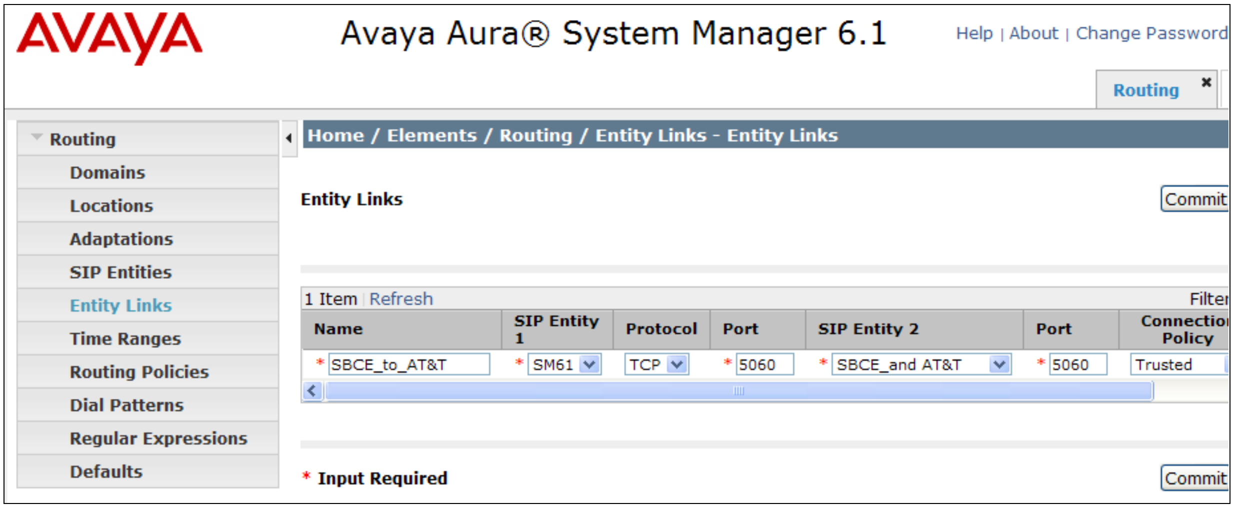
6.5.2 Entity Link to the Avaya SBCE

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 the 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.



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, or Avaya SBCE.

6.6.1 Routing Policy to the 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]

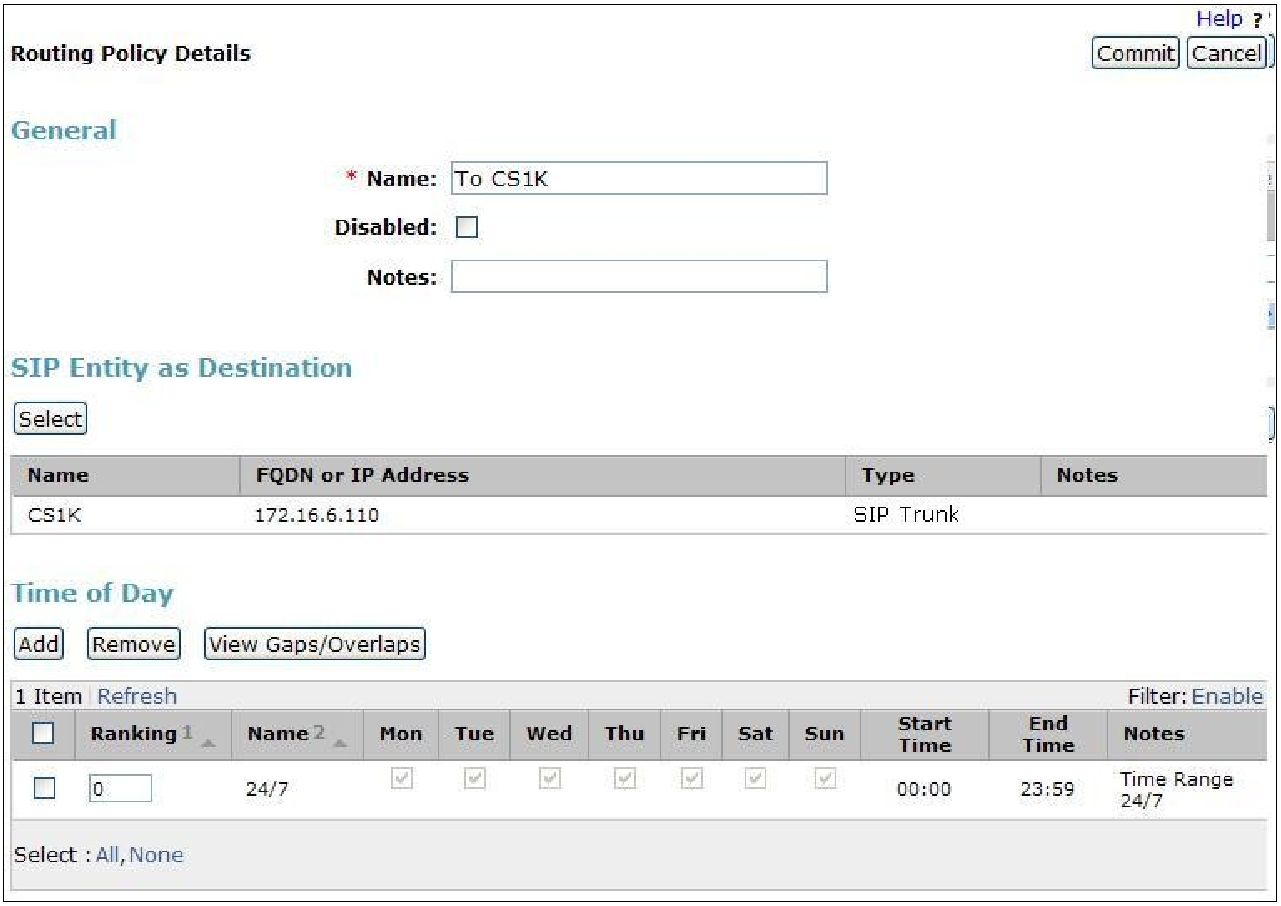
Step 2 - In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

- 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

General

* **Name:** To CS1K

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CS1K	172.16.6.110	SIP Trunk	

Time of Day

1 Item | Refresh — Filter: Enable

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

6.6.2 Routing Policy to the Avaya SBCE

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]

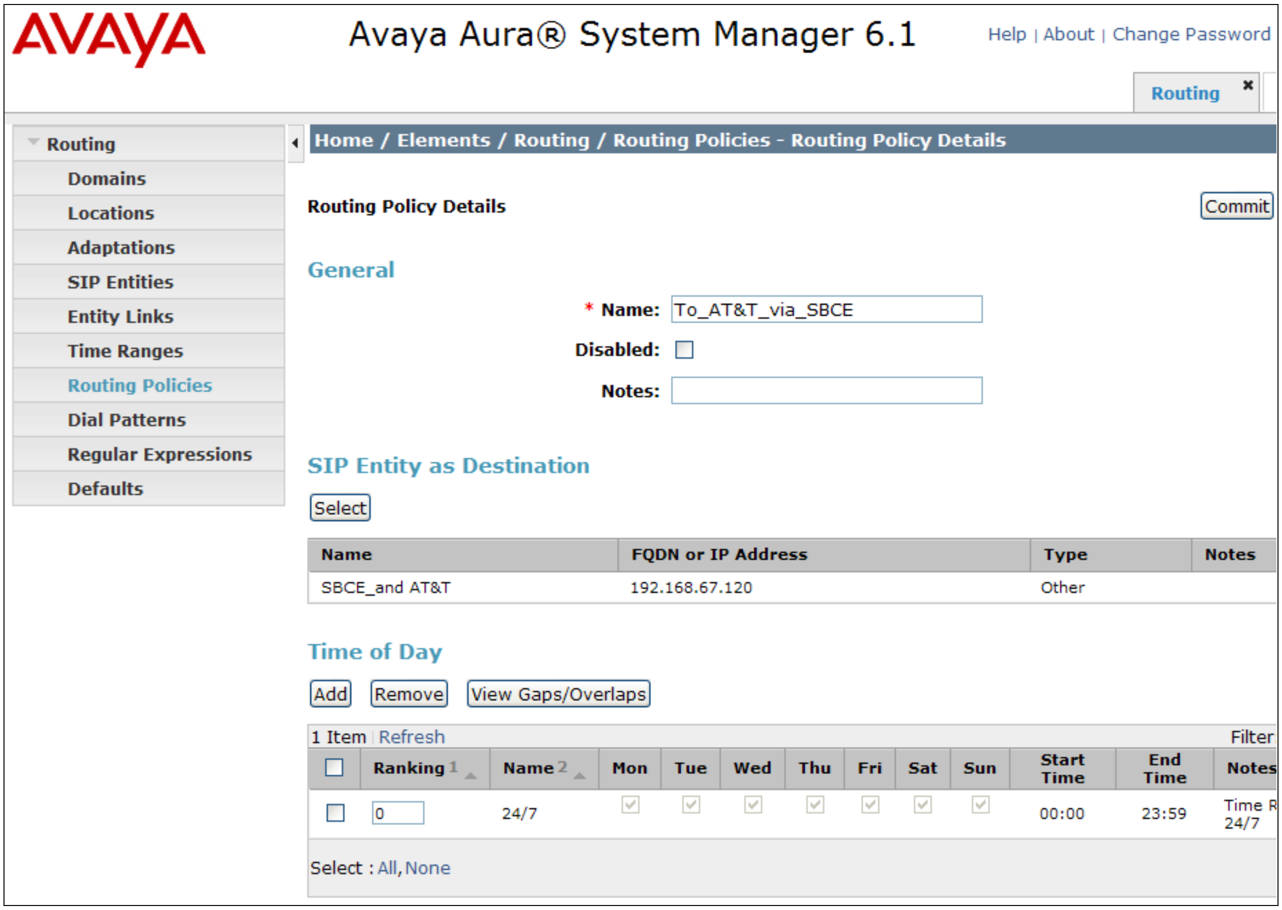
Step 2 - In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown).

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

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

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

The following screen shows the Routing Policy for Avaya SBCE.



Routing Policy Details

General

* **Name:** To_AT&T_via_SBCE

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBCE_and AT&T	192.168.67.120	Other	

Time of Day

☐	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time R 24/7

6.7. Dial Patterns

Dial patterns are used to route calls to the appropriate routing policies, and ultimately to the appropriate SIP Entities. Dial patterns will be configured to route outbound calls from Avaya CS1000E users to the PSTN via the AT&T IP Flexible Reach service. Other dial patterns will be configured to route inbound calls from the AT&T IP Flexible Reach service to 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 Request-URIs are the numbers to be defined here in the **Pattern** fields.

6.7.1 Inbound AT&T calls to Avaya CS1000E Users

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

- **Pattern:** Enter dial pattern for calls to the 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.

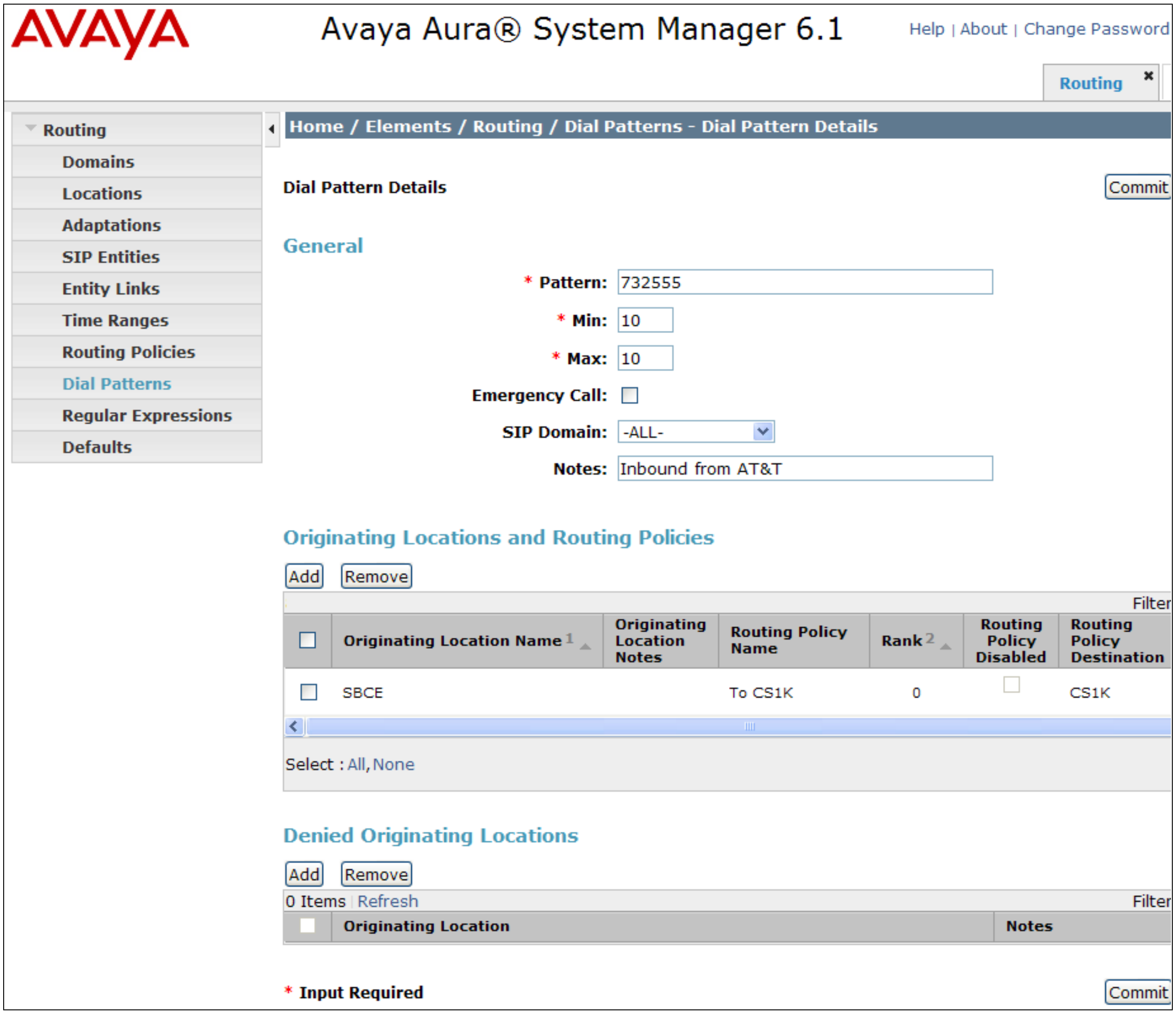
- **Notes:** Enter a brief description. [Optional]

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.



Dial Pattern Details

General

* Pattern: 732555

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Inbound from AT&T

Originating Locations and Routing Policies

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination
☐	SBCE		To CS1K	0	☐	CS1K

Select : All, None

Denied Originating Locations

0 Items | Refresh

☐	Originating Location	Notes

* Input Required

6.7.2 Outbound Calls to AT&T

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

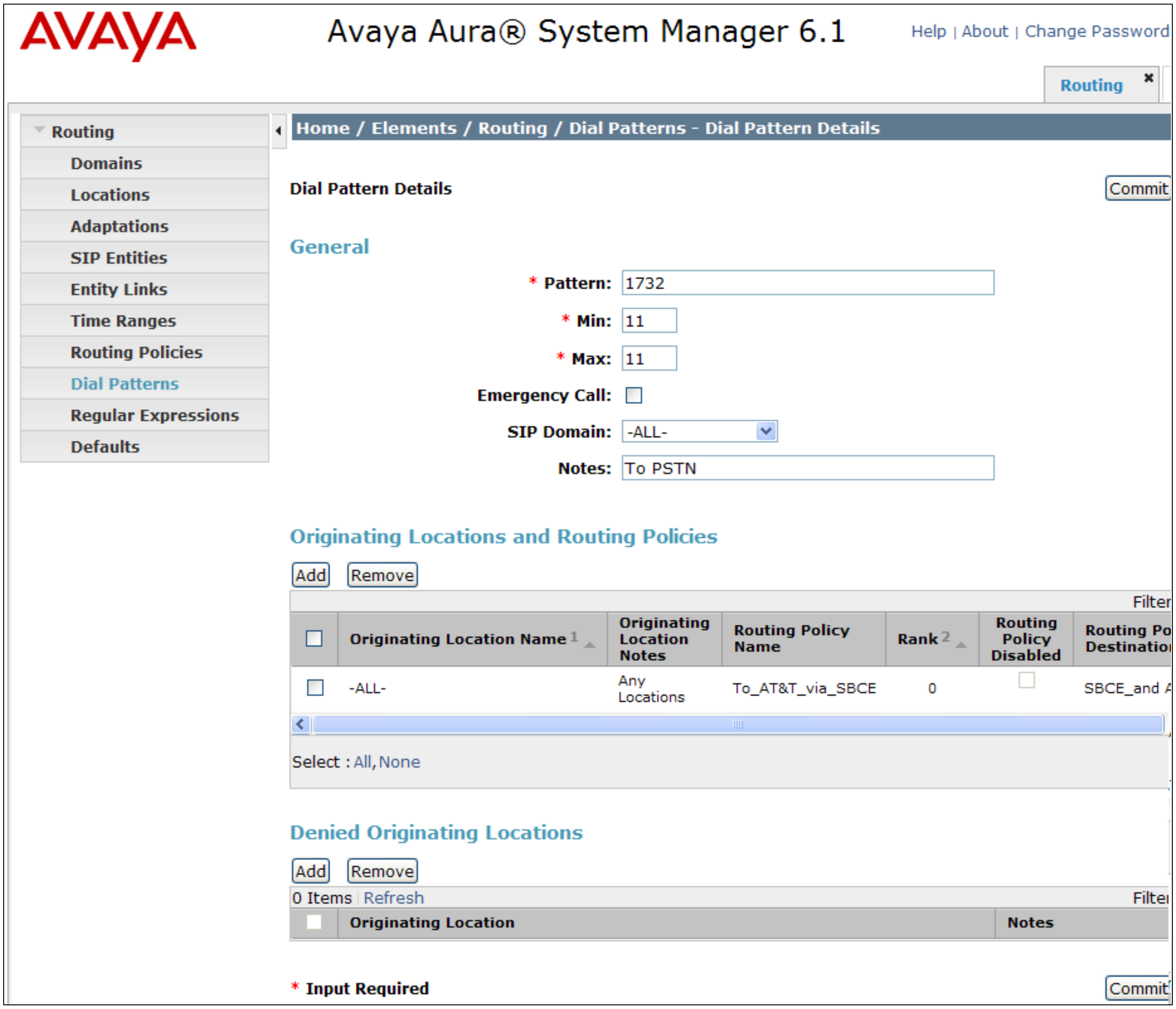
- **Pattern:** Enter dial pattern for calls destined to PSTN via the AT&T network (e.g. 1732xxxxxxx).
- **Min:** Enter the minimum number of digits (e.g. 11).
- **Max:** Enter the maximum number of digits (e.g. 11).
- **SIP Domain:** Select a SIP Domain from drop-down menu or select **"All"** if Session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

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

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

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

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



Dial Pattern Details

General

* **Pattern:**	1732
* **Min:**	11
* **Max:**	11
Emergency Call:	☐
SIP Domain:	-ALL-
Notes:	To PSTN

Originating Locations and Routing Policies

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Po Destinatio
☐	-ALL-	Any Locations	To_AT&T_via_SBCE	0	☐	SBCE_and A

Select : All, None

Denied Originating Locations

0 Items | Refresh

☐	Originating Location	Notes

* **Input Required**

7. Configure Avaya Session Border Controller for Enterprise

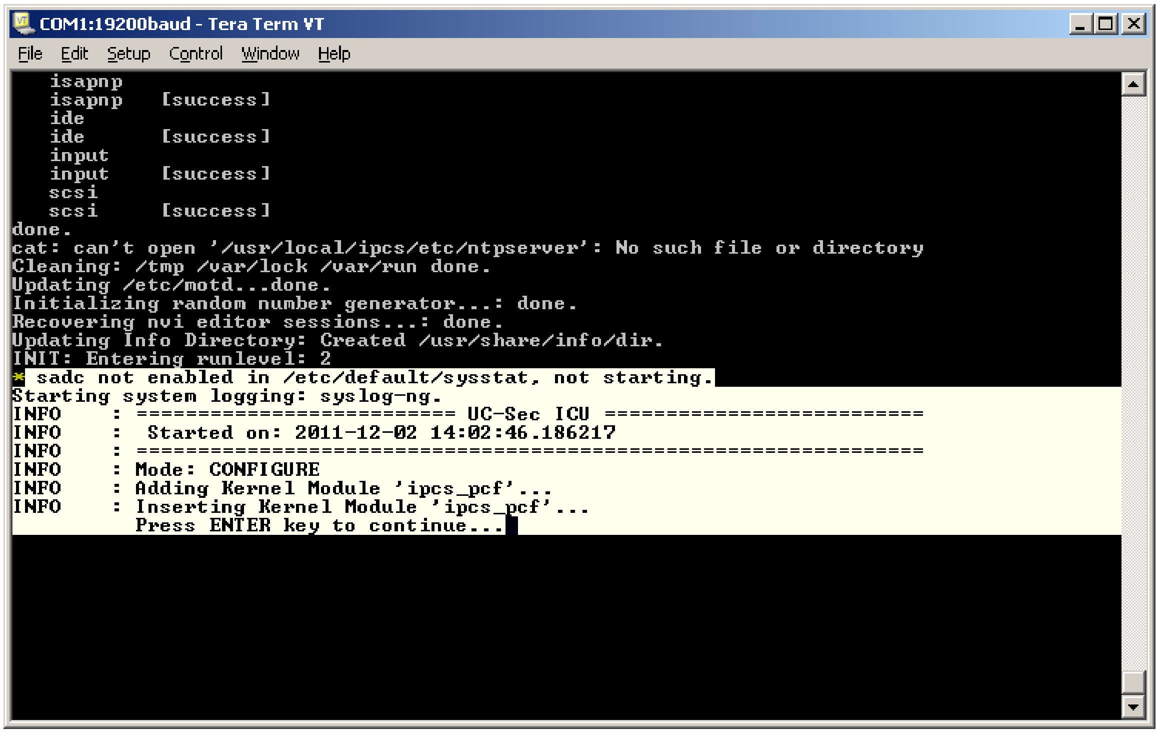
7.1. Initial Provisioning

The following sections describe the provisioning of Avaya SBCE.

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

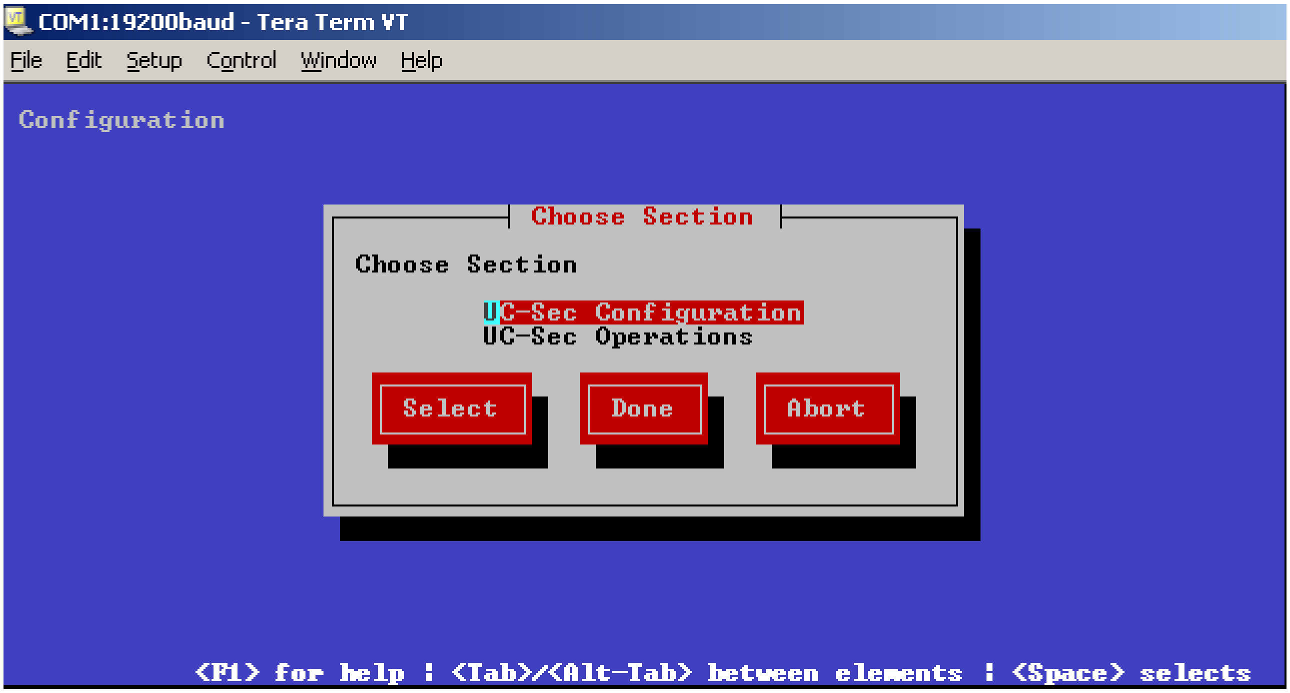
Avaya SBCE was configured via a serial console port connection and via an IP connection once the basic system provisioning was completed. The platform was configured as a single **EMS + UC-SEC** configuration. The following are the steps for provisioning the basic configuration:

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.
4. 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

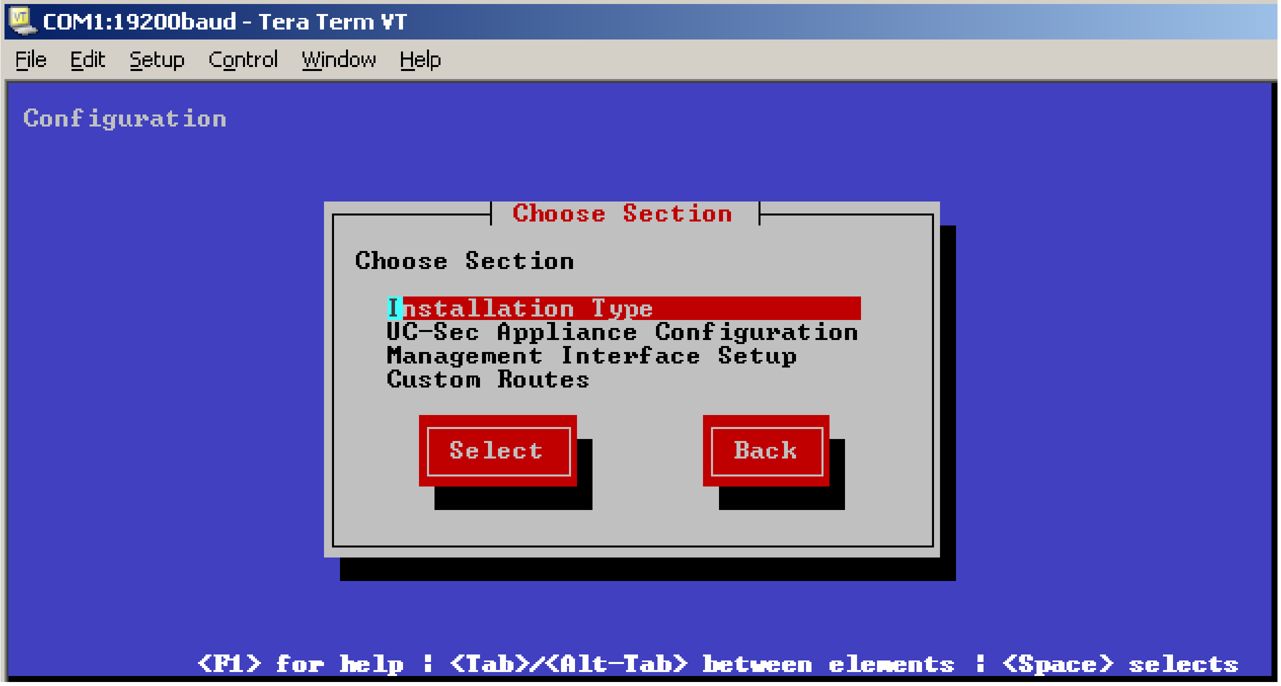
```
    isapnp
    isapnp    [success]
    ide
    ide       [success]
    input
    input     [success]
    scsi
    scsi      [success]
done.
cat: can't open '/usr/local/ipcs/etc/ntpserver': No such file or directory
Cleaning: /tmp /var/lock /var/run done.
Updating /etc/motd...done.
Initializing random number generator...: done.
Recovering nvi editor sessions...: done.
Updating Info Directory: Created /usr/share/info/dir.
INIT: Entering runlevel: 2
* sadc 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...
```

3. A menu will appear. Select **UC Sec Configuration**



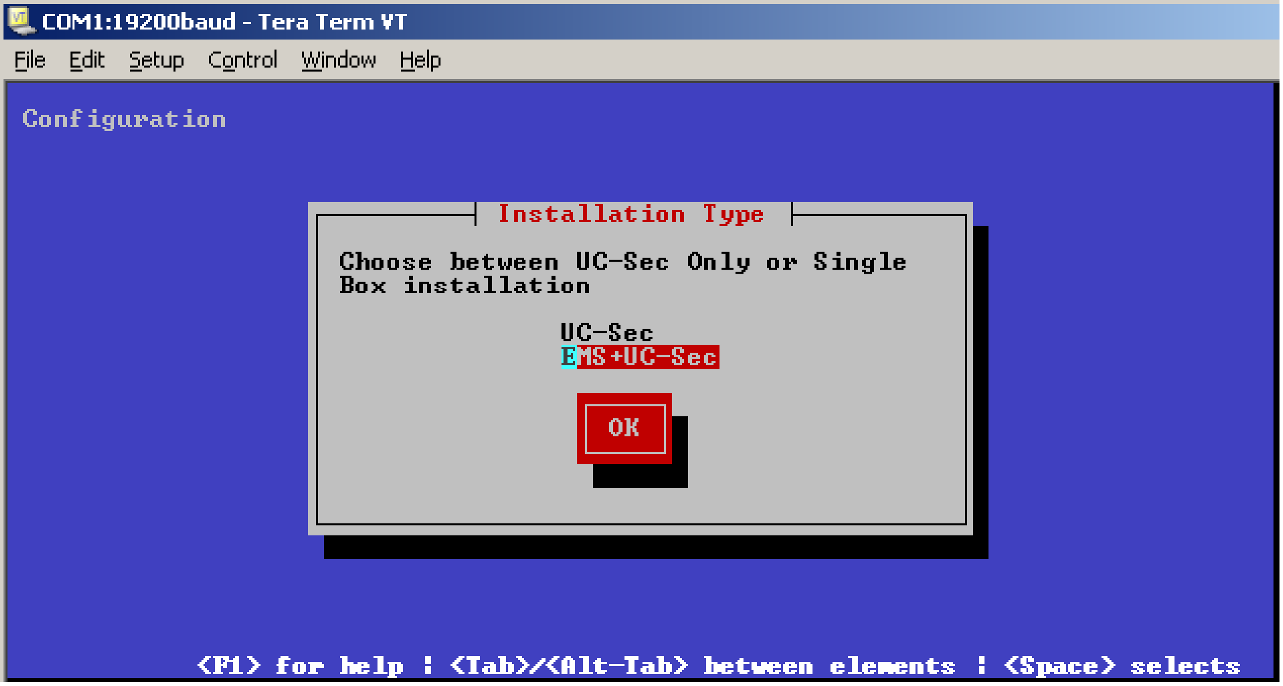
COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Choose Section
Choose Section
UC-Sec Configuration
UC-Sec Operations
Select
Done
Abort
<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects

7. Select **Installation Type**



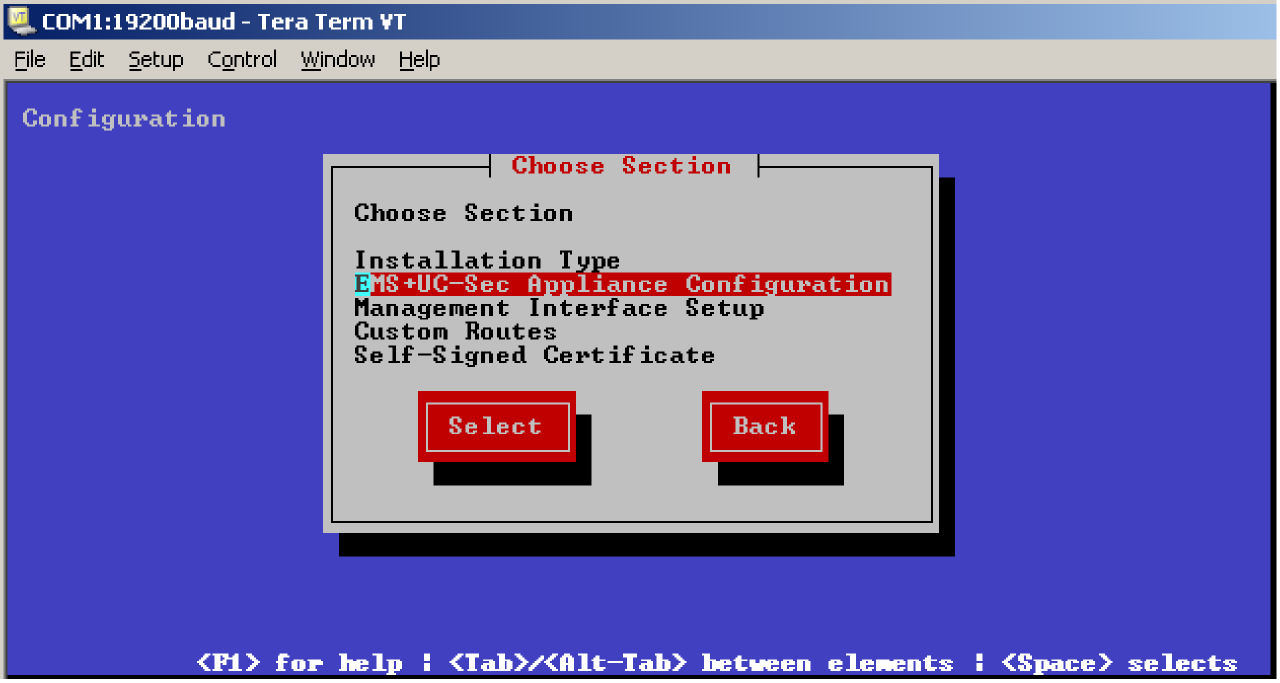
COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Choose Section
Choose Section
Installation Type
UC-Sec Appliance Configuration
Management Interface Setup
Custom Routes
Select
Back
<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects

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


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Installation Type
UC-Sec
EMS+UC-Sec
OK
<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects

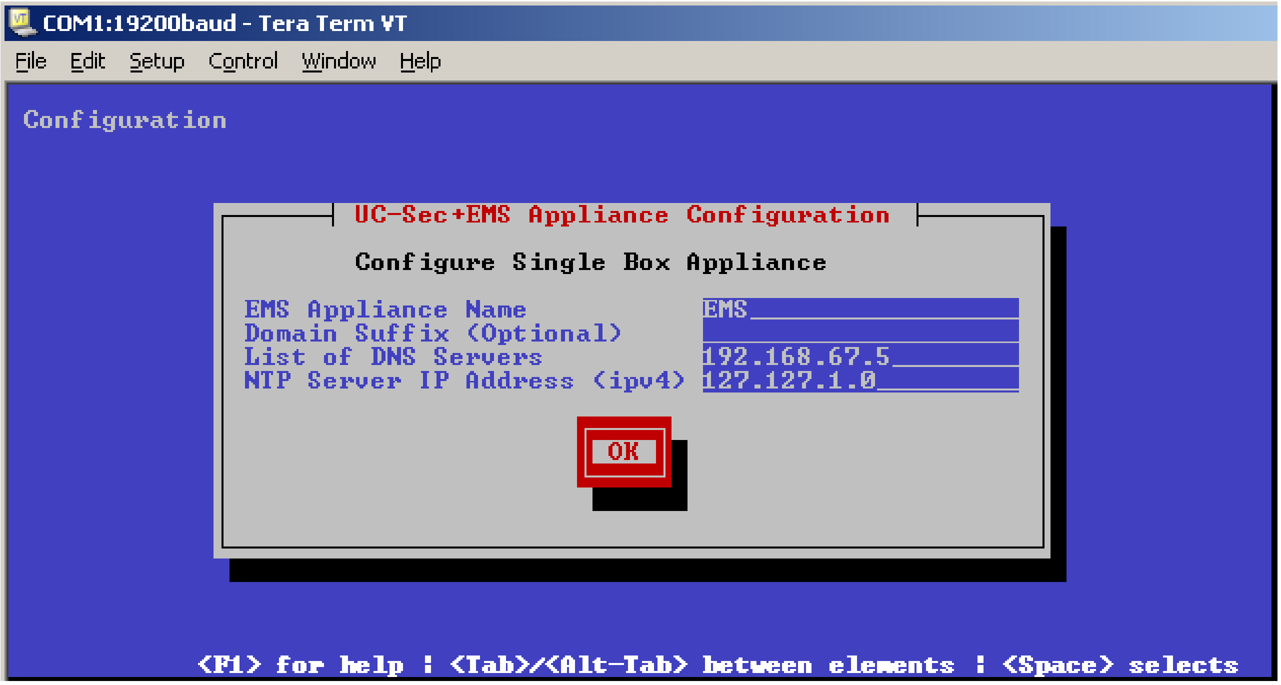
Choose between UC-Sec Only or Single Box installation

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


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Choose Section
Installation Type
EMS+UC-Sec Appliance Configuration
Management Interface Setup
Custom Routes
Self-Signed Certificate
Select
Back
<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects

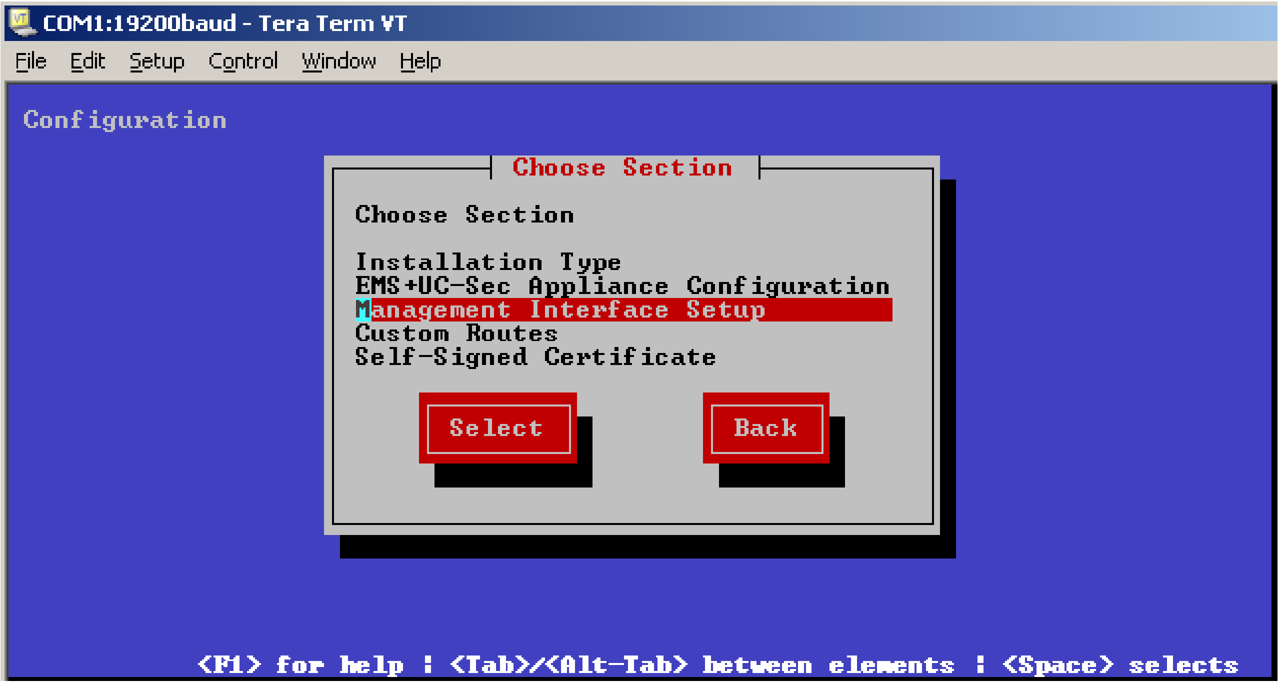
Choose Section

10. Enter or leave Name as default (e.g., **EMS**). Enter IP address of DNS if applicable. If NTP is not used, leave default value. Press OK


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

```
Configuration

            UC-Sec+EMS Appliance Configuration

                 Configure Single Box Appliance

      EMS Appliance Name              EMS
      Domain Suffix (Optional)
      List of DNS Servers             192.168.67.5
      NTP Server IP Address (ipv4)    127.127.1.0

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

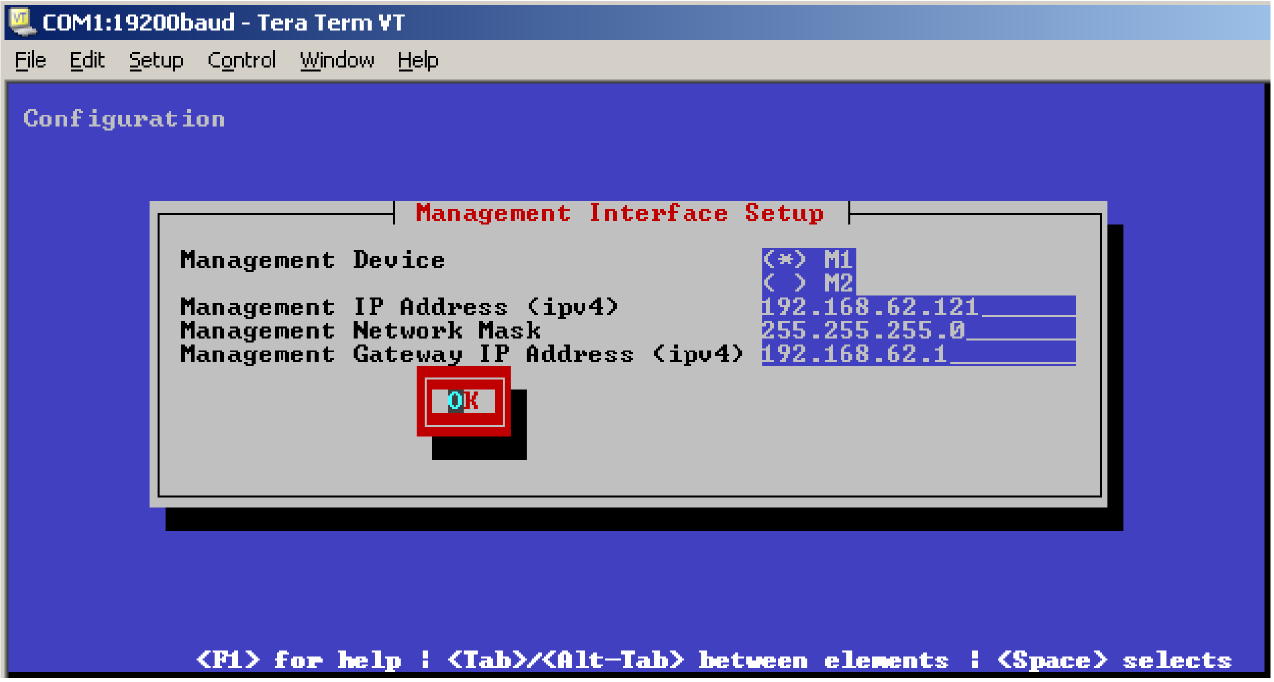
11. Select **Management Interface Setup**.


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

```
Configuration
                    Choose Section

          Choose Section

          Installation Type
          EMS+UC-Sec Appliance Configuration
          Management Interface Setup
          Custom Routes
          Self-Signed Certificate

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

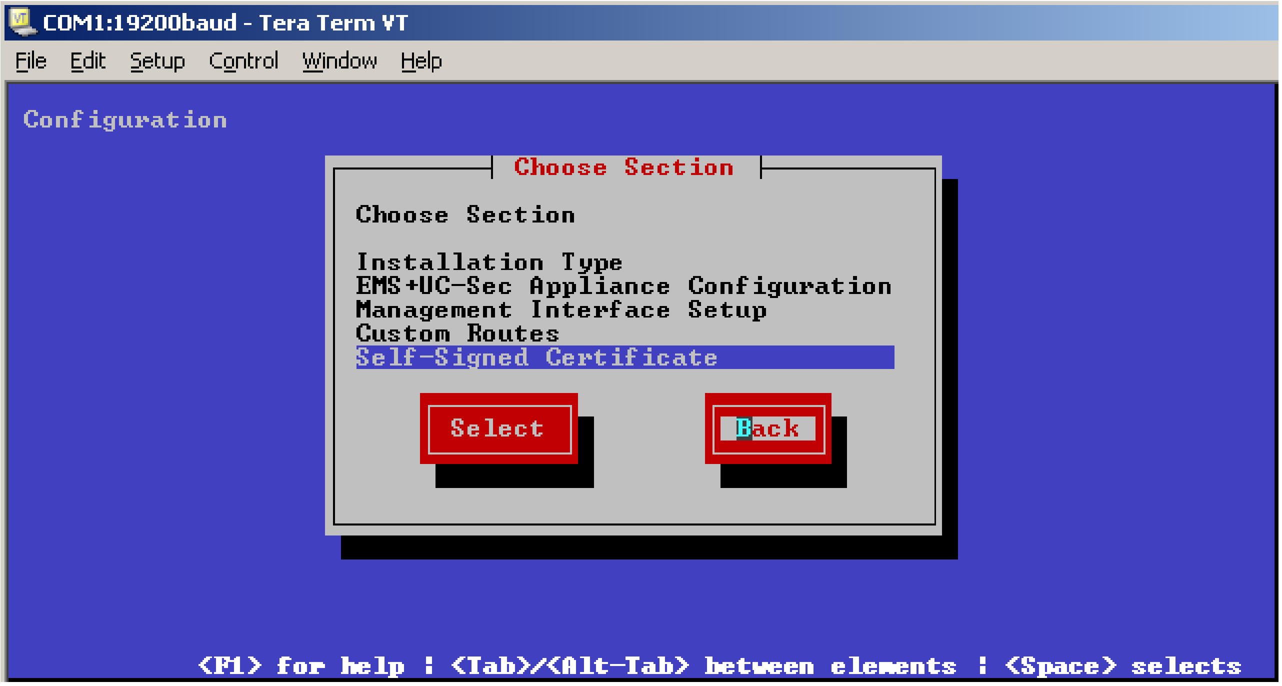
12. Select the **M1** interface. Enter the IP address you want for management (e.g. **192.168.62.121**). Enter mask and gateway. Select OK

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


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Management Interface Setup
OK
<F1> for help ¦ <Tab>/<Alt-Tab> between elements ¦ <Space> selects

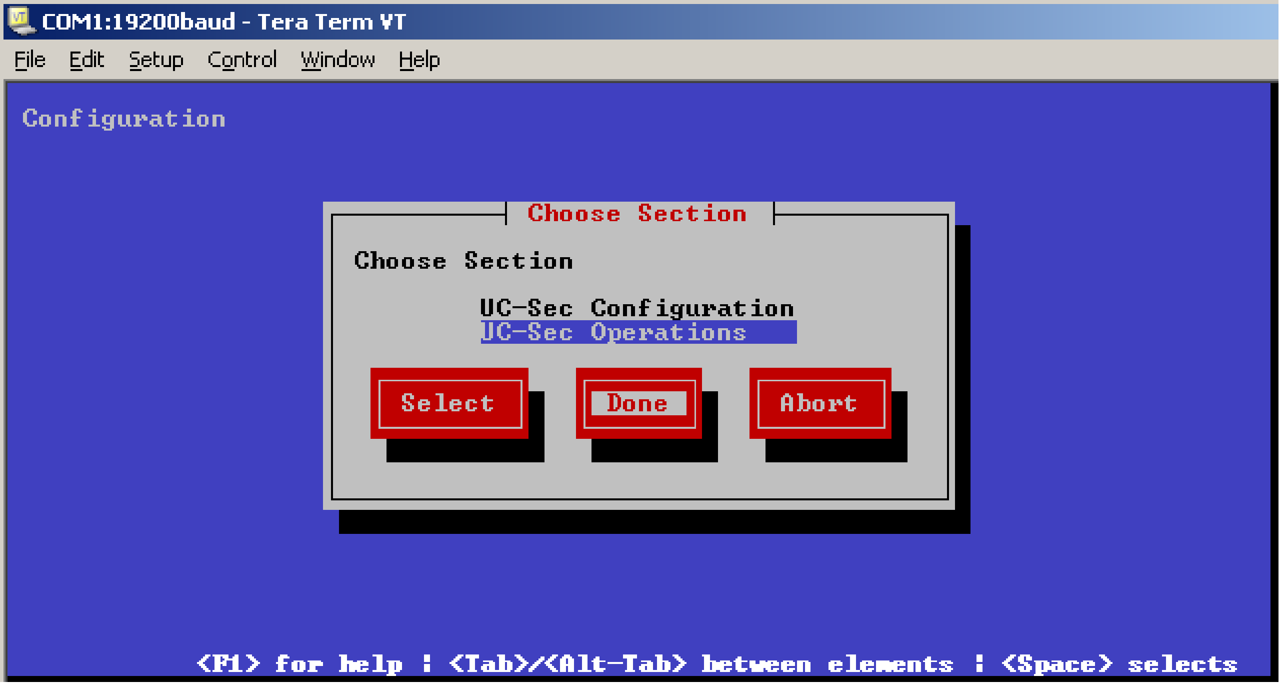
```
Management Device                          (*) M1
                                           ( ) M2
Management IP Address (ipv4)               192.168.62.121
Management Network Mask                    255.255.255.0
Management Gateway IP Address (ipv4)       192.168.62.1
```

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


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Choose Section
Select
Back
<F1> for help ¦ <Tab>/<Alt-Tab> between elements ¦ <Space> selects

```
Choose Section

Installation Type
EMS+UC-Sec Appliance Configuration
Management Interface Setup
Custom Routes
Self-Signed Certificate
```

14. Select **Done**. Avaya SBCE will reboot.

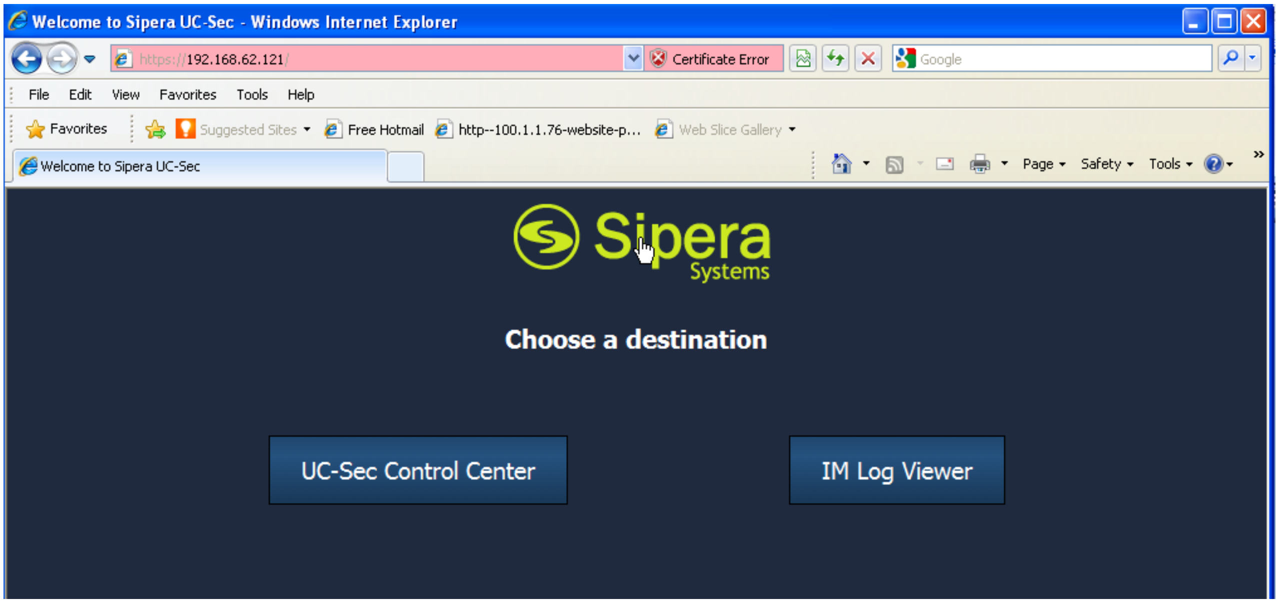

COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Choose Section
Choose Section
UC-Sec Configuration
UC-Sec Operations
Select
Done
Abort
<F1> for help ¦ <Tab>/<Alt-Tab> between elements ¦ <Space> selects

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

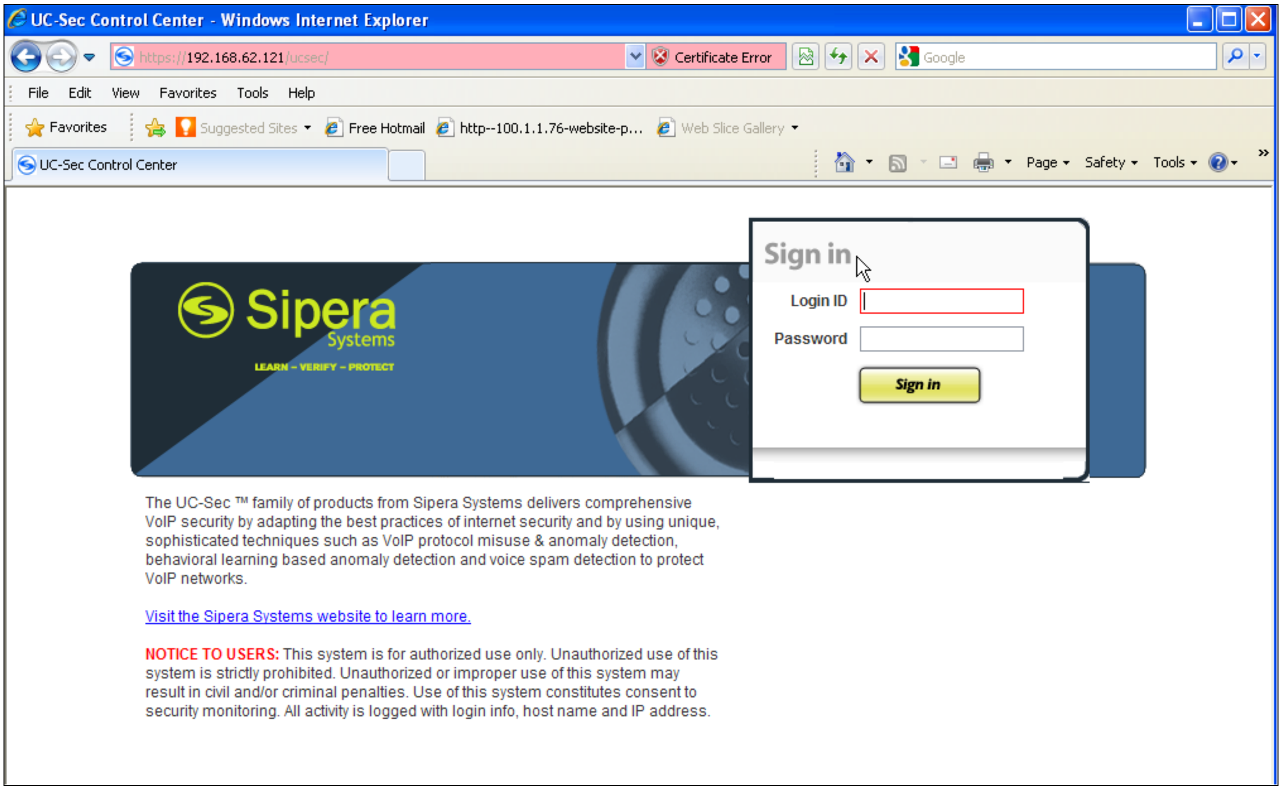
7.2. Advanced Configuration

The follow provisioning is performed via the 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 the Avaya SBCE).
2. Select **UC-SEC Control Center**.



3. Enter the login ID and password



The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

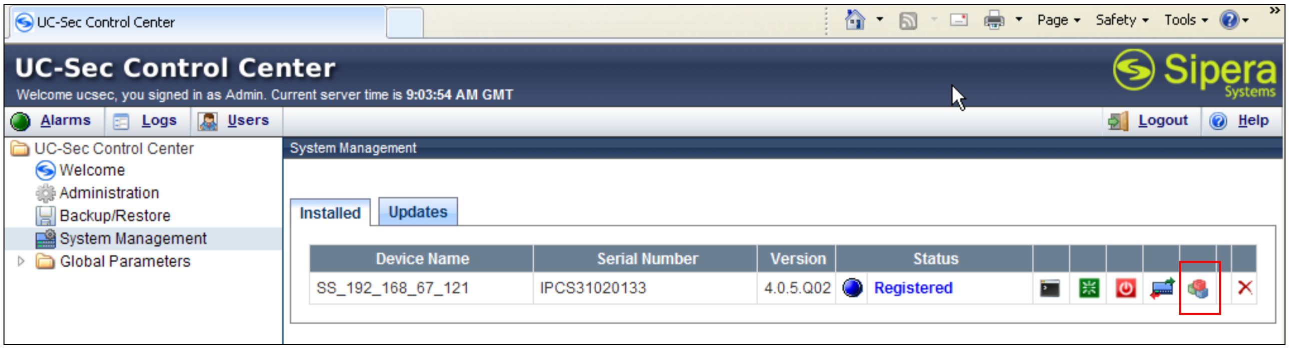
Visit the Sipera Systems website to learn more.

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

7.3. System Management

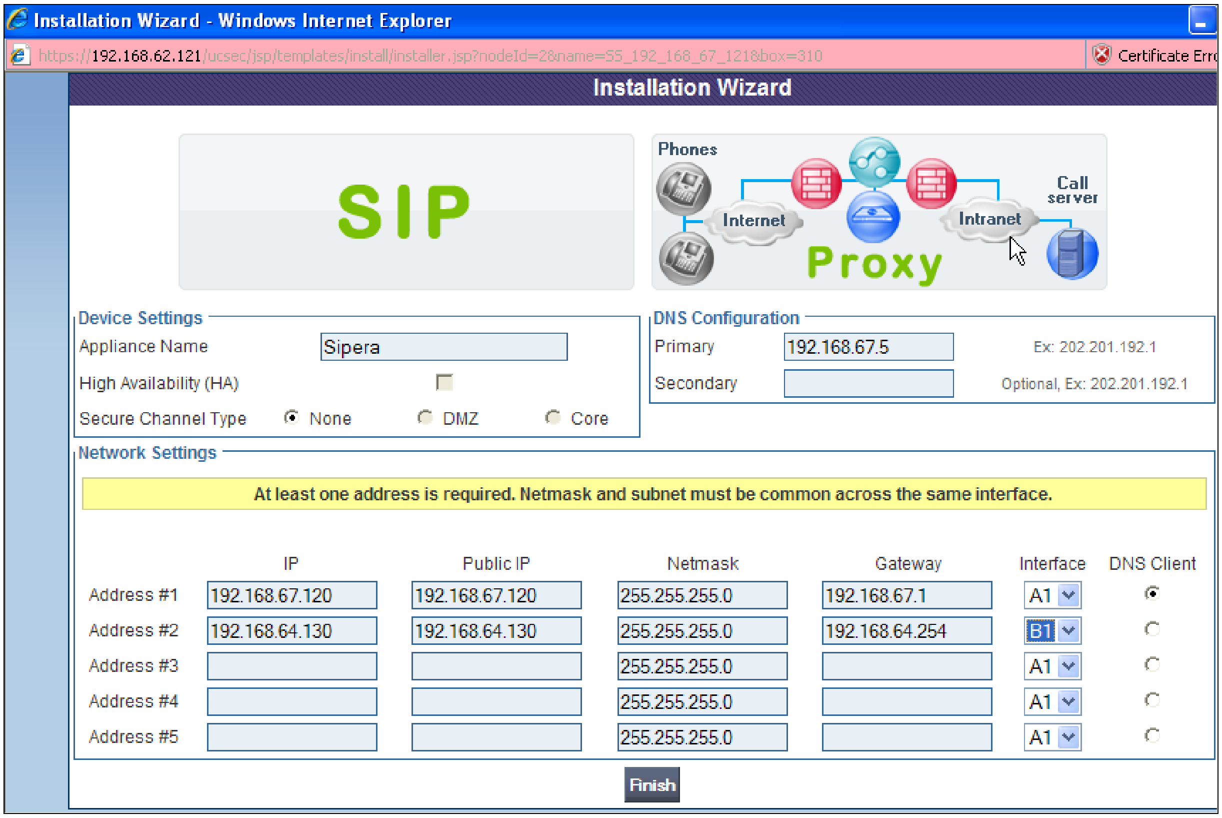
When it is the first time the user accesses the Avaya SBCE system through the web interface, the user needs to configure some basic parameters.

1. Click on the **System Management**, the user will see the screen below:



Device Name	Serial Number	Version	Status
SS_192_168_67_121	IPCS31020133	4.0.5.Q02	Registered

2. The initial status of the SBCE is **Registered**, as shown in above diagram. User should then click on **install** button (highlighted in red). Click on the **System Management**, the screen below will open:


Installation Wizard - Windows Internet Explorer
https://192.168.62.121/ucsec/jsp/templates/install/installer.jsp?nodeId=2&name=SS_192_168_67_121&box=310
Certificate Erro
Installation Wizard
SIP
Phones
Internet
Intranet
Call server
Proxy
Finish

Device Settings

Appliance Name: Sipera

High Availability (HA) ☐

Secure Channel Type ● None ○ DMZ ○ Core

DNS Configuration

Primary: 192.168.67.5 Ex: 202.201.192.1

Secondary: Optional, Ex: 202.201.192.1

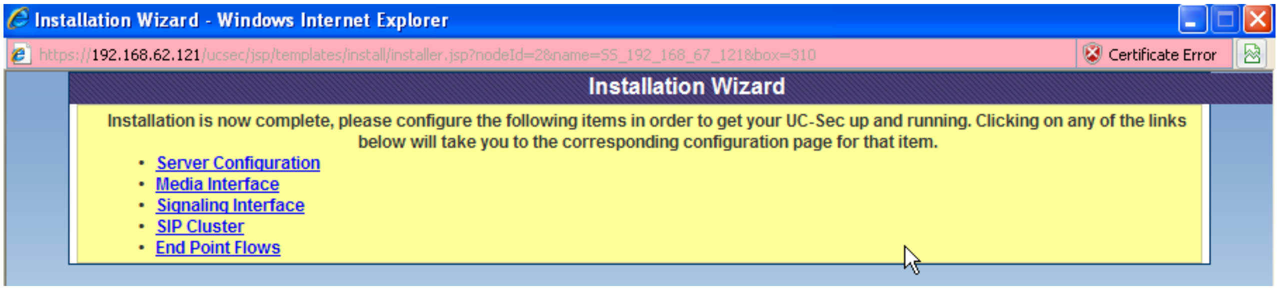
Network Settings

At least one address is required. Netmask and subnet must be common across the same interface.

	IP	Public IP	Netmask	Gateway	Interface	DNS Client
Address #1	192.168.67.120	192.168.67.120	255.255.255.0	192.168.67.1	A1	●
Address #2	192.168.64.130	192.168.64.130	255.255.255.0	192.168.64.254	B1	○
Address #3			255.255.255.0		A1	○
Address #4			255.255.255.0		A1	○
Address #5			255.255.255.0		A1	○

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.


Installation Wizard - Windows Internet Explorer
https://192.168.62.121/ucsec/jsp/templates/install/installer.jsp?nodeId=2&name=SS_192_168_67_121&box=310
Certificate Error

Installation Wizard

Installation is now complete, please configure the following items in order to get your UC-Sec up and running. Clicking on any of the links below will take you to the corresponding configuration page for that item.

- Server Configuration
- Media Interface
- Signaling Interface
- SIP Cluster
- End Point Flows

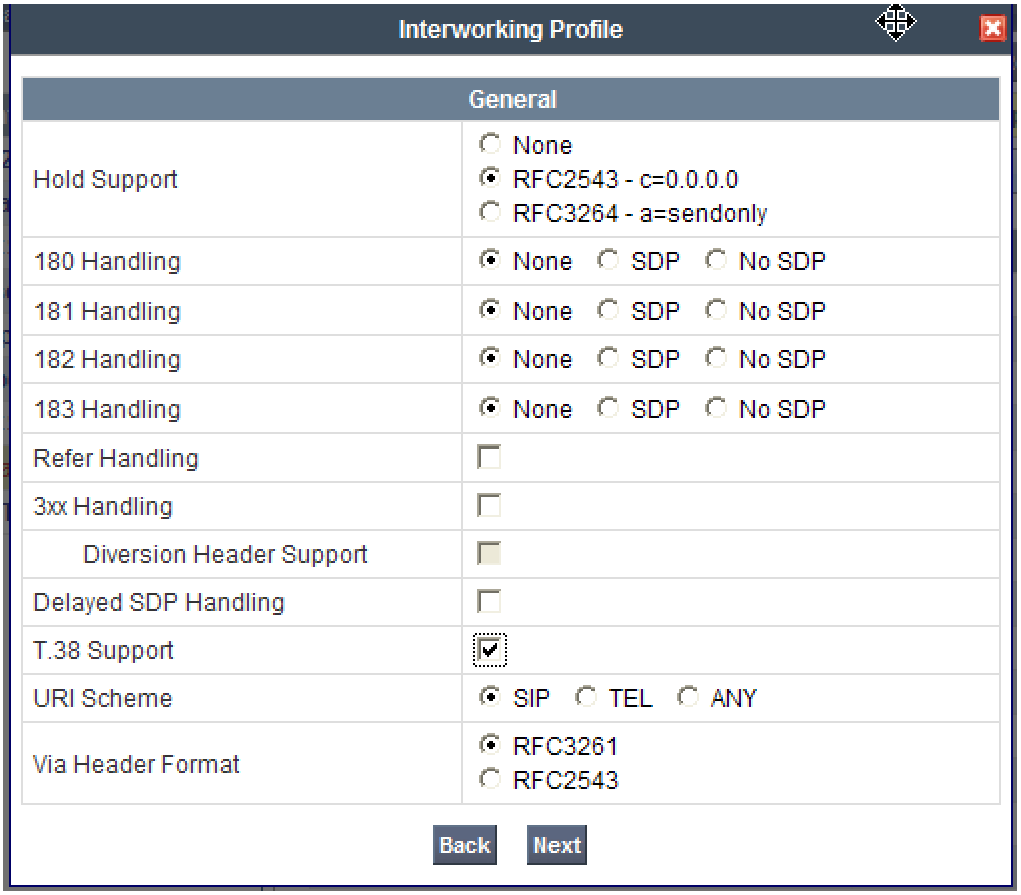
7.4. Global Profiles

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

7.4.1 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**

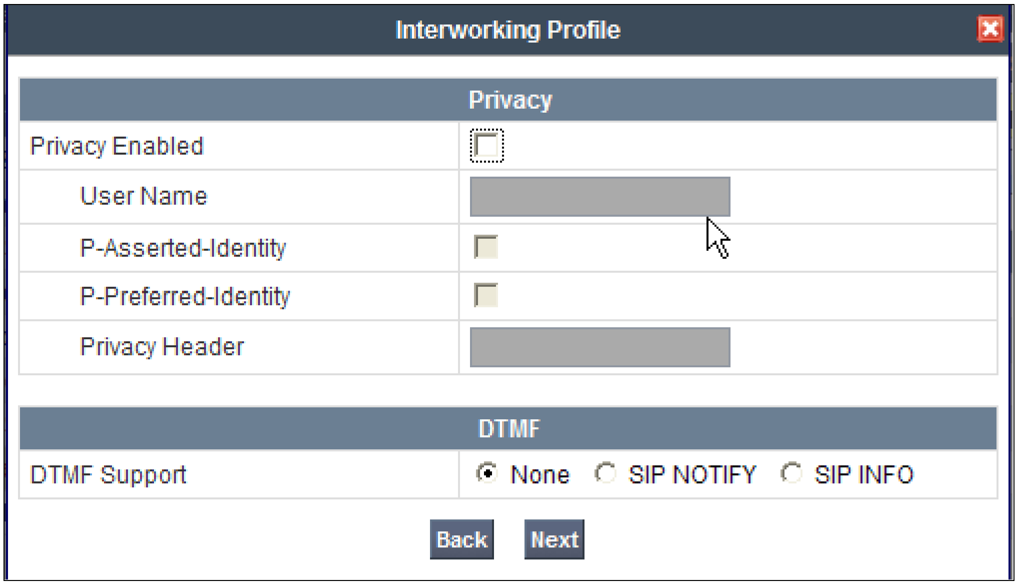


Interworking Profile

General

Hold Support	○ None ● RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☐
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

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



Interworking Profile

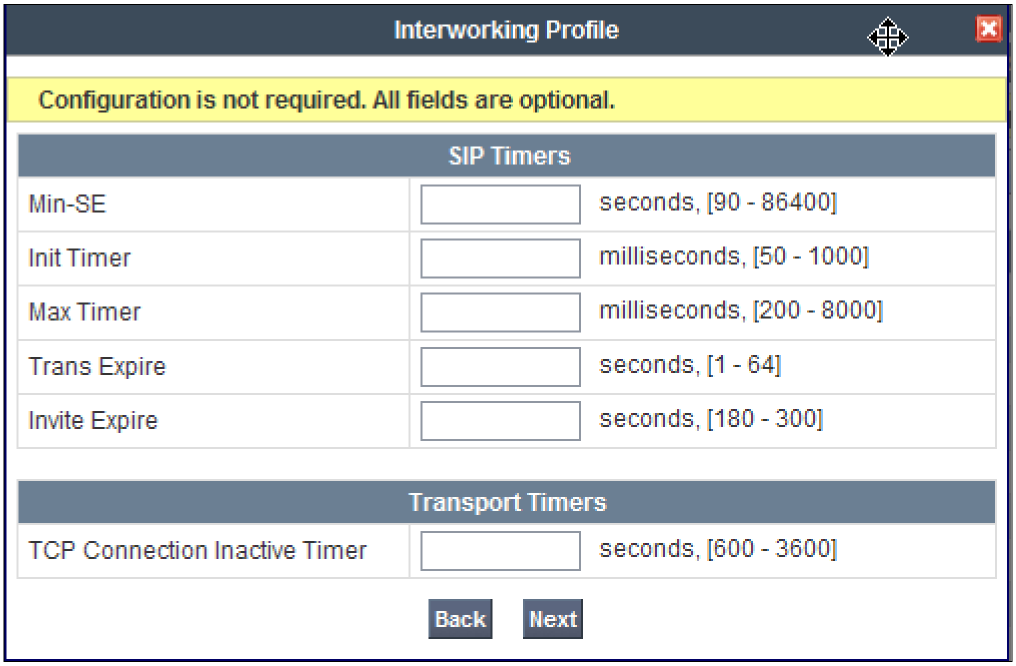
Privacy

Privacy Enabled	☐
User Name	
P-Asserted-Identity	☐
P-Preferred-Identity	☐
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

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



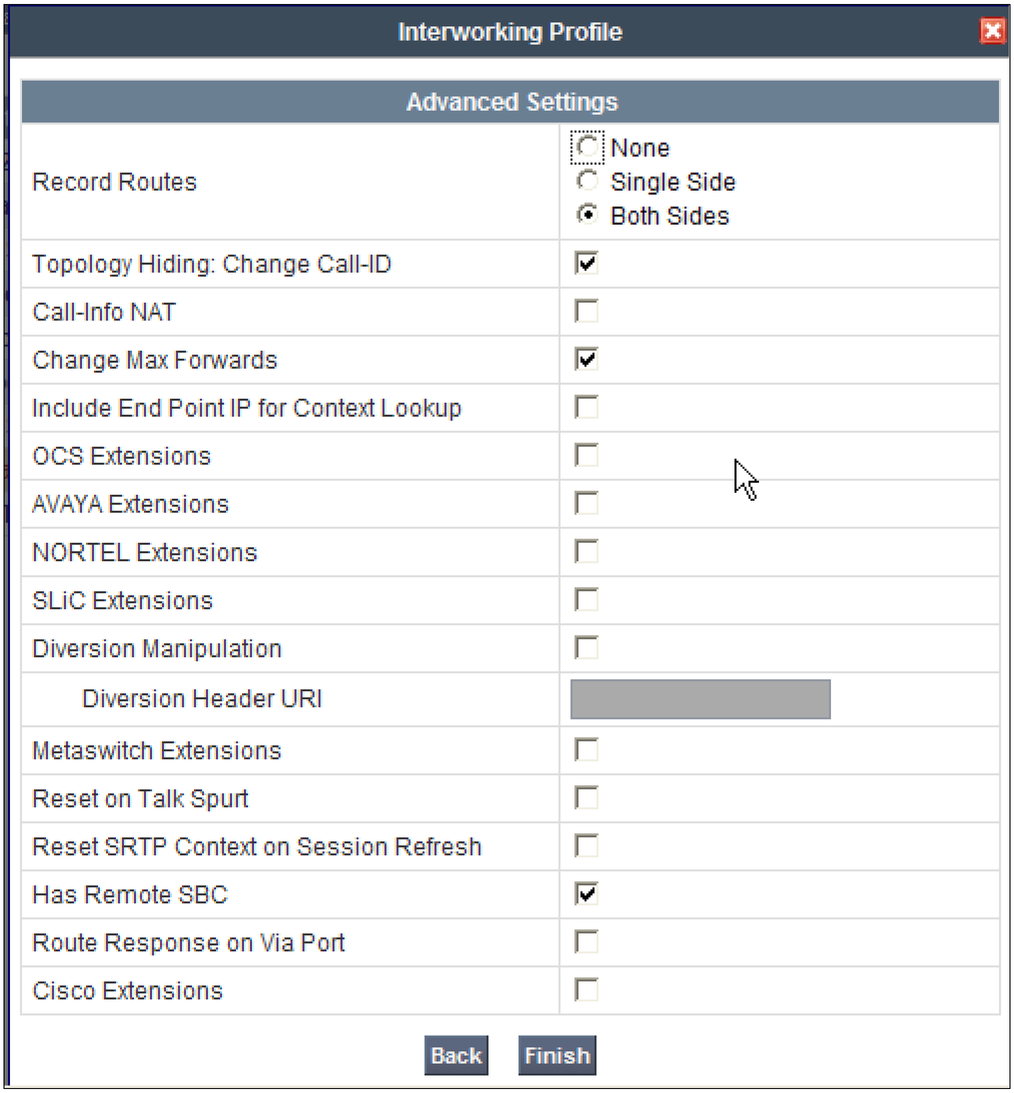
Interworking Profile

Configuration is not required. All fields are optional.

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]

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



Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	☐
Change Max Forwards	☑
Include End Point IP for Context Lookup	☐
OCS Extensions	☐
AVAYA Extensions	☐
NORTEL Extensions	☐
SLiC Extensions	☐
Diversion Manipulation	☐
Diversion Header URI	
Metaswitch Extensions	☐
Reset on Talk Spurt	☐
Reset SRTP Context on Session Refresh	☐
Has Remote SBC	☑
Route Response on Via Port	☐
Cisco Extensions	☐

7.4.2 Server Interworking – AT&T Side

Repeat the steps shown in **Section 7.4.1** to add an Interworking Profile for the connection to AT&T.

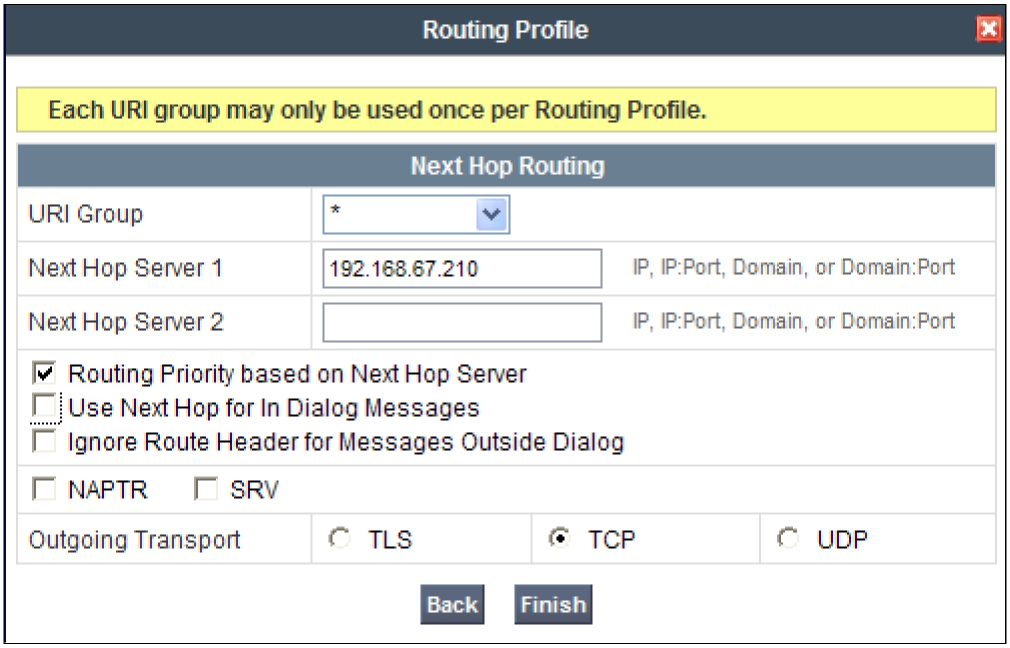
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Interworking**
3. Select **Add Profile**
4. On the **General** Tab:
    a. Enter a profile name**:** (e.g., **ATT**)
    b. Check **T38 Support - Yes**
    c. All other options on the General Tab can be left at default
    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**

7.4.3 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**

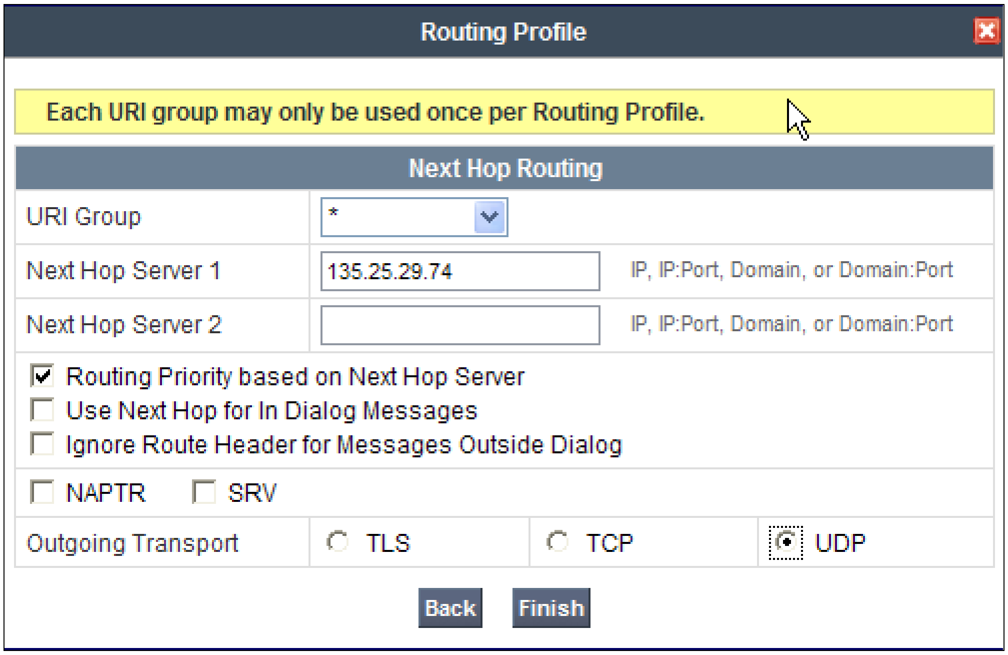

Routing Profile
Each URI group may only be used once per Routing Profile.
Next Hop Routing
IP, IP:Port, Domain, or Domain:Port
IP, IP:Port, Domain, or Domain:Port
Back
Finish

URI Group: *
Next Hop Server 1: 192.168.67.210
Next Hop Server 2:
☑ 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

7.4.4 Routing – AT&T Side

Repeat the steps in **Section 7.4.3** 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
IP, IP:Port, Domain, or Domain:Port
IP, IP:Port, Domain, or Domain:Port
Back
Finish

URI Group: *

Next Hop Server 1: 135.25.29.74

Next Hop Server 2:

☑ Routing Priority based on Next Hop Server
☐ Use Next Hop for In Dialog Messages
☐ Ignore Route Header for Messages Outside Dialog

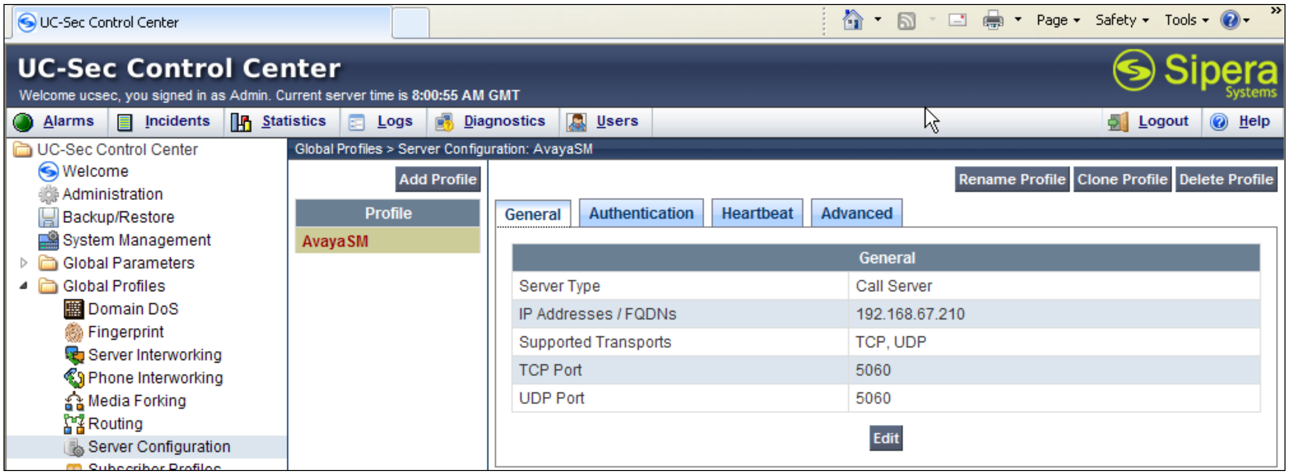
☐ NAPTR ☐ SRV

Outgoing Transport: ○ TLS ○ TCP ● UDP

7.4.5 Server Configuration – To Avaya Aura® Session Manager

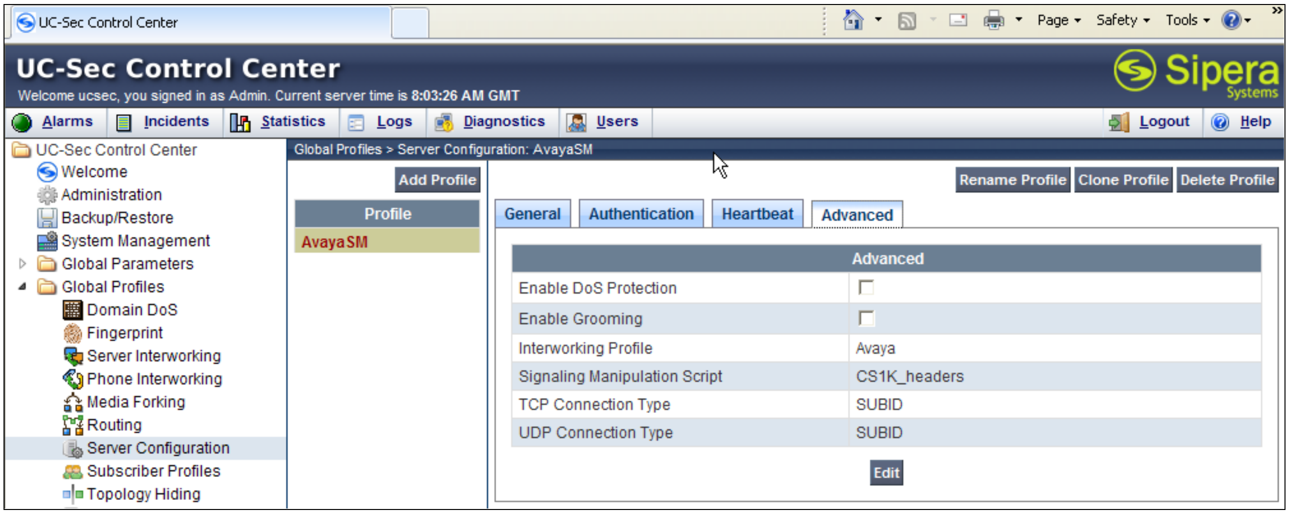
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters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



General	
Server Type	Call Server
IP Addresses / FQDNs	192.168.67.210
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

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 following script defined in Section **7.4.9.** This script will remove any Avaya CS1000E SIP headers not needed by AT&T**.**
        i. **CS1K_headers**
    c. Select **Next.**
8. Click **Finish**.



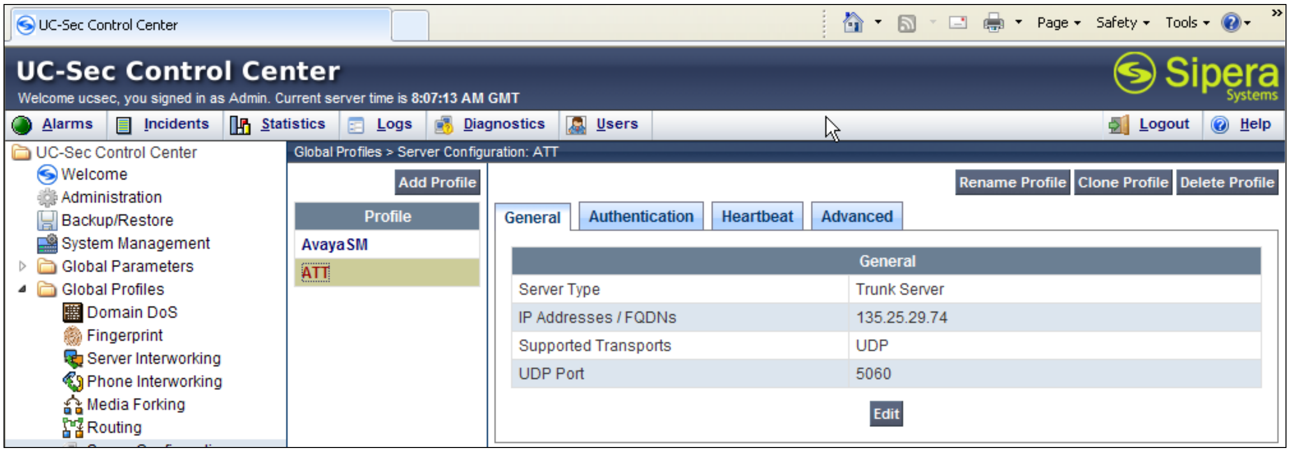
Advanced	
Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	Avaya
Signaling Manipulation Script	CS1K_headers
TCP Connection Type	SUBID
UDP Connection Type	SUBID

7.4.6 Server Configuration – To AT&T

Repeat the steps in **Section 7.4.5** to create a Server Configuration for the connection to AT&T.

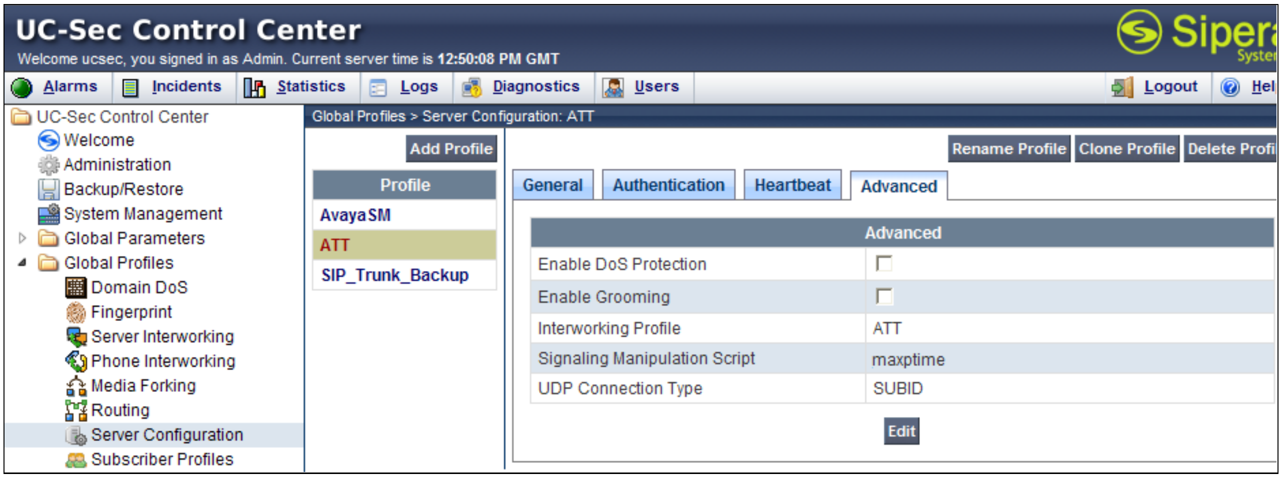
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile, enter profile name:** (e.g., **ATT**)
4. On the **Add Server Configuration Profile** Tab:

    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**.



General	
Server Type	Trunk Server
IP Addresses / FQDNs	135.25.29.74
Supported Transports	UDP
UDP Port	5060

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 following script defined in Section **7.4.9.** This script will remove any leading plus signs from digit strings sent to AT&T, as well as convert the maxtime:30 parameter to ptime:30 for inbound calls from AT&T**.**
        i. **maxptime**
    c. Select **Next.**
8. Click **Finish**.

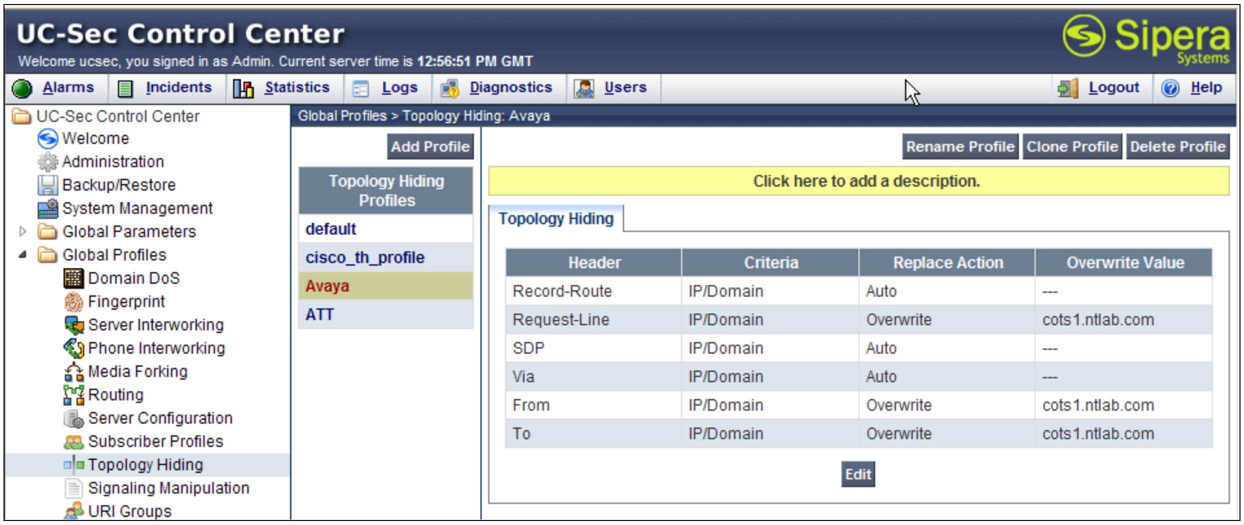


Advanced	
Enable DoS Protection	☐
Enable Grooming	☐
Interworking Profile	ATT
Signaling Manipulation Script	maxptime
UDP Connection Type	SUBID

7.4.7 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. Not that the domain **cots1.ntlab.com** is the also defined in Session Manager in **Section 6.1**.

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**: 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**: cost1.ntlab.com**
8. Click **Finish**



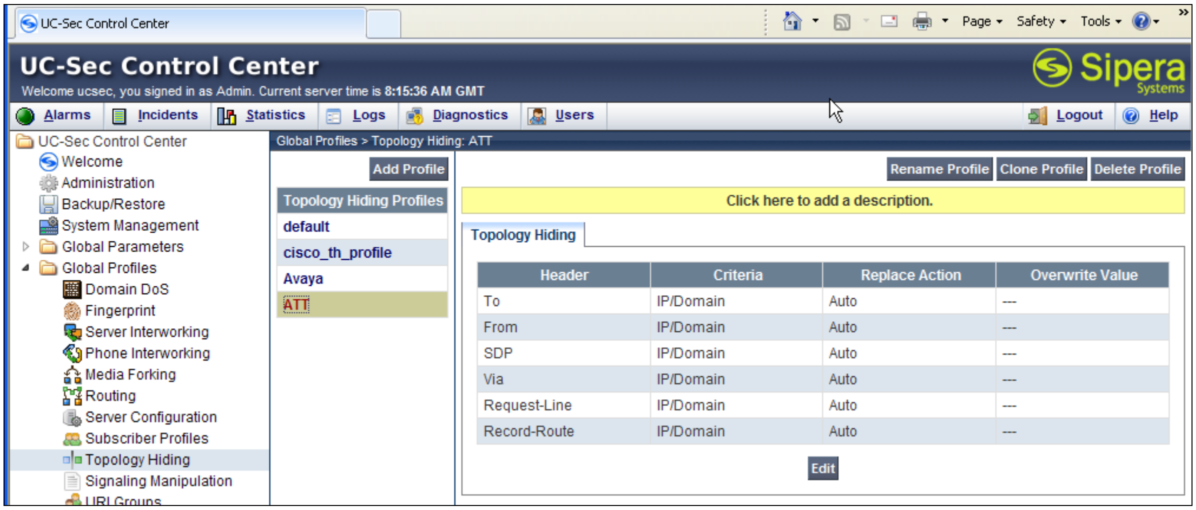
Welcome ucsec, you signed in as Admin. Current server time is 12:56:51 PM GMT

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	cots1.ntlab.com
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	cots1.ntlab.com
To	IP/Domain	Overwrite	cots1.ntlab.com

7.4.8 Topology Hiding – AT&T Side

Repeat the steps in **Section 7.4.7** 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**



Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.4.9 Signaling Manipulations

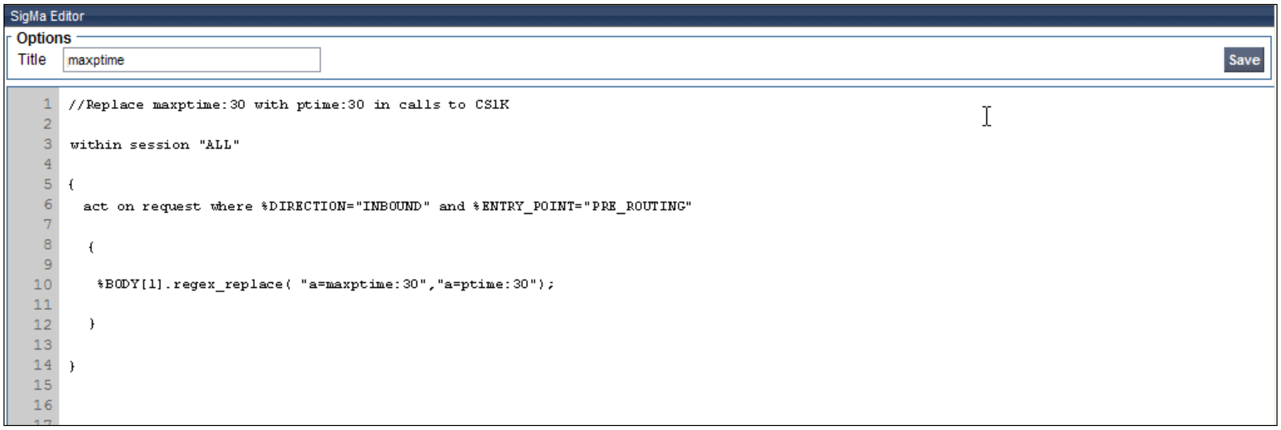
The Avaya SBCE scripts can be used to create custom SIP header manipulations for request and response frames, sent by Avaya CS1000E or by AT&T. Refer to [12] and [13] for information on the Avaya SBCE scripting language. In the reference configuration the following scripts were used for the following 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 7.4.9.1**).
2. In addition to the MIME header removed by Session Manager (see **Section 6.3.2**), Avaya CS1000E generates additional SIP headers that are not required by AT&T (such as Alert-Info, x-nt-e164-clid, and RFC2833 Telephone Event type 111). In the interest of reducing packet overhead, these unnecessary headers are removed (**Section 7.4.9.2**).
3. AT&T does not support the History-Info header. For Call Forward scenarios, Session Manager with change History-Info to Diversion header (see **Section 6.3.2**). For all other call scenarios the Avaya SBCE will remove the History-Info headers (**Section 7.4.9.2**).

7.4.9.1 Script “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");
   }
 }
```

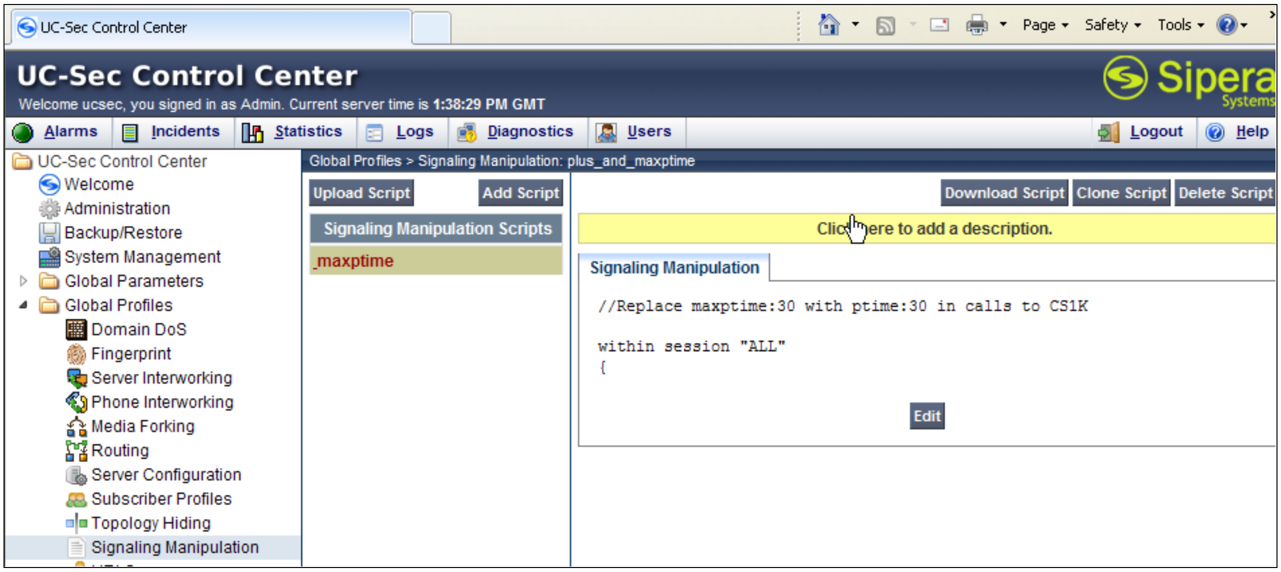


Title: maxptime

```
//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. Click on **Save**. The script editor will test for any errors, and the editor window will close.
7. If changes are required, click on the **Edit** button.

Note -This script is specified in the **Server Configuration** defined in **Section 7.4.6**, **Step 7**.



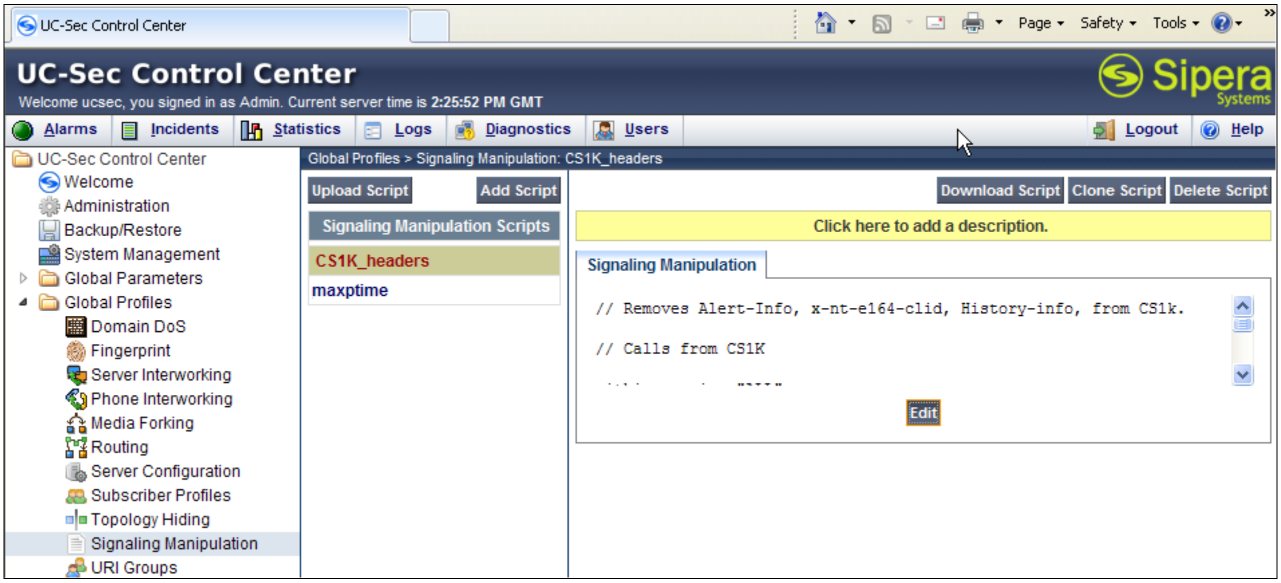
```
//Replace maxptime:30 with ptime:30 in calls to CS1K

within session "ALL"
{
```

7.4.9.2 Script “CS1K_headers”

Create a script called **CS1K_headers** by repeating the steps in **Section 7.4.9.1**, and using the following script:

Note -This script is specified in the **Server Configuration** defined in **Section 7.4.5**, **Step 7**.

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

// Calls 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","");

 }
}

// Remove 111 from CS1K responses

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

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

 }
}
```



Welcome ucsec, you signed in as Admin. Current server time is 2:25:52 PM GMT

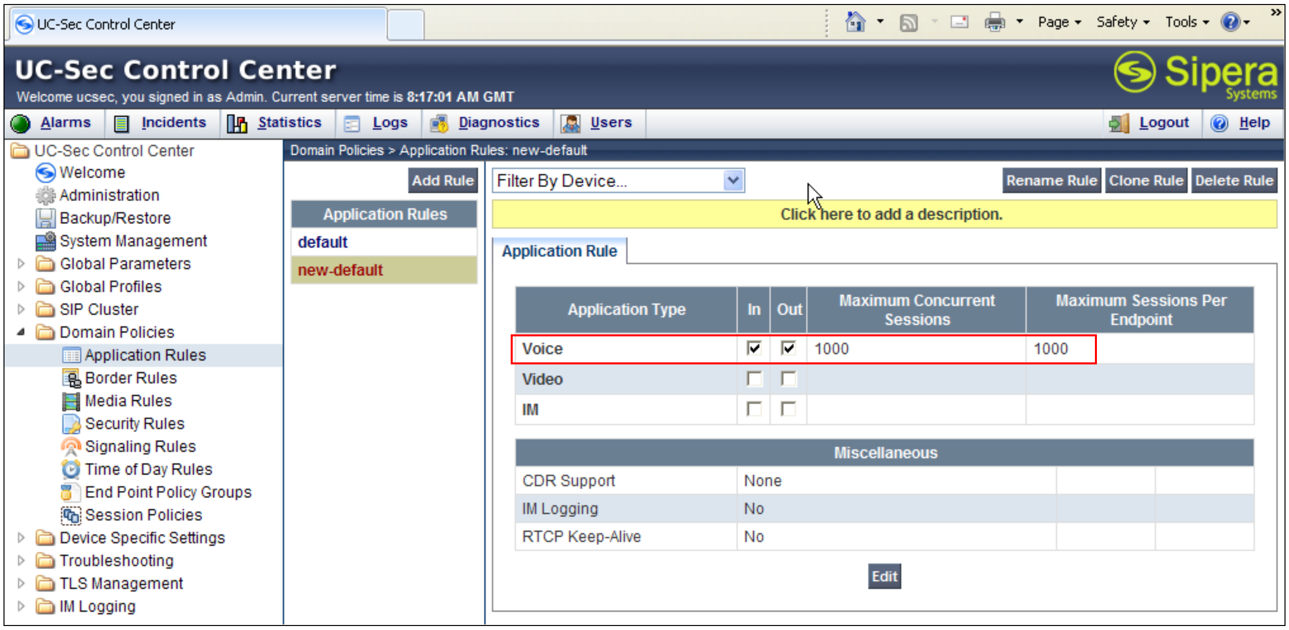
```
// Removes Alert-Info, x-nt-e164-clid, History-info, from CS1k.

// Calls from CS1K
```

7.5. 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.

7.5.1 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 an appropriate value based on the installed license. The number entered here should be larger than the licensed number (e.g., for a license of 500, specify **1000**).
        ii. Change the **Maximum Sessions per Endpoint** to an appropriate value based on the installed license. The number entered here should be larger than the licensed number (e.g., for a license of 500, specify **1000**).



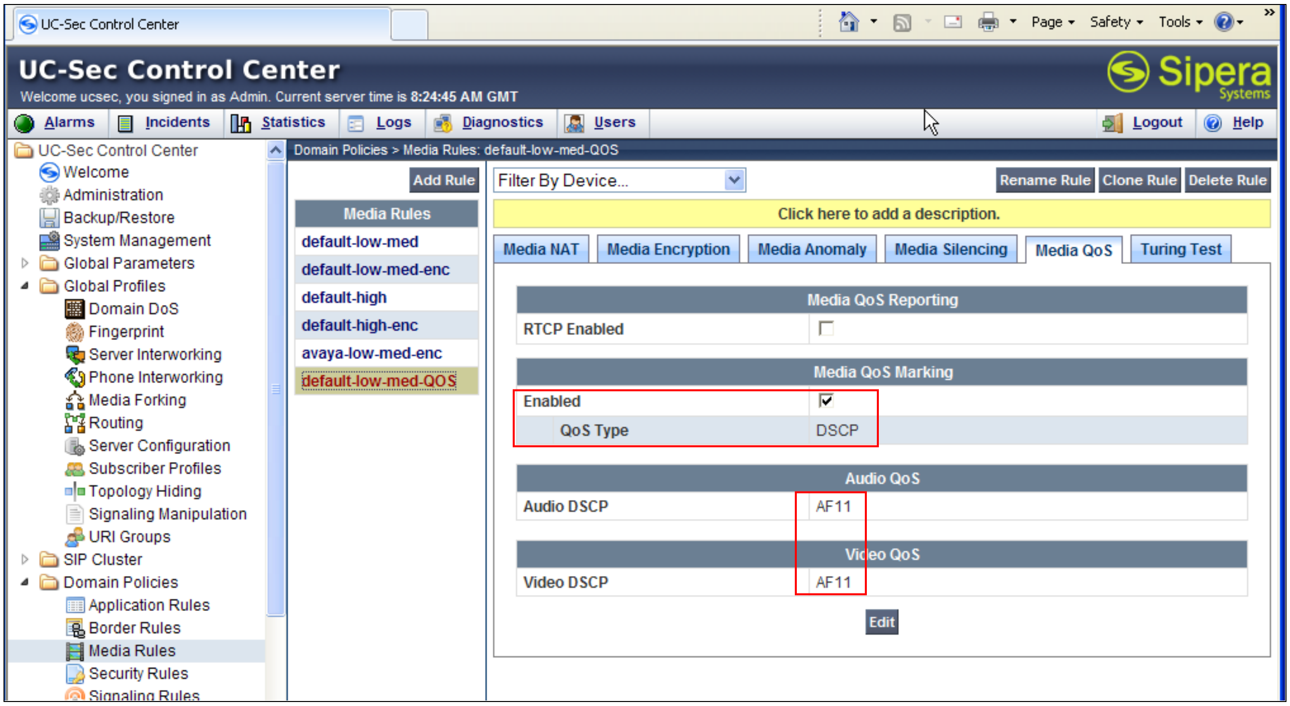
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	1000	1000
Video	☐	☐		
IM	☐	☐		

Miscellaneous	
CDR Support	None
IM Logging	No
RTCP Keep-Alive	No

7.5.2 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**



Welcome ucsec, you signed in as Admin. Current server time is 8:24:45 AM GMT

Domain Policies > Media Rules: default-low-med-QOS

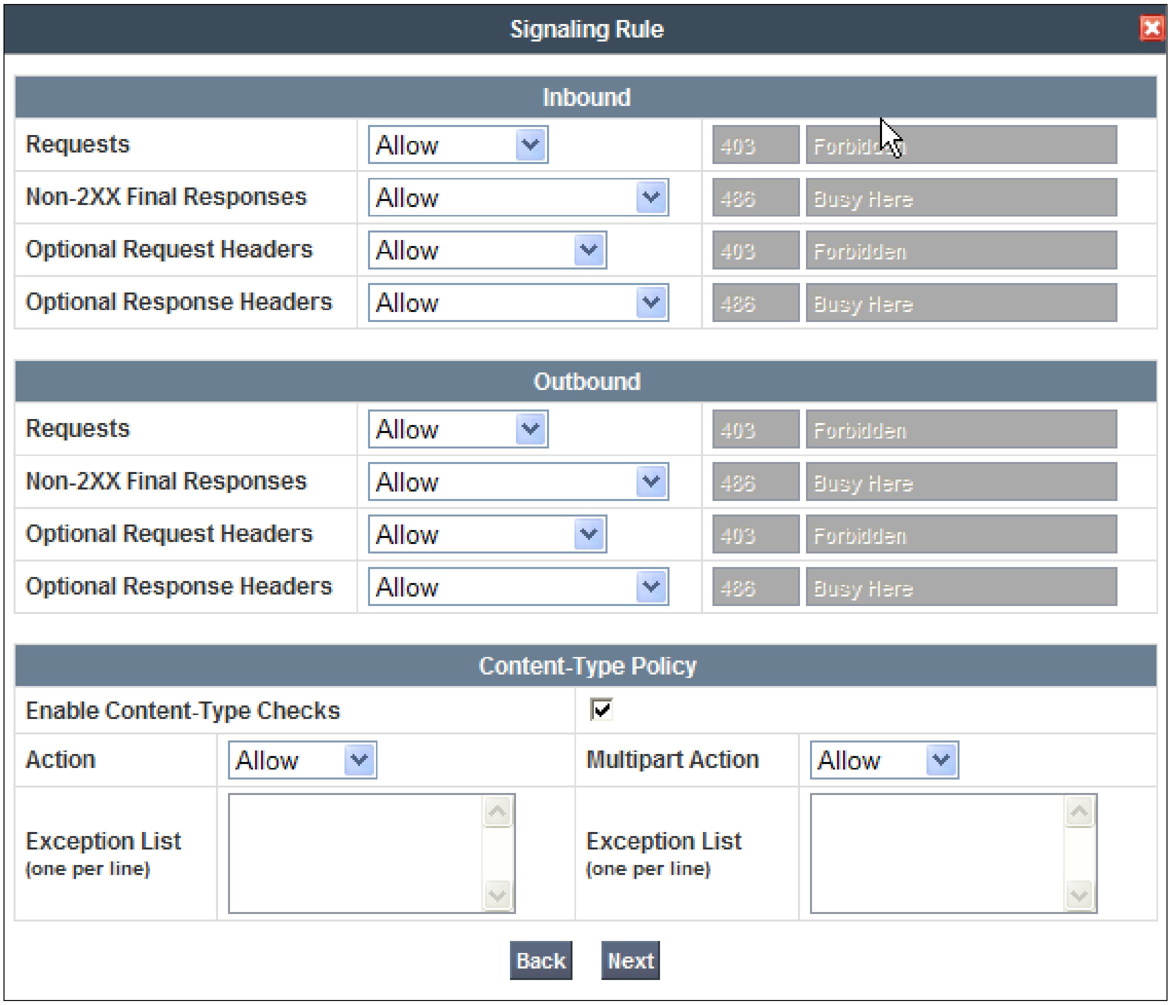
RTCP Enabled ☐
Enabled ☑
QoS Type DSCP
Audio DSCP AF11
Video DSCP AF11

7.5.3 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.



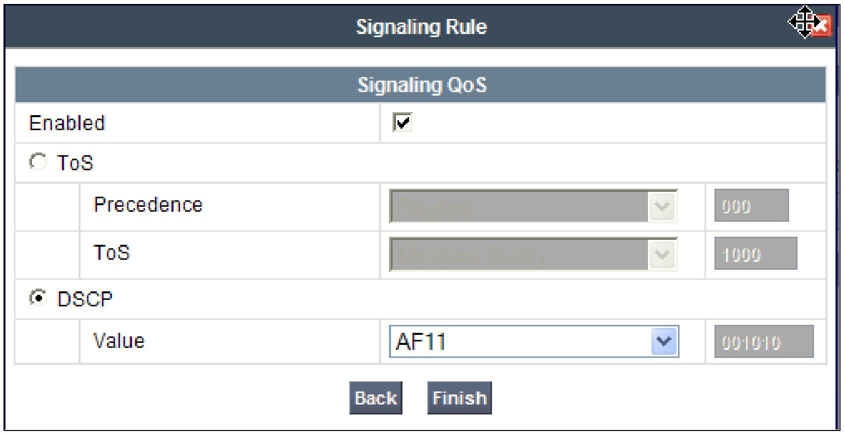
Signaling Rule

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	☑		
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	

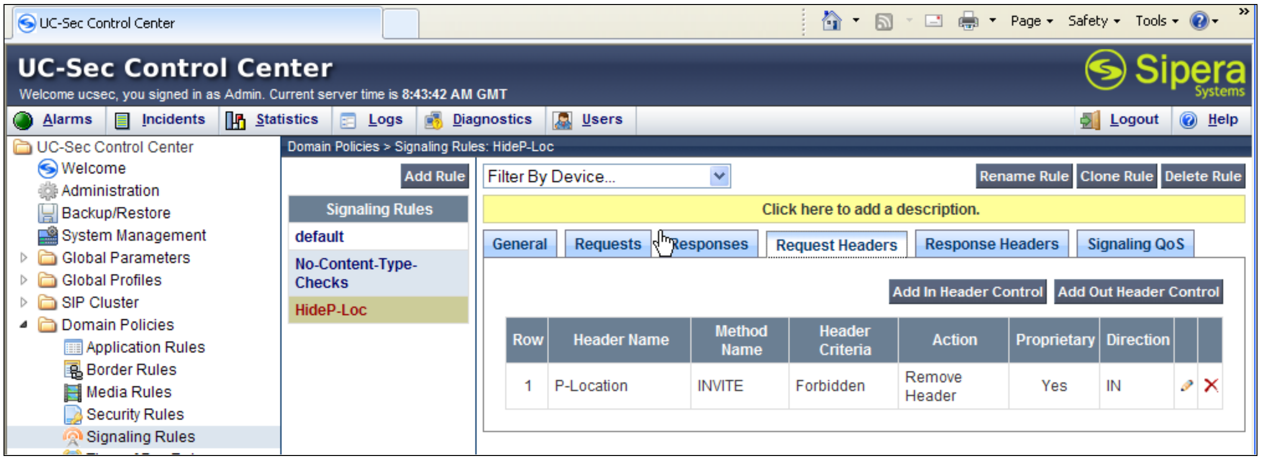
5. On the **Signaling QOS** page
   a. Select **DSCP**
   b. Select **AF11** from the drop-down box
   c. Select **Finish**



Signaling Rule

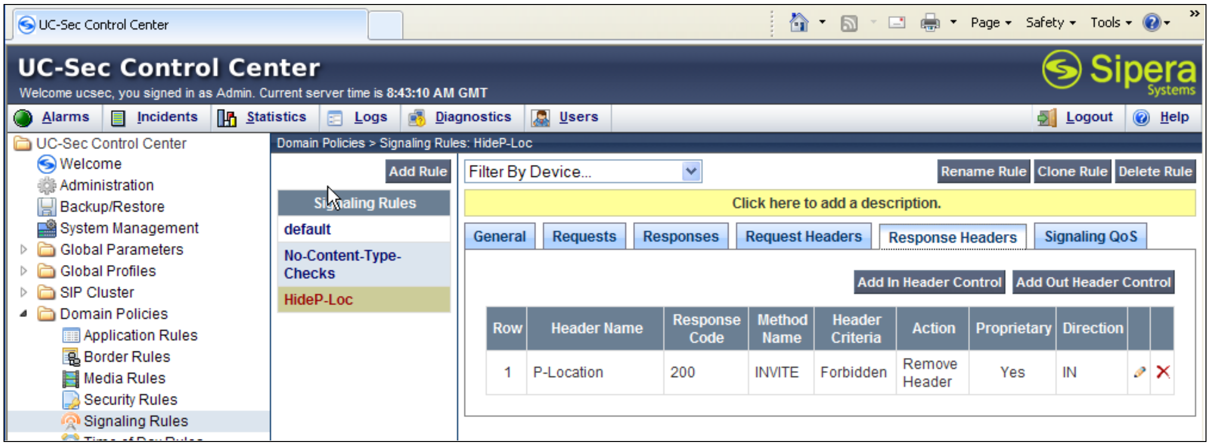
Signaling QoS		
Enabled	☑	
○ ToS		
Precedence		000
ToS		1000
● DSCP		
Value	AF11	001010

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**



Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	P-Location	INVITE	Forbidden	Remove Header	Yes	IN

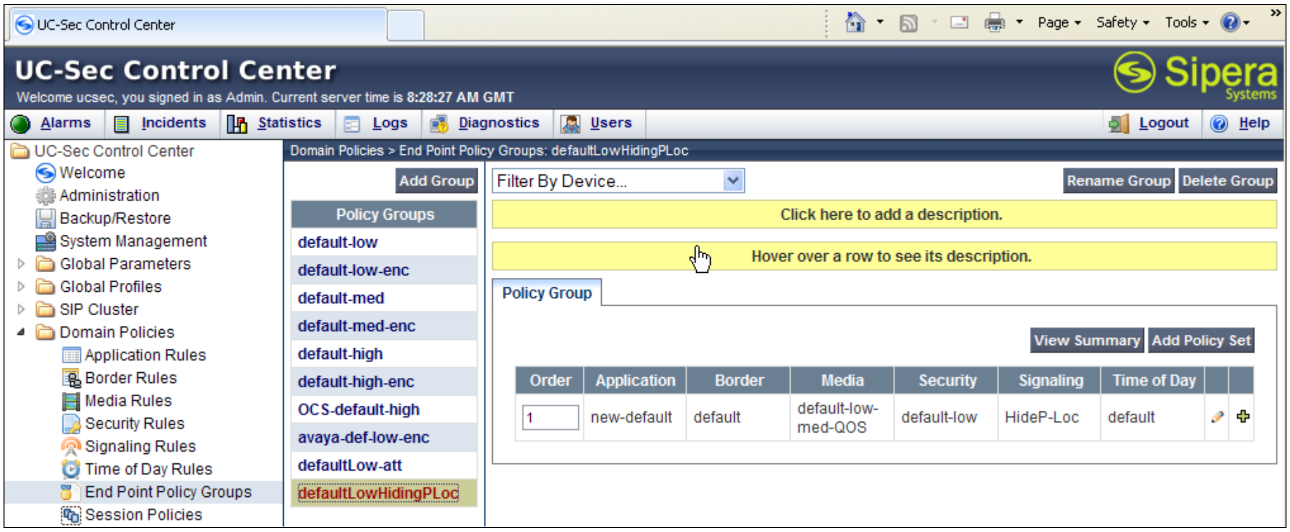
7. Select the **Response Headers** Tab
    a) Select **Add in Header Control**
    b) Check the **Proprietary Request Header** box
    c) **Header Name: P-Location**
    d) **Response Code: 200**
    e) **Method Name: Invite**
    f) **Header Criteria: Forbidden**
    g) **Presence Action: Remove Header**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



Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction
1	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN

7.5.4 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**



Welcome ucsec, you signed in as Admin. Current server time is 8:28:27 AM GMT

Domain Policies > End Point Policy Groups: defaultLowHidingPLoc

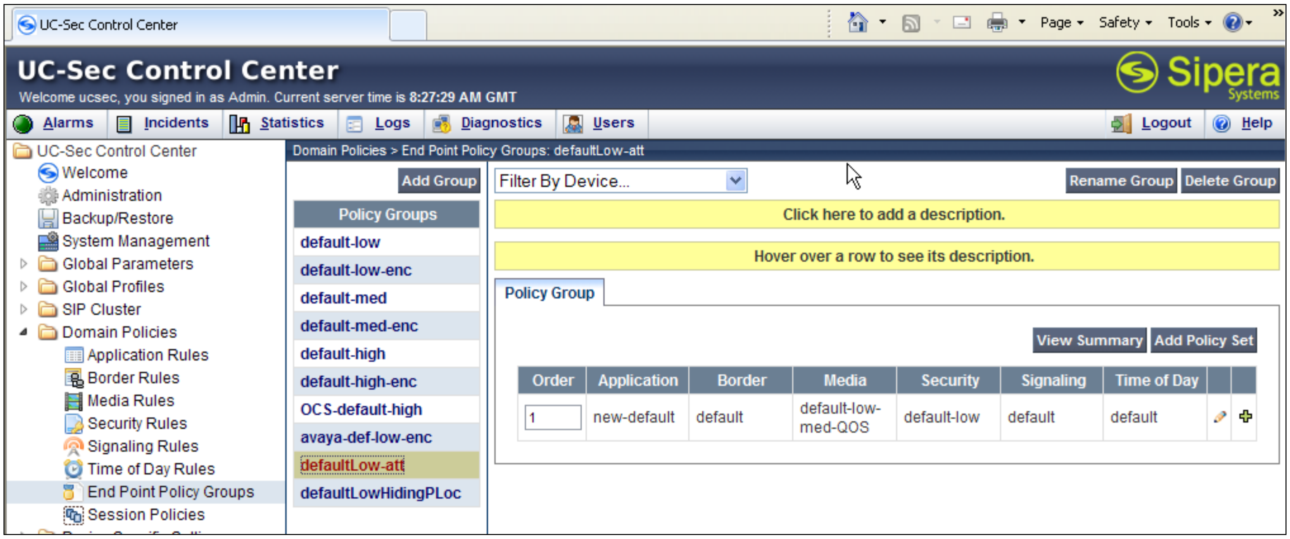
Click here to add a description.

Hover over a row to see its description.

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

7.5.5 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**



Domain Policies > End Point Policy Groups: defaultLow-att

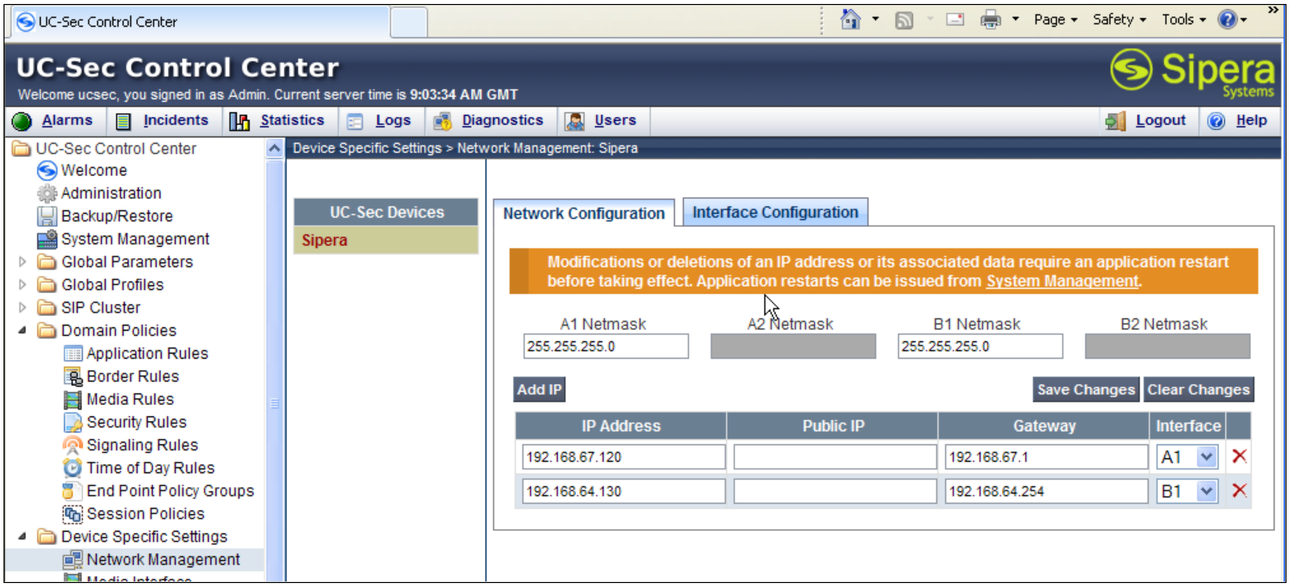
Order	Application	Border	Media	Security	Signaling	Time of Day
1	new-default	default	default-low-med-QOS	default-low	default	default

7.6. 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.

7.6.1 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 7.3**. However if these values need to be modified, do so via this tab.



Device Specific Settings > Network Management: Sipera

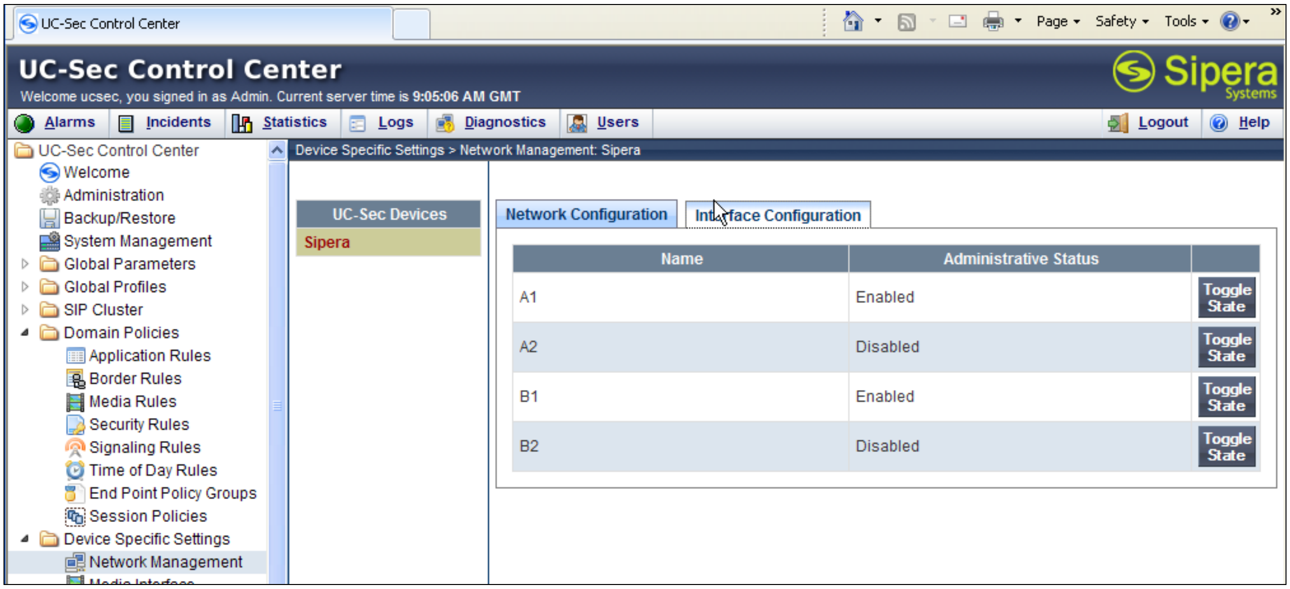
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.0	

IP Address	Public IP	Gateway	Interface
192.168.67.120		192.168.67.1	A1
192.168.64.130		192.168.64.254	B1

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.

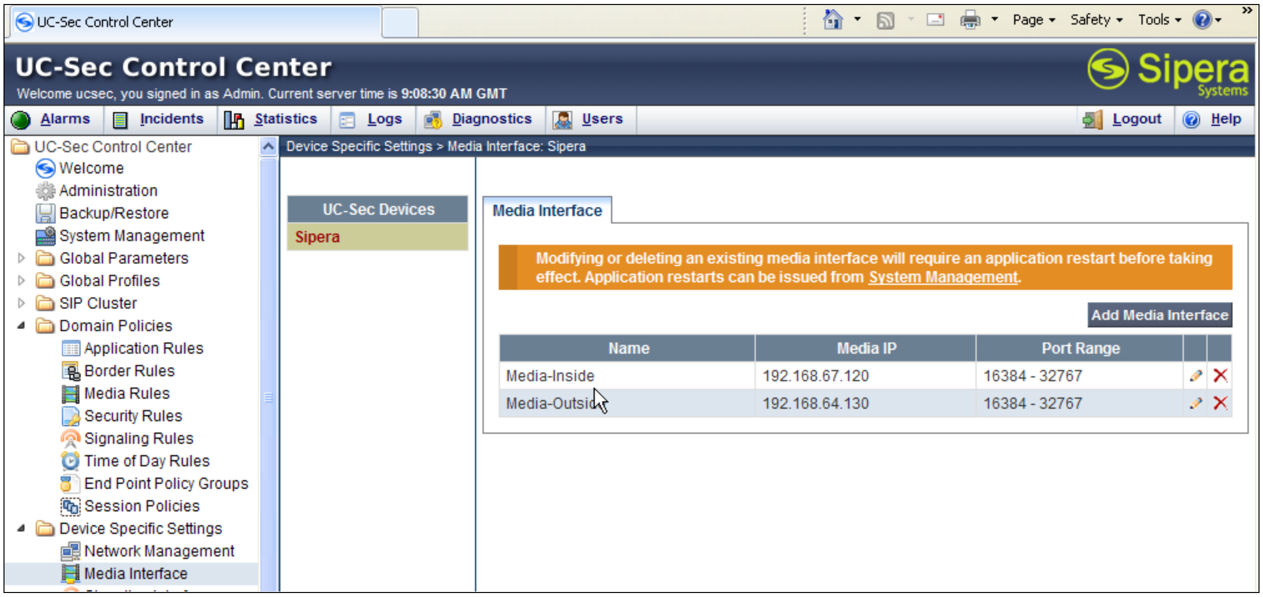


Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

7.6.2 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**



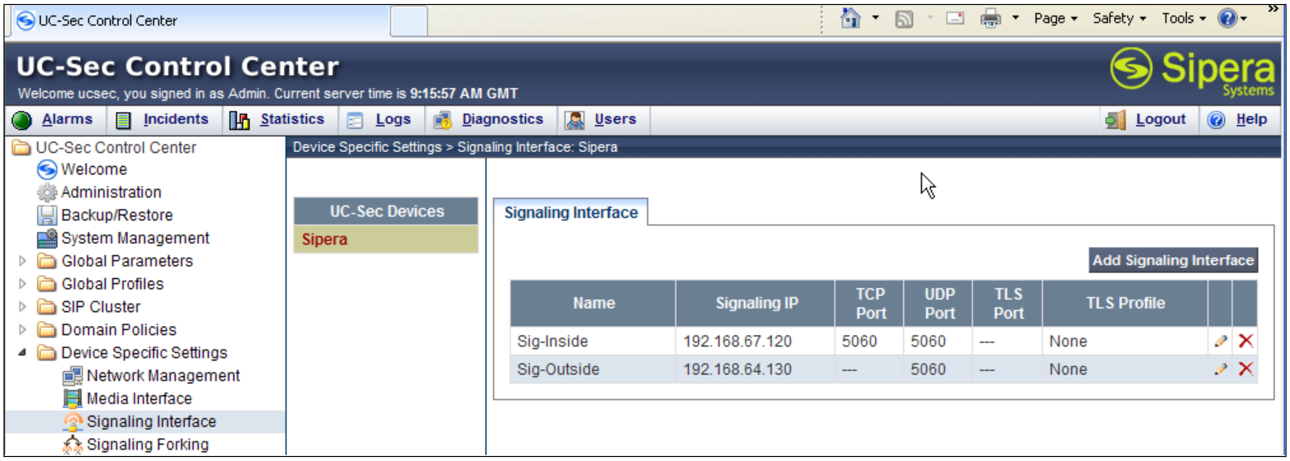
Welcome ucsec, you signed in as Admin. Current server time is 9:08:30 AM GMT

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range
Media-Inside	192.168.67.120	16384 - 32767
Media-Outside	192.168.64.130	16384 - 32767

7.6.3 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**



Welcome ucsec, you signed in as Admin. Current server time is 9:15:57 AM GMT

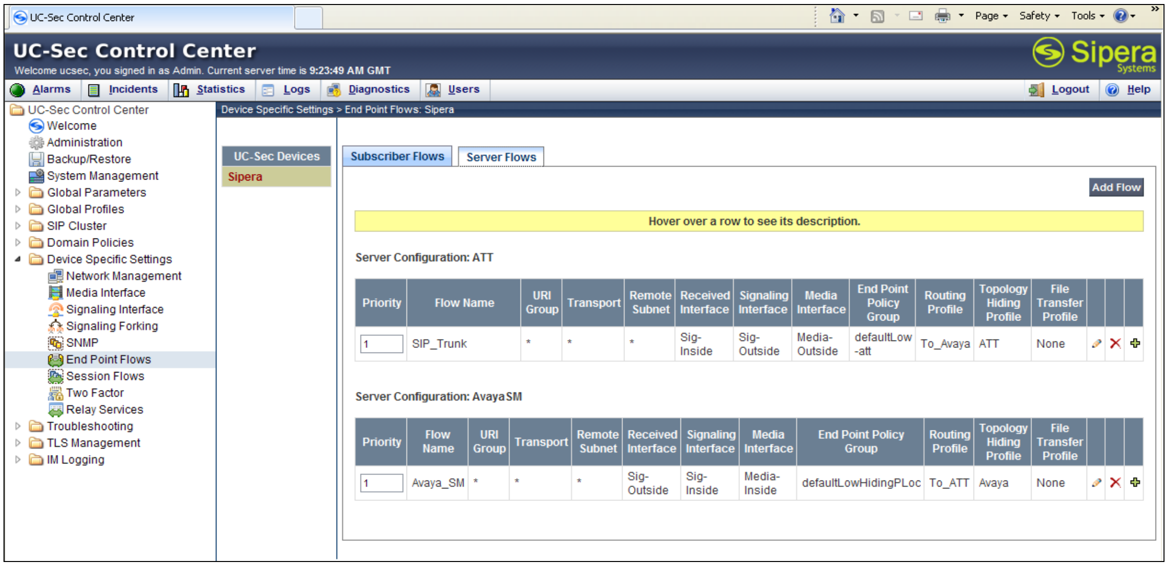
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Sig-Inside	192.168.67.120	5060	5060	---	None
Sig-Outside	192.168.64.130	---	5060	---	None

7.6.4 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**

7.6.5 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**


UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 9:23:49 AM GMT
Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Logout
Help
Device Specific Settings > End Point Flows: Sipera
UC-Sec Devices
Sipera
Subscriber Flows
Server Flows
Add Flow
Hover over a row to see its description.

Server Configuration: ATT

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	SIP_Trunk	*	*	*	Sig-Inside	Sig-Outside	Media-Outside	defaultLow-att	To_Avaya	ATT	None

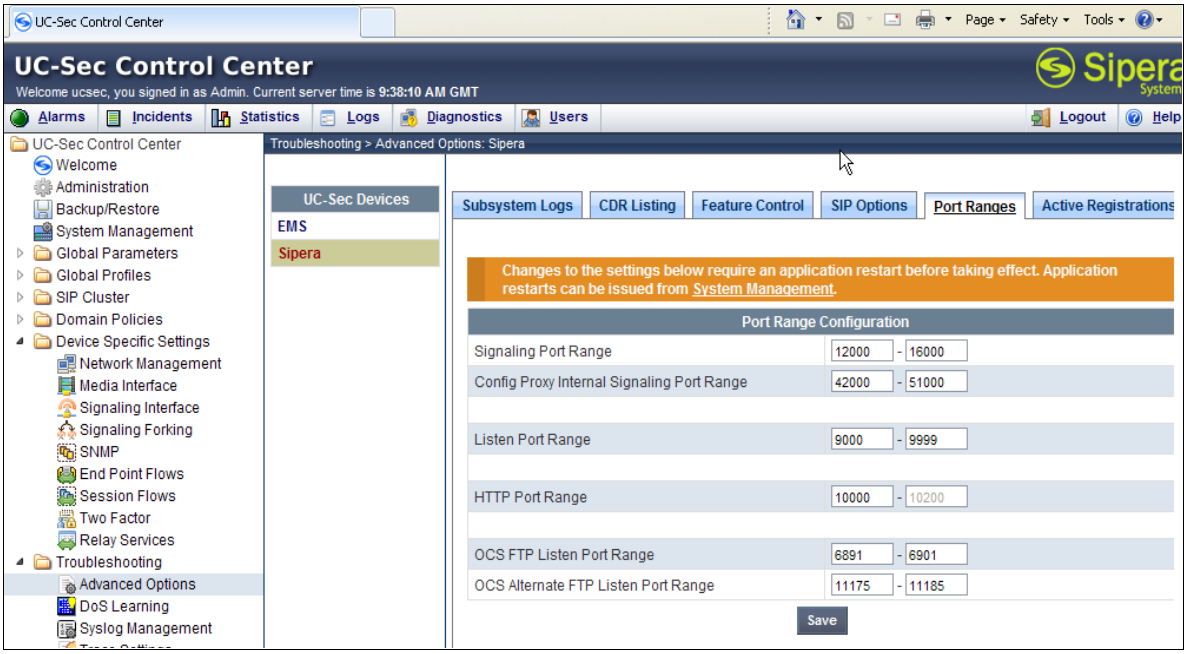
Server Configuration: Avaya SM

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	Avaya_SM	*	*	*	Sig-Outside	Sig-Inside	Media-Inside	defaultLowHidingPLoc	To_ATT	Avaya	None

7.7. Troubleshooting Option - 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 7.6.2**).

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**



Changes to the settings below require an application restart before taking effect. Application restarts can be issued from System Management.

Port Range Configuration

Signaling Port Range	12000	16000
Config Proxy Internal Signaling Port Range	42000	51000
Listen Port Range	9000	9999
HTTP Port Range	10000	10200
OCS FTP Listen Port Range	6891	6901
OCS Alternate FTP Listen Port Range	11175	11185

8. AT&T IP Flexible Reach Service

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

8.1. AT&T Provisioning

The AT&T IP Flexible Reach service provided DID numbers for the reference configuration that could be called from the PSTN. These DID numbers terminated to the Avaya CS1000E location via the AT&T IP Flexible Reach service. Any DID numbers shown in these application notes are examples. Customers will be assigned DIDs by AT&T. It should be noted that the DID numbers dialed, and the DNIS numbers inserted into SIP headers may not be the same digit strings.

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

9. Verification Steps

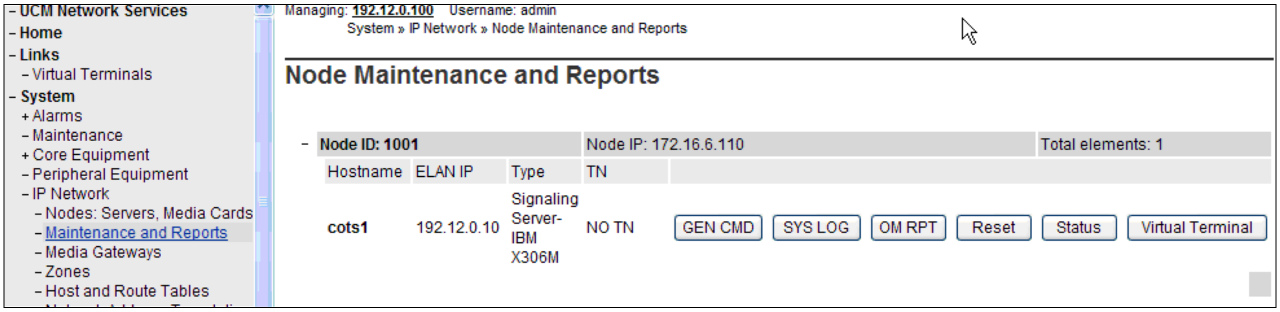
This section provides example verifications of the Avaya configuration with AT&T IP Flexible Reach service.

9.1. Avaya CS1000E Verifications

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

9.1.1 IP Network Maintenance and Reports Commands

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



Managing: 192.12.0.100 Username: admin

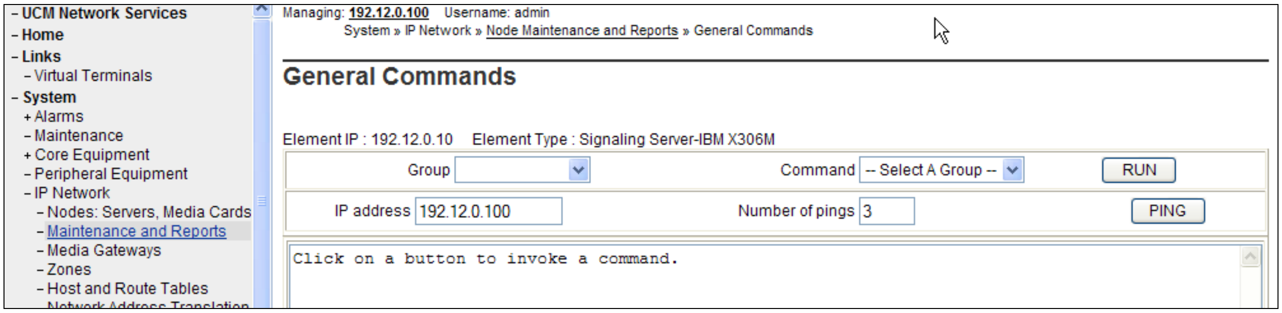
System » IP Network » Node Maintenance and Reports

Node Maintenance and Reports

- Node ID: 1001 | Node IP: 172.16.6.110 | Total elements: 1

Hostname	ELAN IP	Type	TN
cots1	192.12.0.10	Signaling Server-IBM X306M	NO TN

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



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

General Commands

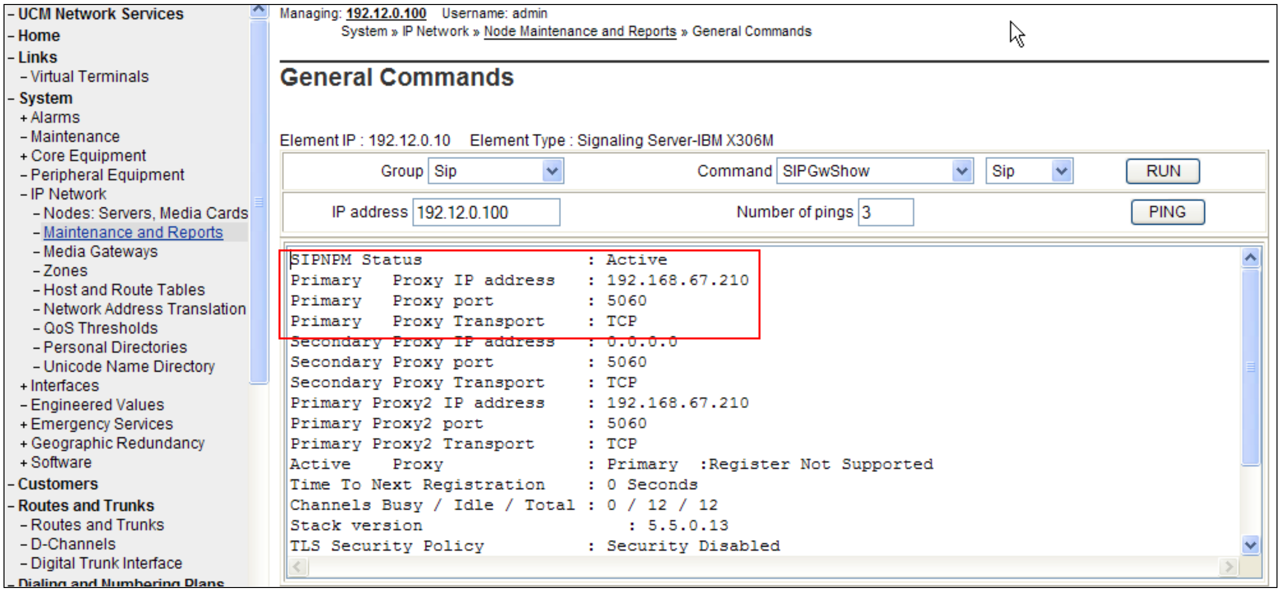
Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group:
Command: -- Select A Group --
IP address: 192.12.0.100
Number of pings: 3

```
Click on a button to invoke a command.
```

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

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



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

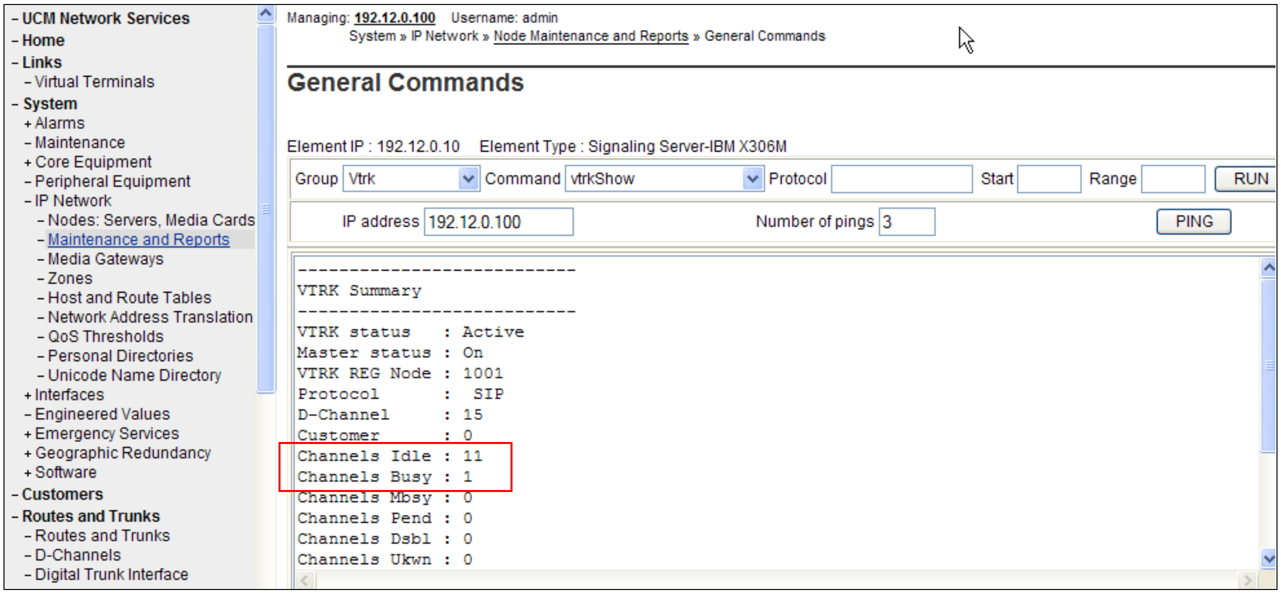
General Commands

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

Group: Sip
Command: SIPGwShow Sip
IP address: 192.12.0.100
Number of pings: 3

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

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



Managing: 192.12.0.100 Username: admin

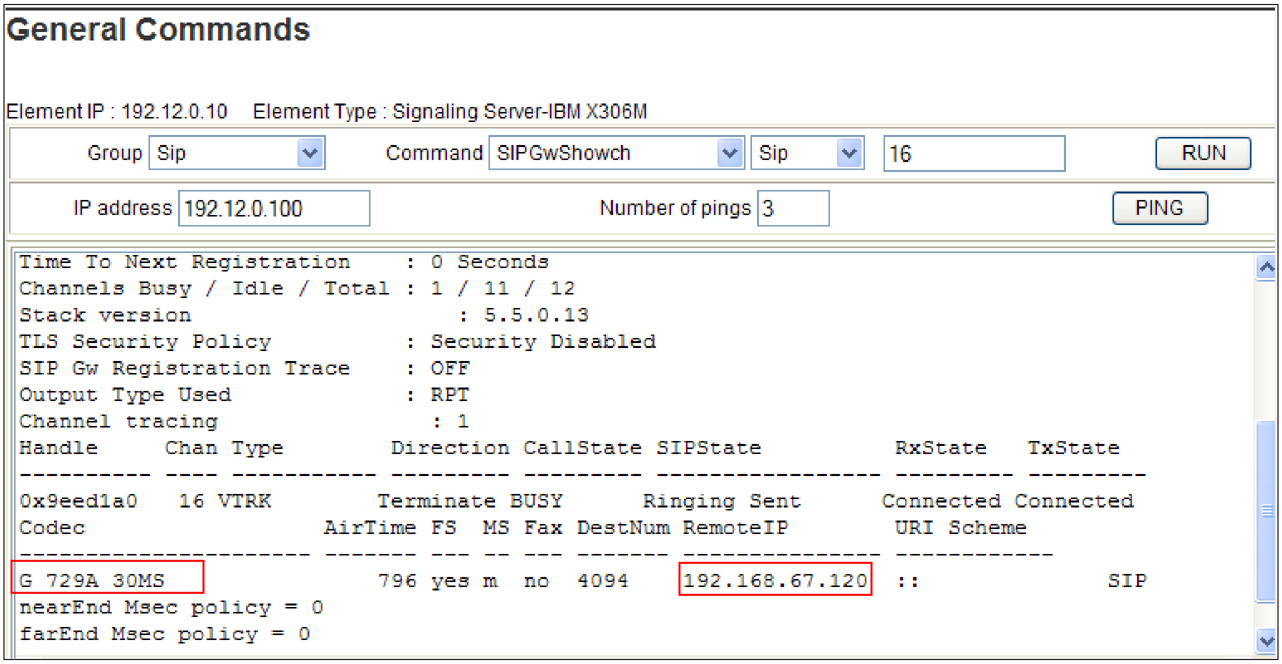
Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group Vtrk Command vtrkShow Protocol Start Range

IP address 192.12.0.100 Number of pings 3

```
--------------------------
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 **16**[3], 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 Avaya SBCE.



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

Group Sip Command SIPGwShowch Sip 16

IP address 192.12.0.100 Number of pings 3

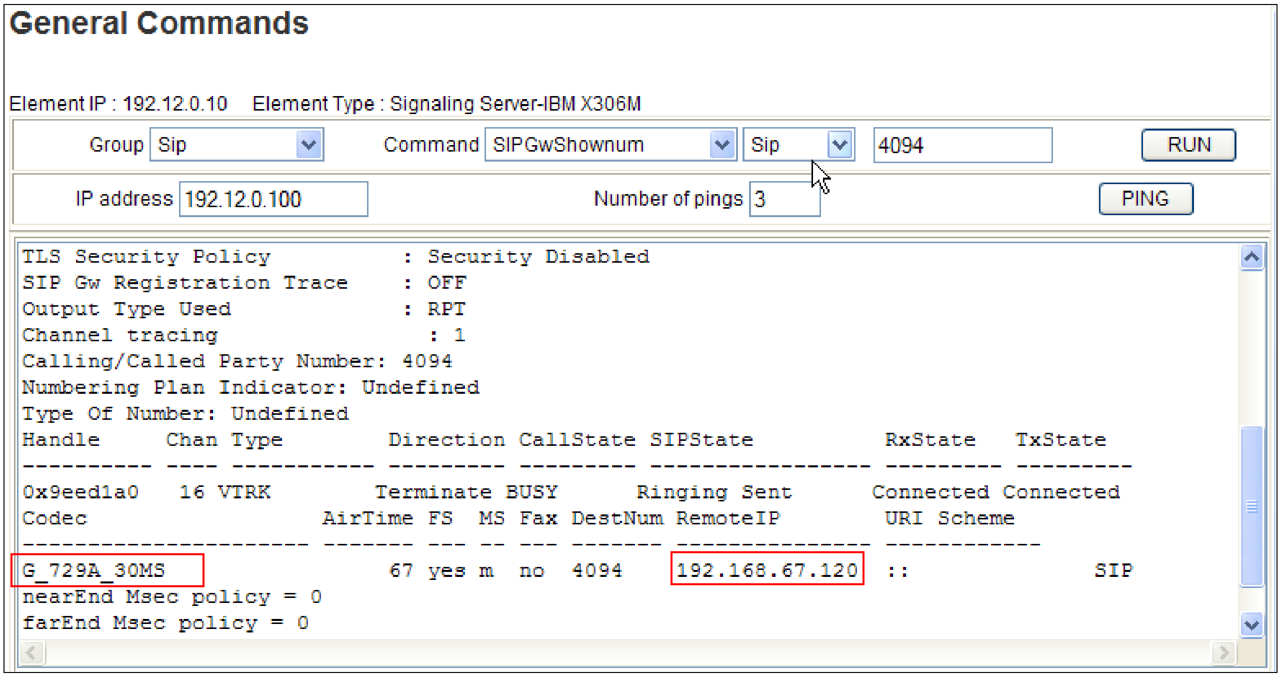
```
Time To Next Registration    : 0 Seconds
Channels Busy / Idle / Total : 1 / 11 / 12
Stack version                  : 5.5.0.13
TLS Security Policy          : Security Disabled
SIP Gw Registration Trace    : OFF
Output Type Used             : RPT
Channel tracing                : 1
Handle     Chan Type         Direction CallState SIPState           RxState   TxState
---------- ---- ----------- --------- --------- ----------------- --------- ---------
0x9eed1a0   16 VTRK        Terminate BUSY      Ringing Sent      Connected Connected
Codec                  AirTime FS  MS Fax DestNum RemoteIP          URI Scheme
---------------------- ------- --- -- --- ------- ---------------  ------------
G 729A 30MS                796 yes m  no  4094    192.168.67.120    ::             SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
```

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

---

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

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 Avaya SBCE.



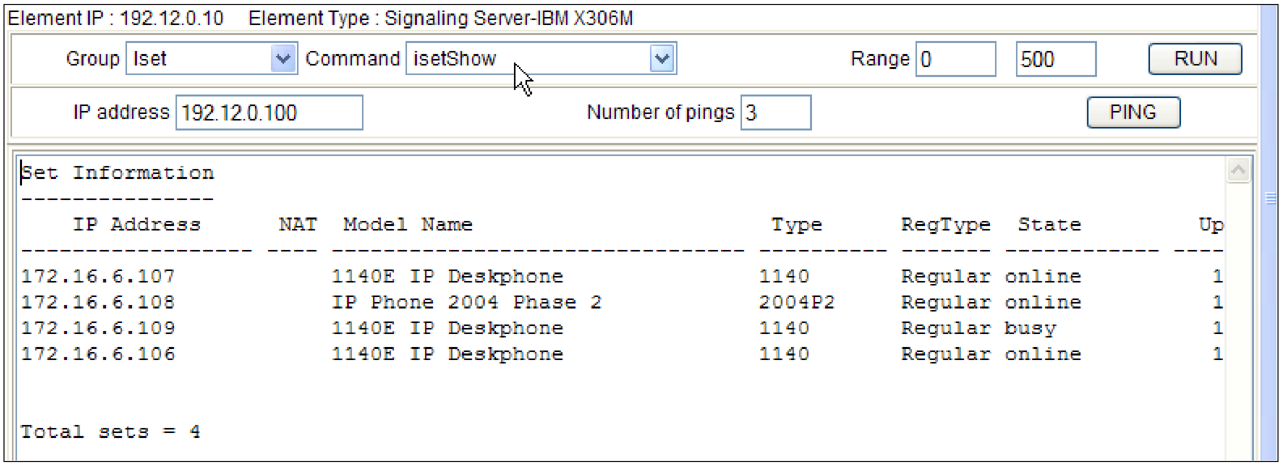
General Commands

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

Group: Sip
Command: SIPGwShownum
Sip
4094
IP address: 192.12.0.100
Number of pings: 3

```
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.



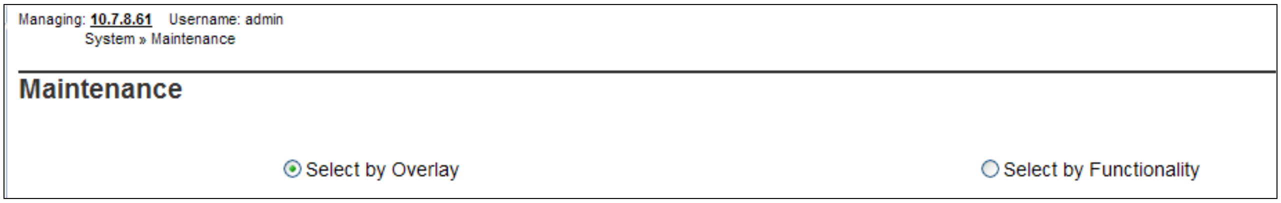
Element IP : 192.12.0.10 Element Type : Signaling Server-IBM X306M

Group: Iset
Command: isetShow
Range: 0 500
IP address: 192.12.0.100
Number of pings: 3

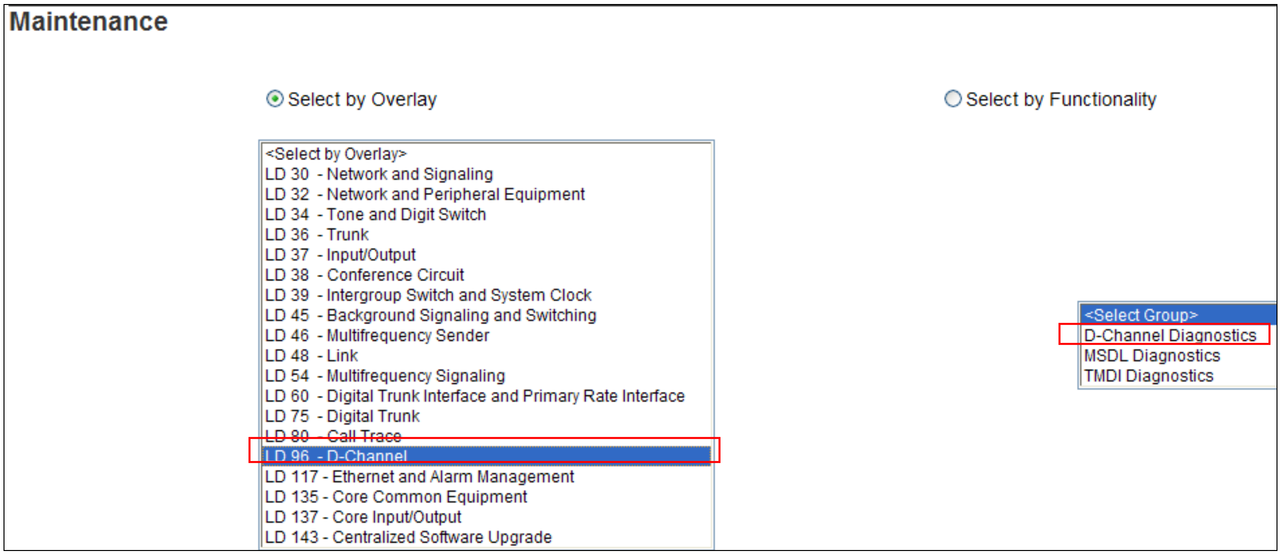
```
Set Information
---------------
    IP Address      NAT  Model Name                       Type      RegType  State         Up
------------------ ---- -------------------------------- ---------- ------- ------------ ----
172.16.6.107            1140E IP Deskphone               1140       Regular online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


Total sets = 4
```

9.1.2 System Maintenance Commands

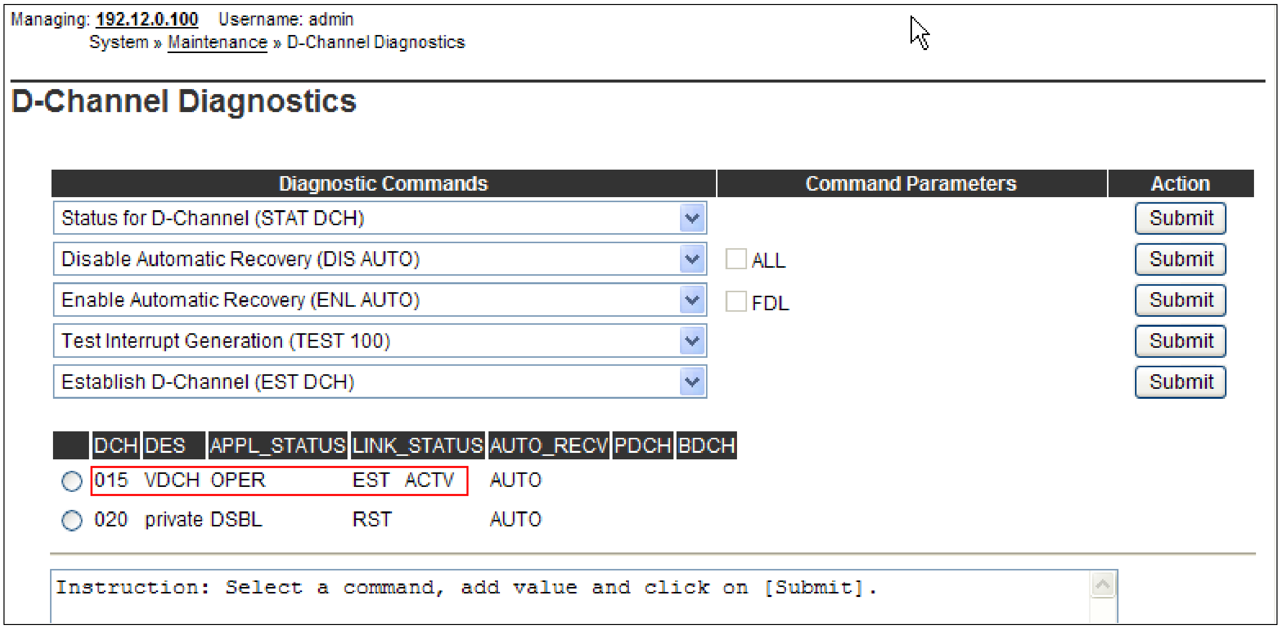
A variety of system maintenance commands are available by navigating to **System → Maintenance** using Element Manager. The user can navigate the maintenance commands using either the "**Select by Overlay**" approach or the "**Select by Functionality**" approach.


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)
Disable Automatic Recovery (DIS AUTO)
Enable Automatic Recovery (ENL AUTO)
Test Interrupt Generation (TEST 100)
Establish D-Channel (EST DCH)
☐ ALL
☐ FDL
Submit
Submit
Submit
Submit
Submit

	DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
○	015	VDCH	OPER	EST ACTV	AUTO		
○	020	private	DSBL	RST	AUTO		

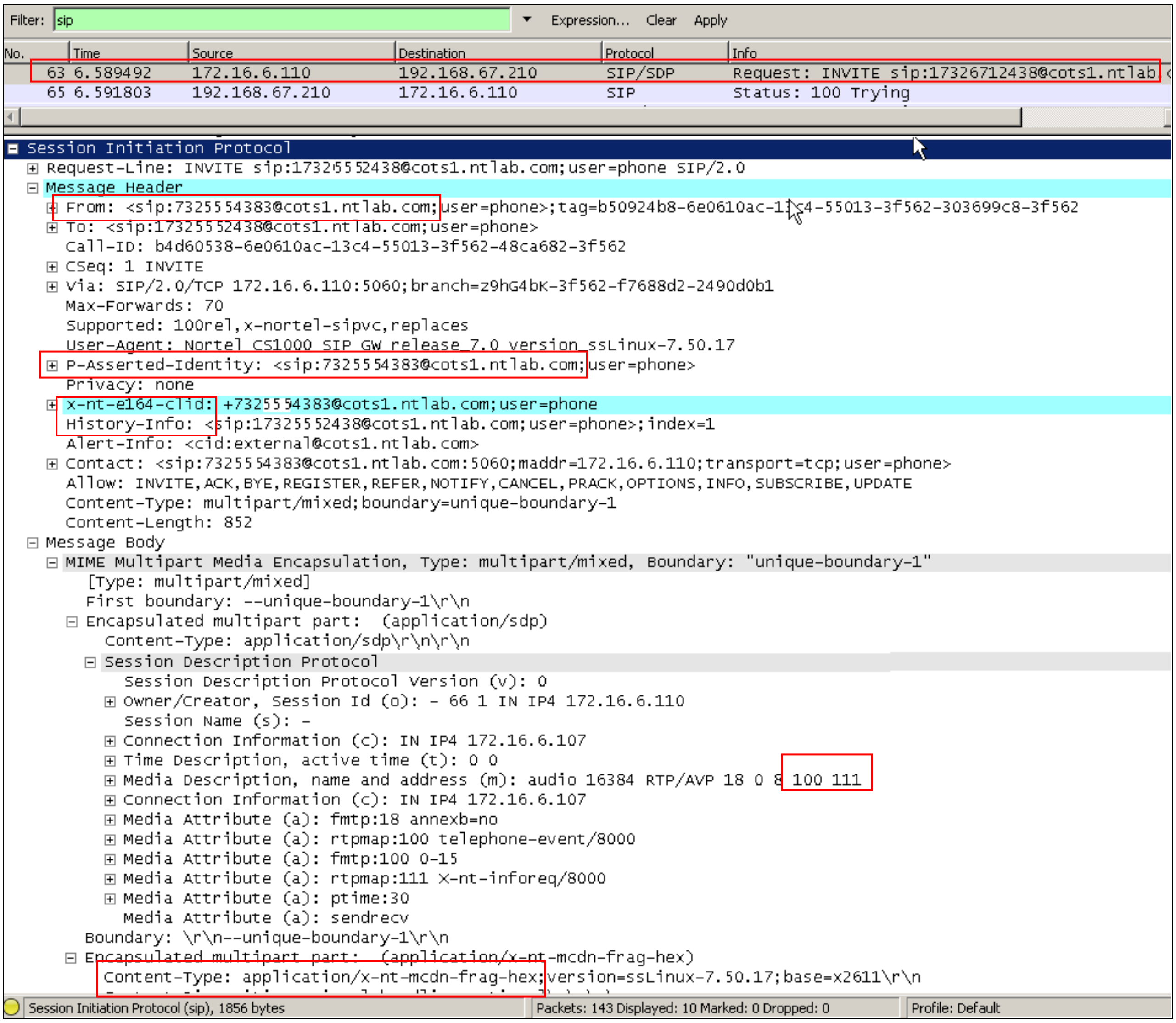
Instruction: Select a command, add value and click on [Submit].

9.2. Wireshark Verifications

This section illustrates an example outbound call from an Avaya CS1000E 1140E IP UNIStim user with Directory Number 4095 to PSTN.

The following screen capture shows a Wireshark trace captured on the CPE private network, filtered on SIP messages. The INVITE message sent by Avaya CS1000E to Session Manager is selected. As can be observed in the example below:

- Avaya CS1000E sends the calling station's associated AT&T DID number **17325554383** (see **Section 5.9**) in SIP headers such as the From and P-Asserted-Identity headers.
- Avaya CS1000E proprietary headers such as "**x-nt-e164-clid**" can be observed, and such headers will be removed by the Avaya SBCE.
- Avaya CS1000E is sending RFC2833 Telephone event types **100** and **111**. The 111 telephone event will be removed by the Avaya SBCE.
- Avaya CS1000E **MIME** headers can be observed in the Message Body and will be removed by Session Manager.
- The **History-Info** header will be removed by Avaya SBCE.



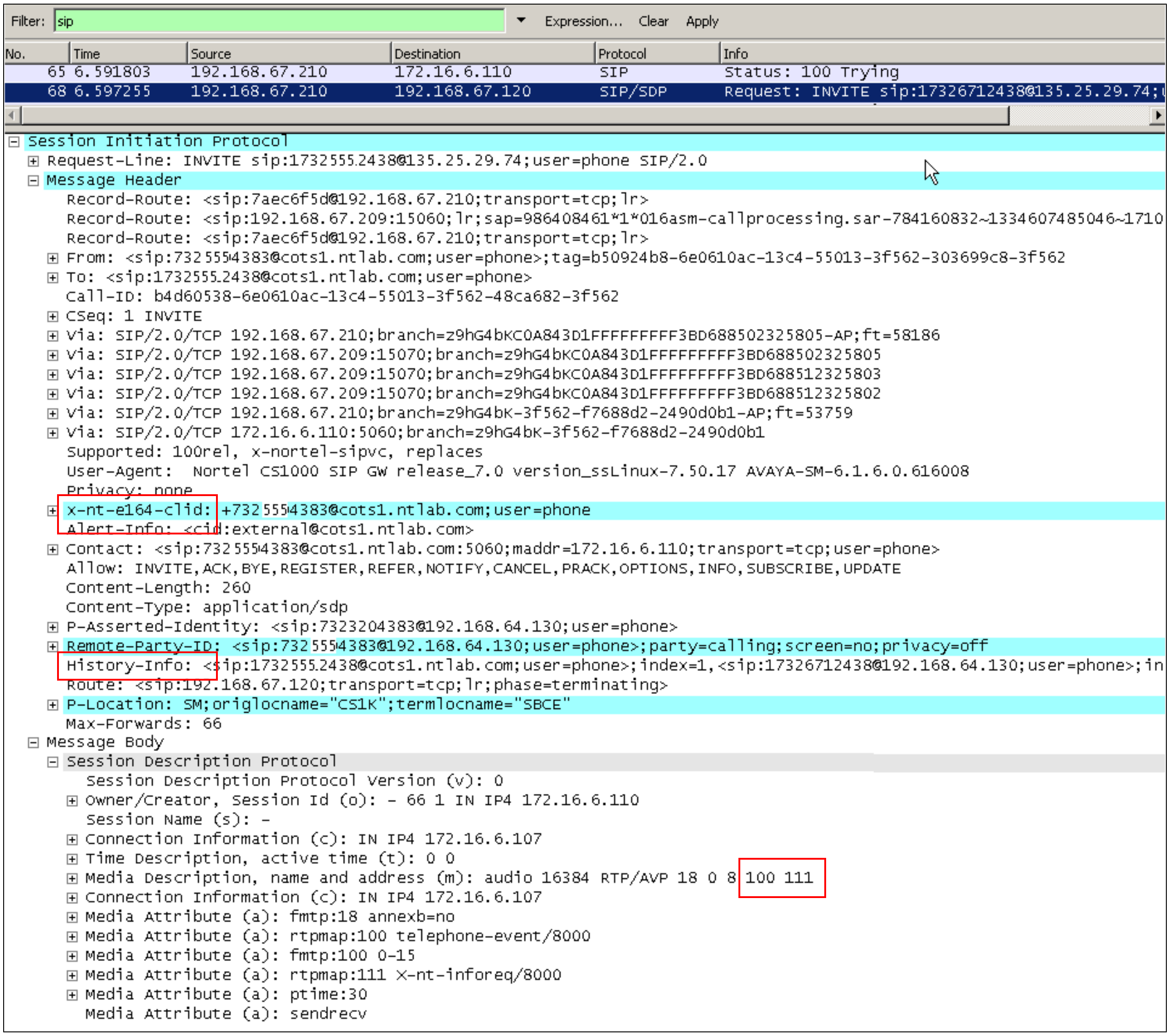
```
No.  Time      Source          Destination     Protocol  Info
  63 6.589492  172.16.6.110    192.168.67.210  SIP/SDP   Request: INVITE sip:17326712438@cots1.ntlab
  65 6.591803  192.168.67.210  172.16.6.110    SIP       Status: 100 Trying
```

```
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:17325552438@cots1.ntlab.com;user=phone SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:7325554383@cots1.ntlab.com;user=phone>;tag=b50924b8-6e0610ac-13c4-55013-3f562-303699c8-3f562
    ⊞ To: <sip:17325552438@cots1.ntlab.com;user=phone>
      Call-ID: b4d60538-6e0610ac-13c4-55013-3f562-48ca682-3f562
    ⊞ CSeq: 1 INVITE
    ⊞ Via: SIP/2.0/TCP 172.16.6.110:5060;branch=z9hG4bK-3f562-f7688d2-2490d0b1
      Max-Forwards: 70
      Supported: 100rel,x-nortel-sipvc,replaces
      User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
    ⊞ P-Asserted-Identity: <sip:7325554383@cots1.ntlab.com;user=phone>
      Privacy: none
    ⊞ x-nt-e164-clid: +7325554383@cots1.ntlab.com;user=phone
      History-Info: <sip:17325552438@cots1.ntlab.com;user=phone>;index=1
      Alert-Info: <cid:external@cots1.ntlab.com>
    ⊞ Contact: <sip:7325554383@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: multipart/mixed;boundary=unique-boundary-1
      Content-Length: 852
  ⊟ Message Body
    ⊟ MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "unique-boundary-1"
        [Type: multipart/mixed]
        First boundary: --unique-boundary-1\r\n
      ⊟ Encapsulated multipart part:  (application/sdp)
          Content-Type: application/sdp\r\n\r\n
        ⊟ Session Description Protocol
            Session Description Protocol Version (v): 0
          ⊞ Owner/Creator, Session Id (o): - 66 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 0 8 100 111
          ⊞ 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-inforeq/8000
          ⊞ Media Attribute (a): ptime:30
            Media Attribute (a): sendrecv
        Boundary: \r\n--unique-boundary-1\r\n
      ⊟ Encapsulated multipart part:  (application/x-nt-mcdn-frag-hex)
          Content-Type: application/x-nt-mcdn-frag-hex;version=ssLinux-7.50.17;base=x2611\r\n
```

Session Initiation Protocol (sip), 1856 bytes
Packets: 143 Displayed: 10 Marked: 0 Dropped: 0
Profile: Default

The following screen capture shows the subsequent INVITE message sent by Session Manager to Avaya SBCE. As can be observed in the example below:

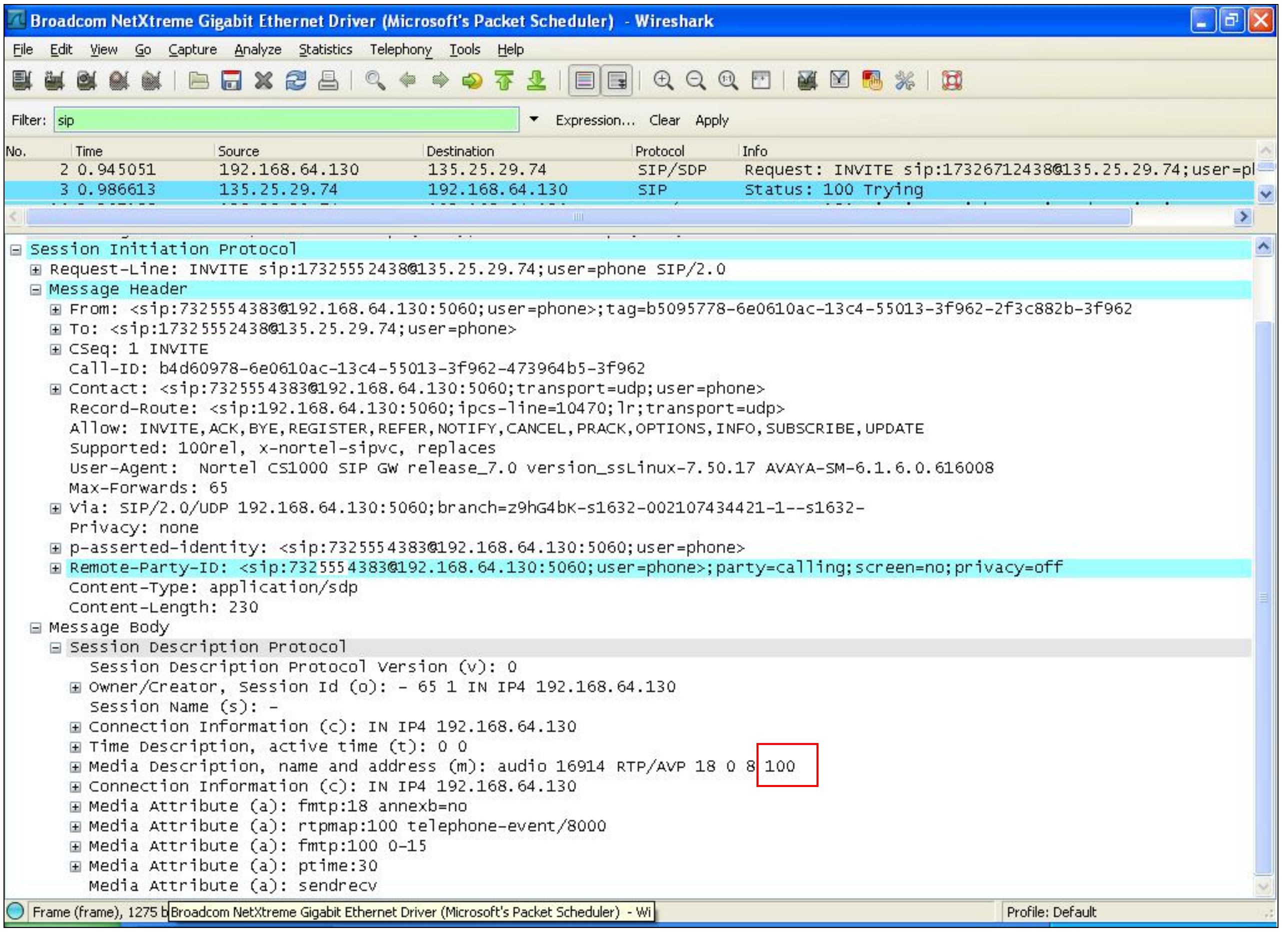
- The Avaya CS1000E proprietary header "**x-nt-e164-clid**" can be observed, and will be removed by the Avaya SBCE.
- The RFC2833 Telephone event types **100** and **111** both remain. The 111 telephone event will be removed by the Avaya SBCE.
- Avaya CS1000E **MIME** headers have been removed from the Message Body.
- The **History-Info** header will be removed by Avaya SBCE.



```
No.  Time      Source          Destination     Protocol  Info
 65 6.591803  192.168.67.210  172.16.6.110    SIP       Status: 100 Trying
 68 6.597255  192.168.67.210  192.168.67.120  SIP/SDP   Request: INVITE sip:17326712438@135.25.29.74;

⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:1732555.2438@135.25.29.74;user=phone SIP/2.0
  ⊟ Message Header
      Record-Route: <sip:7aec6f5d@192.168.67.210;transport=tcp;lr>
      Record-Route: <sip:192.168.67.209:15060;lr;sap=986408461*1*016asm-callprocessing.sar-784160832~1334607485046~1710
      Record-Route: <sip:7aec6f5d@192.168.67.210;transport=tcp;lr>
    ⊞ From: <sip:732 5554383@cots1.ntlab.com;user=phone>;tag=b50924b8-6e0610ac-13c4-55013-3f562-303699c8-3f562
    ⊞ To: <sip:1732555.2438@cots1.ntlab.com;user=phone>
      Call-ID: b4d60538-6e0610ac-13c4-55013-3f562-48ca682-3f562
    ⊞ CSeq: 1 INVITE
    ⊞ Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bKC0A843D1FFFFFFFFF3BD688502325805-AP;ft=58186
    ⊞ Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKC0A843D1FFFFFFFFF3BD688502325805
    ⊞ Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKC0A843D1FFFFFFFFF3BD688512325803
    ⊞ Via: SIP/2.0/TCP 192.168.67.209:15070;branch=z9hG4bKC0A843D1FFFFFFFFF3BD688512325802
    ⊞ Via: SIP/2.0/TCP 192.168.67.210;branch=z9hG4bK-3f562-f7688d2-2490d0b1-AP;ft=53759
    ⊞ Via: SIP/2.0/TCP 172.16.6.110:5060;branch=z9hG4bK-3f562-f7688d2-2490d0b1
      Supported: 100rel, x-nortel-sipvc, replaces
      User-Agent:  Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-6.1.6.0.616008
      Privacy: none
    ⊞ x-nt-e164-clid: +732 5554383@cots1.ntlab.com;user=phone
      Alert-Info: <cid:external@cots1.ntlab.com>
    ⊞ Contact: <sip:732 5554383@cots1.ntlab.com:5060;maddr=172.16.6.110;transport=tcp;user=phone>
      Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
      Content-Length: 260
      Content-Type: application/sdp
    ⊞ P-Asserted-Identity: <sip:7323204383@192.168.64.130;user=phone>
    ⊞ Remote-Party-ID: <sip:732 5554383@192.168.64.130;user=phone>;party=calling;screen=no;privacy=off
      History-Info: <sip:1732555.2438@cots1.ntlab.com;user=phone>;index=1,<sip:17326712438@192.168.64.130;user=phone>;in
      Route: <sip:192.168.67.120;transport=tcp;lr;phase=terminating>
    ⊞ P-Location: SM;origlocname="CS1K";termlocname="SBCE"
      Max-Forwards: 66
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): - 66 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 0 8 100 111
      ⊞ 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-inforeq/8000
      ⊞ Media Attribute (a): ptime:30
        Media Attribute (a): sendrecv
```

The following screen capture shows the subsequent INVITE message sent by Avaya SBCE to the AT&T border element. As can be observed in the example below:

- The Avaya CS1000E proprietary header "**x-nt-e164-clid**" was removed by the Avaya SBCE.
- The **111** telephone event was removed by Avaya SBCE.
- The **History-Info** header was removed by Avaya SBCE.


Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

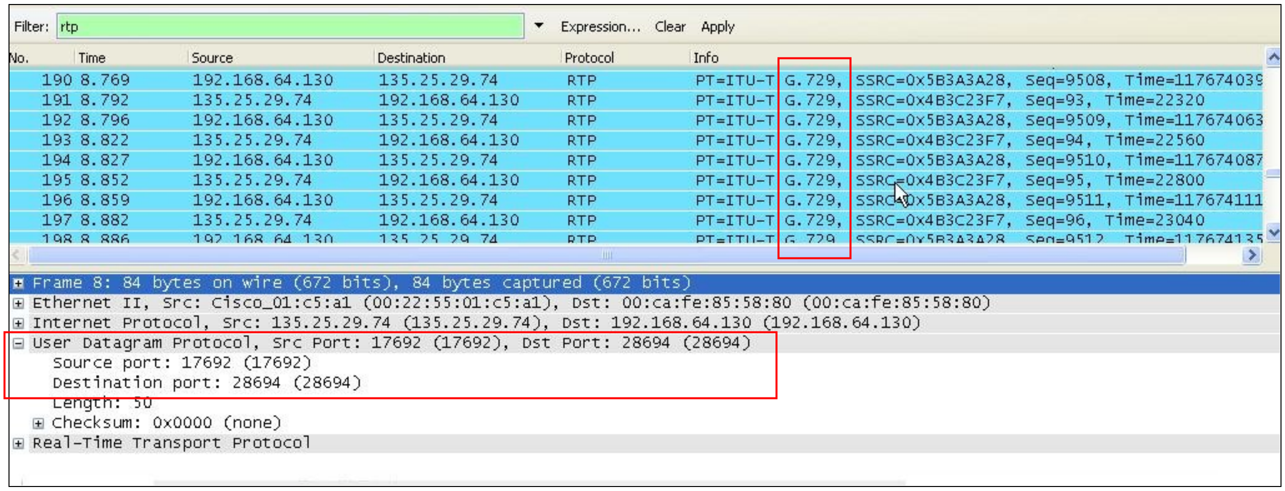
Filter: sip

```
No.   Time        Source            Destination      Protocol   Info
    2 0.945051    192.168.64.130    135.25.29.74     SIP/SDP    Request: INVITE sip:17326712438@135.25.29.74;user=pl
    3 0.986613    135.25.29.74      192.168.64.130   SIP        Status: 100 Trying
```

```
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:17325552438@135.25.29.74;user=phone SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:7325554383@192.168.64.130:5060;user=phone>;tag=b5095778-6e0610ac-13c4-55013-3f962-2f3c882b-3f962
    ⊞ To: <sip:17325552438@135.25.29.74;user=phone>
    ⊞ CSeq: 1 INVITE
      Call-ID: b4d60978-6e0610ac-13c4-55013-3f962-473964b5-3f962
    ⊞ Contact: <sip:7325554383@192.168.64.130:5060;transport=udp;user=phone>
      Record-Route: <sip:192.168.64.130:5060;ipcs-line=10470;lr;transport=udp>
      Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
      Supported: 100rel, x-nortel-sipvc, replaces
      User-Agent:  Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-6.1.6.0.616008
      Max-Forwards: 65
    ⊞ Via: SIP/2.0/UDP 192.168.64.130:5060;branch=z9hG4bK-s1632-002107434421-1--s1632-
      Privacy: none
    ⊞ p-asserted-identity: <sip:7325554383@192.168.64.130:5060;user=phone>
    ⊞ Remote-Party-ID: <sip:7325554383@192.168.64.130:5060;user=phone>;party=calling;screen=no;privacy=off
      Content-Type: application/sdp
      Content-Length: 230
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): - 65 1 IN IP4 192.168.64.130
        Session Name (s): -
      ⊞ Connection Information (c): IN IP4 192.168.64.130
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 16914 RTP/AVP 18 0 8 100
      ⊞ Connection Information (c): IN IP4 192.168.64.130
      ⊞ 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): ptime:30
        Media Attribute (a): sendrecv
```

Frame (frame), 1275 b
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler) - Wi
Profile: Default

Changing the display filter to **rtp**, the media streams for this call are displayed. Note that the UDP ports used are within the range defined in **Section 7.6.2**. Also note that G.729 was the codec used.



Filter: rtp

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

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

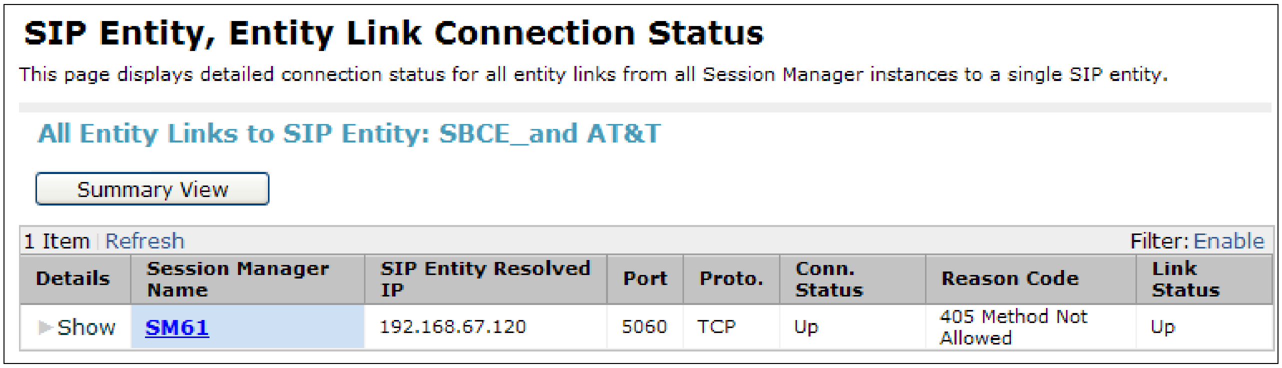
9.3. System Manager and Session Manager Verification

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

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_and AT&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.



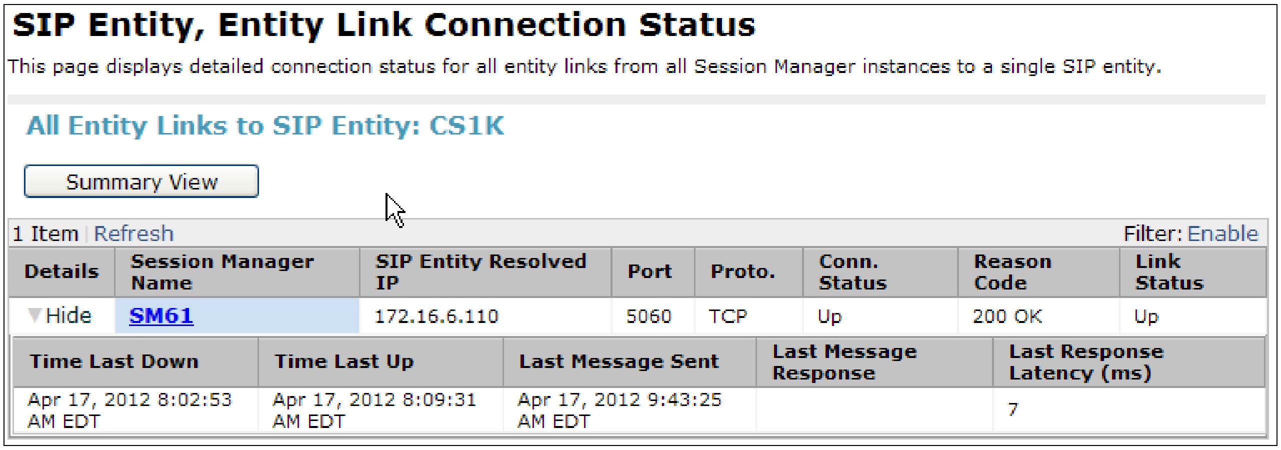
SIP Entity, Entity Link Connection Status

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

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

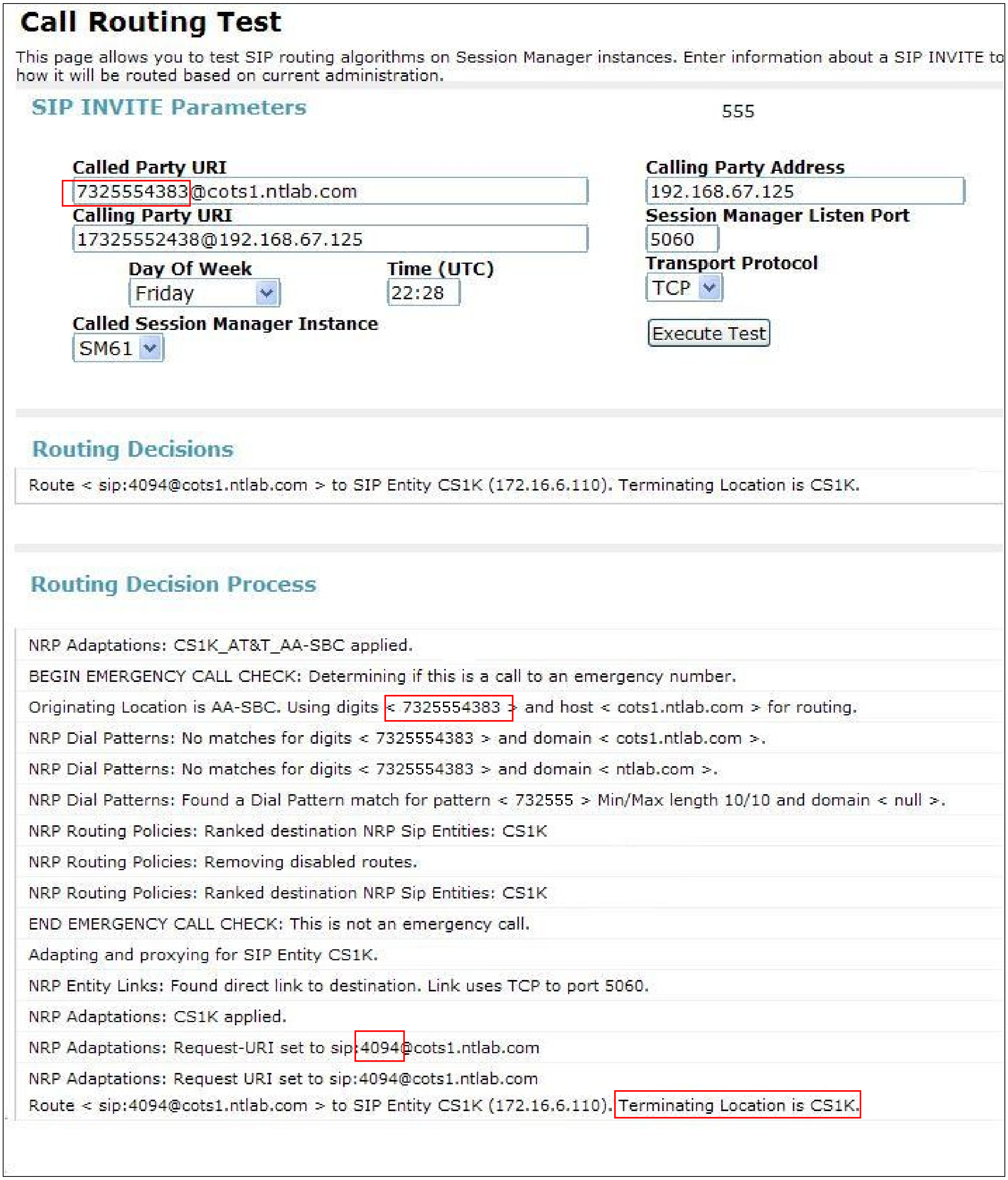
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM61	172.16.6.110	5060	TCP	Up	200 OK	Up

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 AvayaCS1000E 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 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 URI: 17325552438@192.168.67.125
Day Of Week: Friday
Time (UTC): 22:28
Called Session Manager Instance: SM61
Calling Party Address: 192.168.67.125
Session Manager Listen Port: 5060
Transport Protocol: TCP

Routing Decisions

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

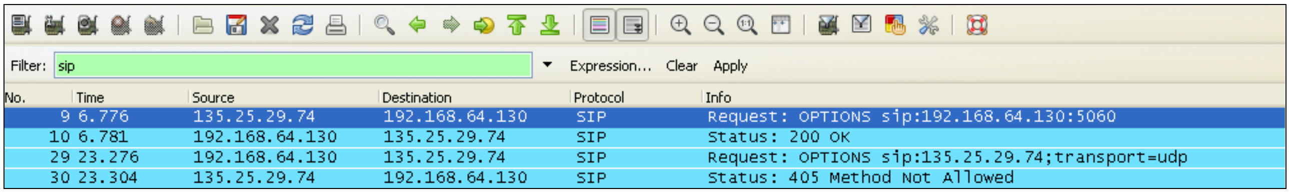
Routing Decision Process

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. Avaya Aura® Session Border Controller Verification

9.4.1 Verify Sipera SBCE Connectivity to AT&T IP Flexible Reach

Verify that your entity links from Avaya SBCE (192.168.64.130) to AT&T IP Flexible Reach 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.



Filter: sip

```
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
```

9.4.2 Internal Tracing

Avaya SBCE can take internal traces of specified interfaces.

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

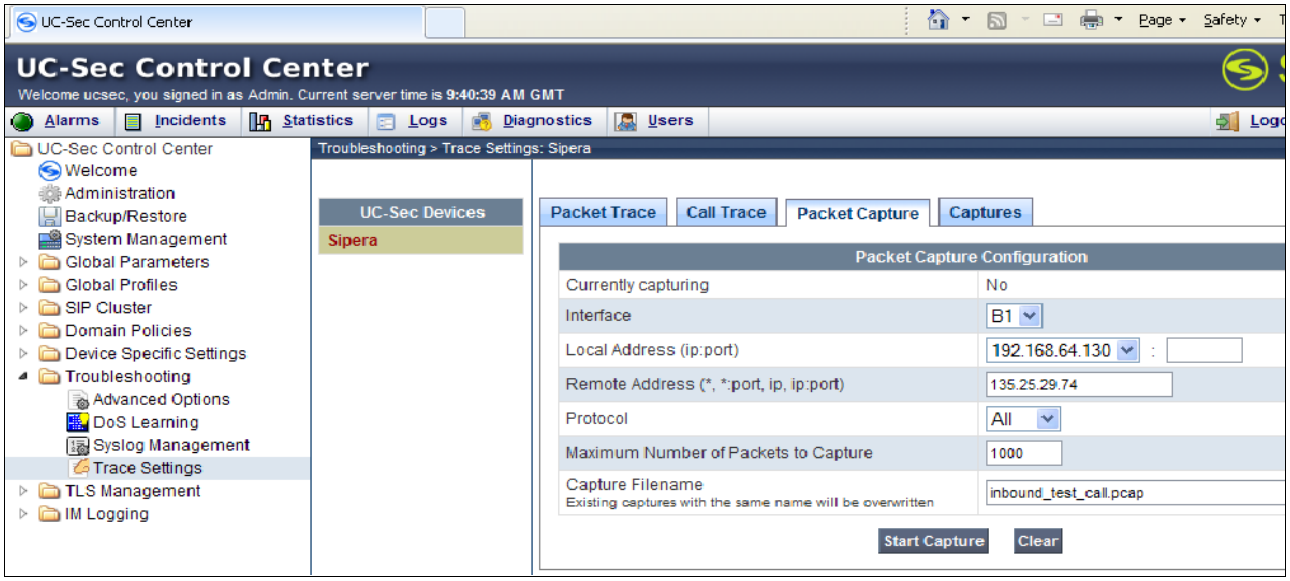
Step 2 - Select the **Packet Capture** tab and select the following:

a. Select the desired **Interface** from the drop down menu (e.g., B1, the interface to AT&T)

b. Specify the **Maximum Number of Packets to Capture** (.e.g., **1000**)

c. Specify a **Capture Filename**.

d. Click **Start Capture** to begin the trace.



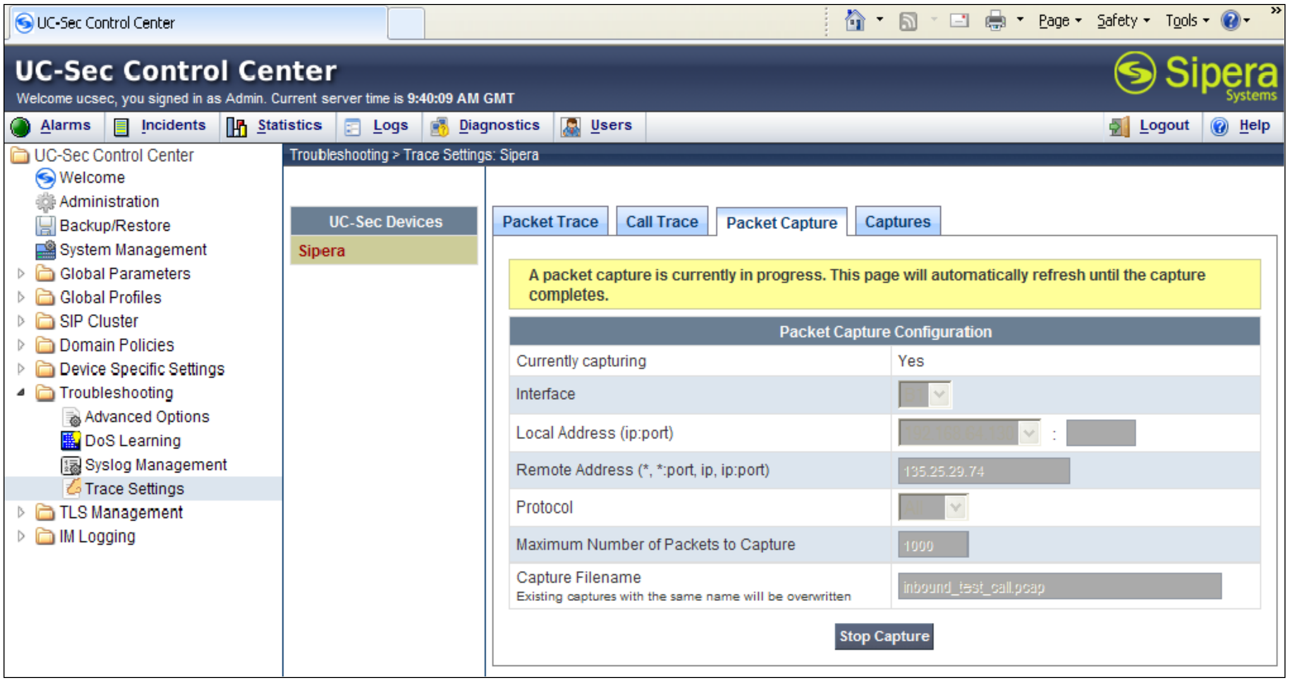
Welcome ucsec, you signed in as Admin. Current server time is 9:40:39 AM GMT

Troubleshooting > Trace Settings: Sipera

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 Existing captures with the same name will be overwritten	inbound_test_call.pcap

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



Welcome ucsec, you signed in as Admin. Current server time is 9:40:09 AM GMT

Troubleshooting > Trace Settings: Sipera

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

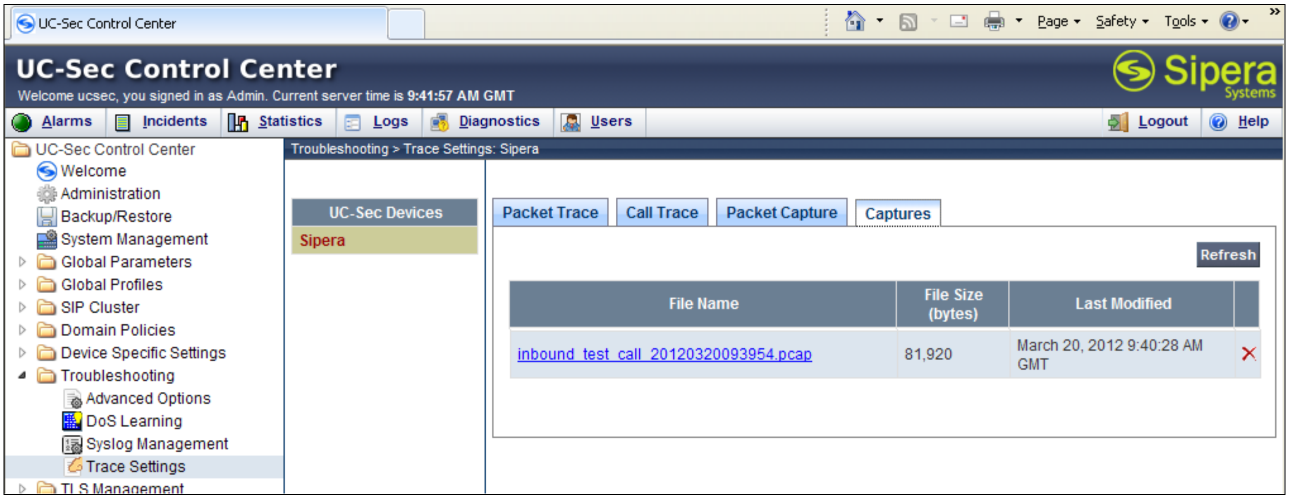
Packet Capture Configuration	
Currently capturing	Yes
Interface	B1
Local Address (ip:port)	192.168.64.130 :
Remote Address (*, *:port, ip, ip:port)	135.25.29.74
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename Existing captures with the same name will be overwritten	inbound_test_call.pcap

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.



Welcome ucsec, you signed in as Admin. Current server time is 9:41:57 AM GMT

Troubleshooting > Trace Settings: Sipera

File Name	File Size (bytes)	Last Modified	
inbound_test_call_20120320093954.pcap	81,920	March 20, 2012 9:40:28 AM GMT	✕

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server Release 7.5, Avaya Aura® Session Manager 6.1, and the Avaya Session Border Controller for Enterprise 4.0.5 can be configured to interoperate successfully with AT&T IP Flexible Reach service via either AVPN or MIS-PNT transport. This solution allows Avaya Communication Server 1000E user access to the PSTN using an AT&T IP Flexible Reach service connection.

11. References

This section references documentation relevant to these Applications.

11.1. Avaya

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

Avaya Aura® Session Manager/System Manager

[1] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Issue 4, 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] *Communication Server 1000 Release 7.0 and Acme Packet Net-Net 6.2.0 Configuration Guide For Use with AT&T IP Flexible Reach,* Issue 1.1, 4/12/2011 available at: http://support.avaya.com/css/P8/documents/100129069
[6] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313
[7] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116
[8] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02
[9] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509
[10] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125
[11] Avaya Call Pilot® information can be found at: http://support.avaya.com/css/Products/P0712

Avaya Session Border Controller for Enterprise

Current product documentation for UC-Sec can be obtained from the Sipera web site using the link at http://www.sipera.com.

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

11.2. AT&T IP Flexible Reach service.

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

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

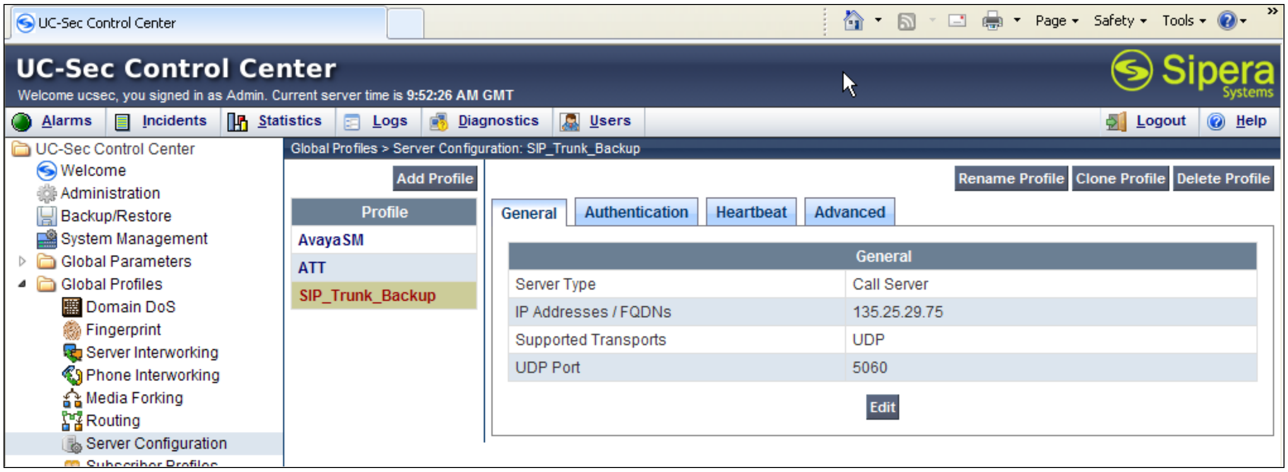
12. Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements

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 7.4.6**).

12.1.1 Configure the Secondary Location in Server Configuration

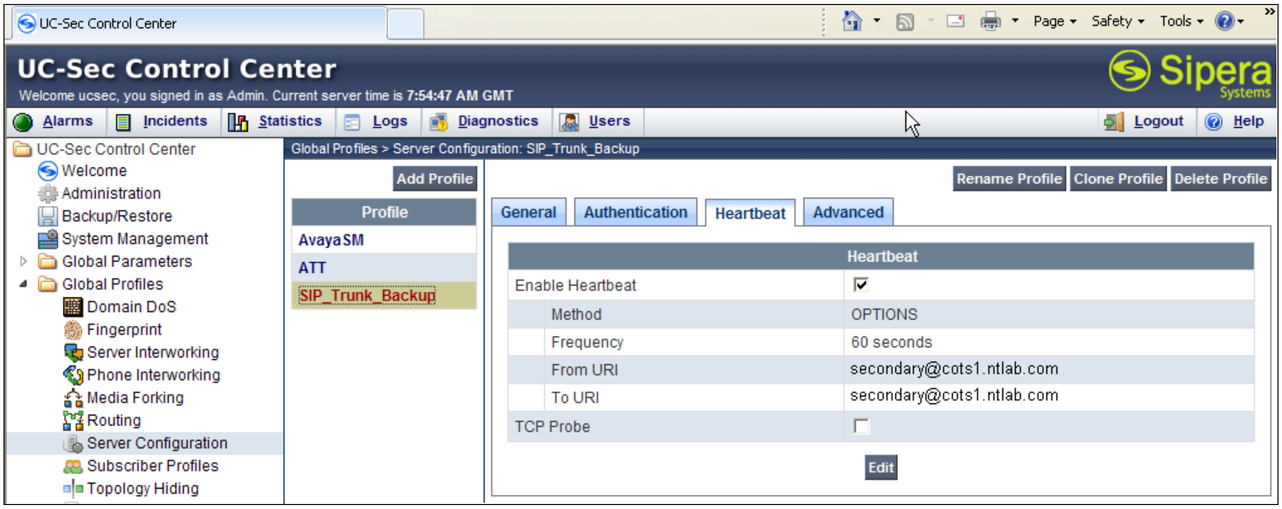
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
    a) **Name: SIP_Trunk_backup**
4. On the **Add Server Configuration Profile – General** Tab:
    a) Select Server Type**: Call Server**
    b) **IP Address: 135.25.29.75**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



Global Profiles > Server Configuration: SIP_Trunk_Backup

General	
Server Type	Call Server
IP Addresses / FQDNs	135.25.29.75
Supported Transports	UDP
UDP Port	5060

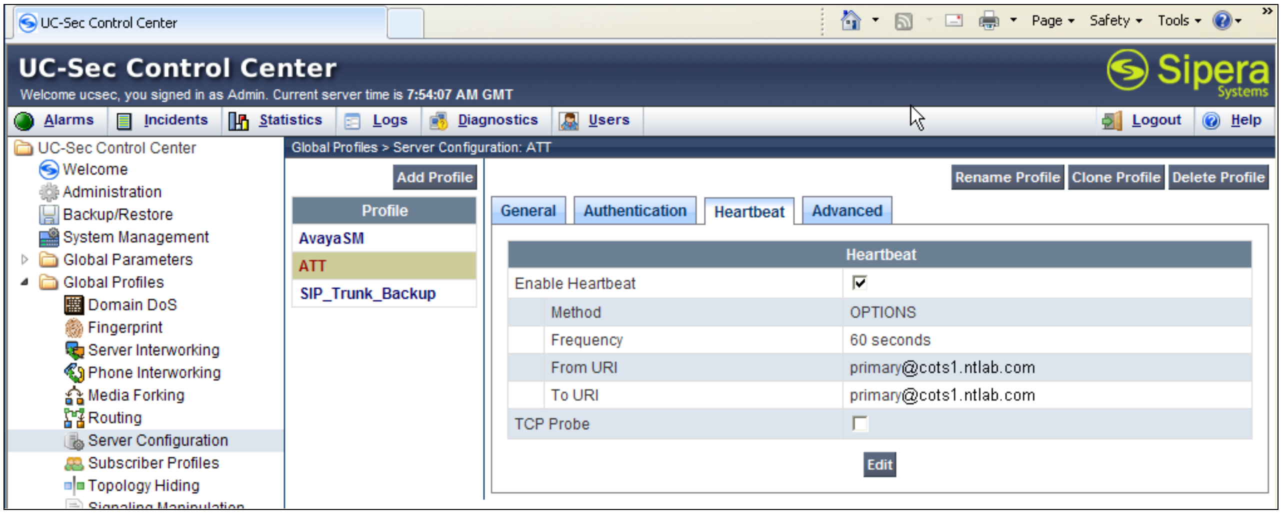
5. On the **Authentication** tab
    a) Select **Next**
6. On the **Heartbeat** tab (The Heartbeat must be enabled on the Primary trunk also)
    a) Check **Enable Heartbeat**
    b) **Method: OPTIONS**
    c) **Frequency: 60 seconds**
    d) **From URI: secondary@cots1.ntlab.com.com**
    e) **To URI: secondary@cots1.ntlab.com.com**
    f) Select **Next**



Global Profiles > Server Configuration: SIP_Trunk_Backup

Heartbeat	
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	secondary@cots1.ntlab.com
To URI	secondary@cots1.ntlab.com
TCP Probe	☐

7. On the **Advanced** Tab
   a) Click **Finish**
8. Select the Primary Trunk created in **Section 7.4.6** (e.g., **ATT**)
9. Select the **Heartbeat Tab**
10. Select **Edit**
11. Repeat **Steps 6 – 7**

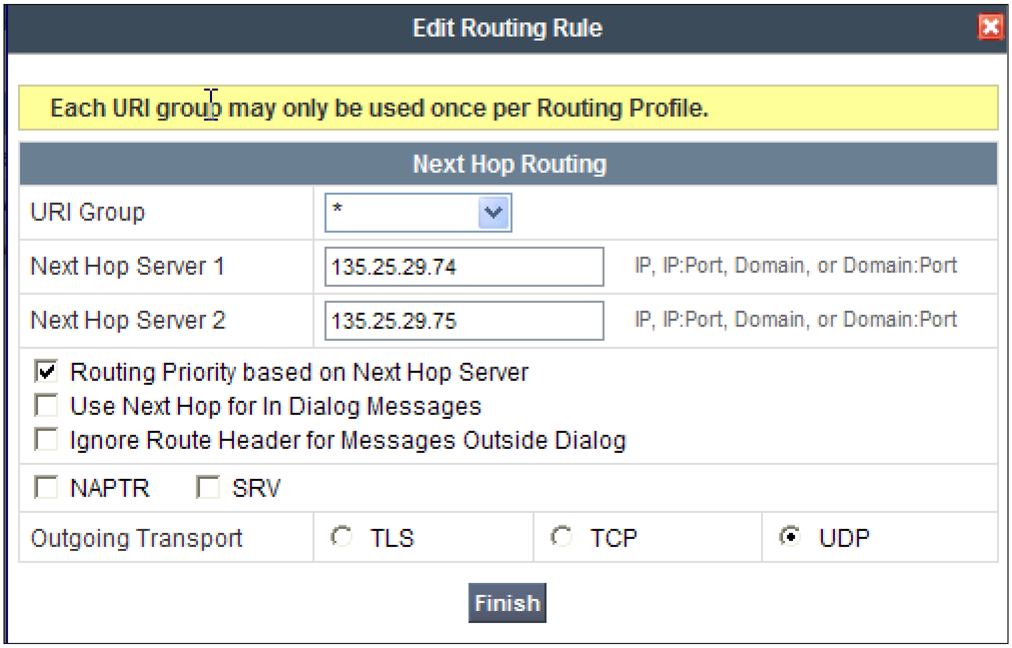


Global Profiles > Server Configuration: ATT

Heartbeat	
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	primary@cots1.ntlab.com
To URI	primary@cots1.ntlab.com
TCP Probe	☐

12.1.2 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**



Edit Routing Rule

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	135.25.29.75	IP, IP:Port, Domain, or Domain:Port

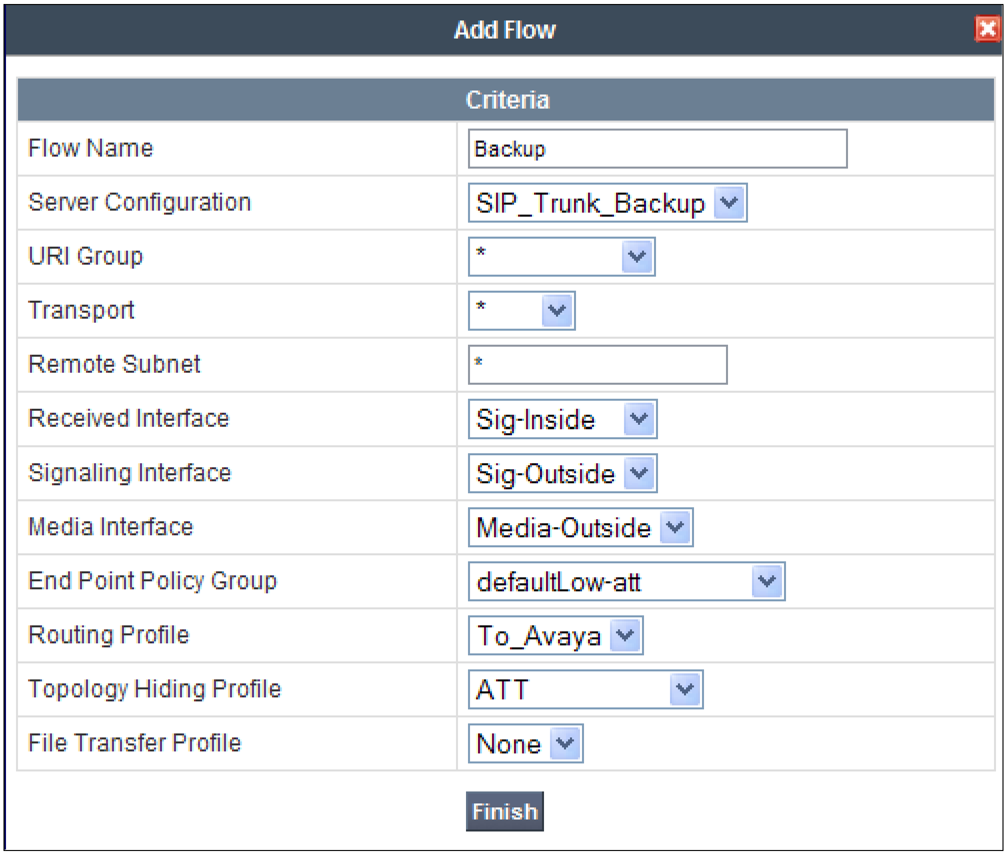
☑ Routing Priority based on Next Hop Server
☐ Use Next Hop for In Dialog Messages
☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

Outgoing Transport ○ TLS ○ TCP ● UDP

12.1.3 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**



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

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

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