



## Avaya Solution & Interoperability Test Lab

---

# Applications Notes for Avaya Communication Server 1000E Release 7.6 with Avaya Aura<sup>®</sup> Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 with AT&T IP Toll Free SIP Trunk Service – Issue 1.0

## Abstract

These Application Notes describe the steps for configuring Avaya Aura<sup>®</sup> Session Manager 6.3, Avaya Communication Server 1000E 7.6 and Avaya Session Border Controller for Enterprise 6.2 with the AT&T IP Toll Free service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura<sup>®</sup> Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Communication Server 1000E 7.6 is a telephony server, and is the point of connection between the enterprise endpoints and Avaya Aura<sup>®</sup> Session Manager. Avaya Session Border Controller for Enterprise 6.2 is the point of connection between Avaya Aura<sup>®</sup> Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability. In addition, Avaya Aura<sup>®</sup> Contact Center is used to provide Agent access for Avaya Communication Server 1000E

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

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

## **TABLE OF CONTENTS**

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing.....	6
2.2.	Test Results .....	6
2.2.1.	Known Limitations .....	6
2.3.	Support .....	8
2.3.1.	AT&T.....	8
2.3.2.	Avaya .....	8
3.	Reference Configuration .....	8
3.1.	Illustrative Configuration Information .....	10
3.2.	Call Flows .....	11
3.2.1.	Inbound Call to the Avaya CS1000E.....	11
3.2.2.	Coverage to Voicemail .....	12
4.	Equipment and Software Validated .....	13
5.	Configure Avaya Communication Server 1000E .....	14
5.1.	Logging In and Selecting the System Element .....	14
5.2.	Administer Telephony Node .....	15
5.2.1.	Node Information and IP Addresses .....	15
5.2.2.	Enable Terminal Proxy Server (TPS) .....	17
5.2.3.	Synchronize Configuration .....	18
5.3.	Voice Codecs.....	19
5.3.1.	IP Telephony Node Codec Configuration.....	19
5.3.2.	Media Gateway Codec Configuration .....	21
5.4.	Zones and Bandwidth Management.....	23
5.4.1.	Zone 5 – SIP Trunk.....	24
5.4.2.	Zone 3 – IP Telephones .....	25
5.5.	SIP Trunk Gateway .....	25
5.5.1.	Provision SIP Gateway .....	25
5.5.2.	Integrated Services Digital Network (ISDN).....	28
5.5.3.	Virtual D-Channel Configuration .....	28
5.5.4.	SIP Routes Configuration .....	30
5.5.5.	SIP Trunk Configuration to Session Manager .....	32
5.5.6.	Administer Virtual Super-Loop .....	36
5.6.	Routing of Inbound Numbers to CS1000E .....	36
5.7.	CS1000E Agent Access Provisioning.....	38
5.7.1.	CS1000E IP Agent Phone .....	38
5.7.2.	CS1000E Auto Call Distribution (ACD) .....	42
5.7.3.	CS1000E Control DN (CDN) .....	43
5.7.4.	Analog Fax Line .....	44
5.8.	Customer Information .....	44
5.8.1.	Caller ID Provisioning .....	44
5.9.	Changing RFC2833 DTMF Telephone Event Type .....	47
5.10.	Inbound Calls to Call Pilot® .....	48

5.11.	Configuration Backup.....	49
6.	Configure Avaya Aura® Session Manager .....	50
6.1.	SIP Domain .....	51
6.2.	Locations .....	52
6.2.1.	Location for CS1000E Subnet .....	52
6.2.2.	Location for Customer Premises Equipment Subnet.....	54
6.3.	Configure Adaptations .....	54
6.3.1.	Adaptation for Traffic to CS1000E.....	55
6.3.2.	Adaptation for Traffic from CS1000E to AT&T .....	56
6.4.	SIP Entities .....	57
6.4.1.	SIP Entity for Session Manager .....	57
6.4.2.	SIP Entity for CS1000E .....	58
6.4.3.	SIP Entity for Avaya SBCE.....	59
6.5.	Entity Links .....	60
6.5.1.	Entity Link to CS1000E.....	60
6.5.2.	Entity Link to Avaya SBCE.....	60
6.6.	Routing Policies .....	61
6.6.1.	Routing Policy to CS1000E .....	61
6.6.2.	Routing Policy to Avaya SBCE.....	62
6.7.	Dial Patterns .....	63
6.7.1.	Inbound AT&T calls to CS1000E Extensions .....	63
7.	Avaya Aura® Contact Center.....	65
7.1.	Create Avaya Aura® Contact Center Agent .....	65
7.2.	Verify Control DN (CDN) and Agent Connection Status.....	67
7.2.1.	CDN Connection status.....	67
7.2.2.	Agent Connection status .....	67
8.	Configure Avaya Session Border Controller for Enterprise .....	68
8.1.	Initial Installation/Provisioning.....	68
8.2.	Log into the Avaya SBCE.....	68
8.3.	Global Profiles.....	69
8.3.1.	Server Interworking – Avaya Side.....	69
8.3.2.	Server Interworking – AT&T Side .....	70
8.3.3.	Routing – Avaya Side .....	70
8.3.4.	Routing – AT&T Side.....	71
8.3.5.	Server Configuration –Session Manager .....	71
8.3.6.	Server Configuration –AT&T Primary Border Element .....	72
8.3.7.	Topology Hiding – Avaya Side .....	73
8.3.8.	Topology Hiding – AT&T Side.....	74
8.3.9.	Signaling Manipulation.....	75
8.4.	Domain Policies .....	78
8.4.1.	Application Rules.....	78
8.4.2.	Media Rules .....	78
8.4.3.	Signaling Rules .....	79
8.4.4.	Endpoint Policy Groups – Avaya .....	82

8.4.5.	Endpoint Policy Groups – AT&T .....	83
8.5.	Device Specific Settings.....	84
8.5.1.	Network Management.....	84
8.5.2.	Media Interface .....	84
8.5.3.	Signaling Interface .....	85
8.5.4.	Endpoint Flows – Avaya (Session Manager).....	85
8.5.5.	Endpoint Flows – AT&T Primary .....	86
9.	Verification Steps.....	87
9.1.	General .....	87
9.2.	Avaya CS1000E Verifications .....	87
9.2.1.	IP Network Maintenance and Reports Commands .....	87
9.2.2.	System Maintenance Commands.....	89
9.3.	System Manager / Session Manager Verification .....	90
9.3.1.	Verify Service State and Entity Link Status .....	90
9.3.2.	Call Routing Test .....	91
9.4.	Protocol Traces.....	92
9.5.	Avaya Session Border Controller for Enterprise Verification .....	96
9.5.1.	Verify Avaya SBCE Connectivity to AT&T IP Toll Free.....	96
9.5.2.	Internal Tracing.....	96
10.	Conclusion .....	98
11.	References.....	99
11.1.	Avaya.....	99
12.	Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements.....	101
12.1.1.	Configure the Secondary Border Element Server Configuration.....	101
12.1.2.	Add Secondary Border Element IP Address to Routing .....	102
12.1.3.	Configure Secondary AT&T Border Element End Point Flow .....	103

# 1. Introduction

These Application Notes describe the steps for configuring Avaya Aura<sup>®</sup> Session Manager 6.3 (referred to in subsequent sections of this document as Session Manager), Avaya Communication Server 1000E 7.6 (referred to in subsequent sections of this document as CS1000E), and Avaya Session Border Controller for Enterprise 6.2 (referred to in subsequent sections of this document as Avaya SBCE) with the AT&T IP Toll Free service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura<sup>®</sup> Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura<sup>®</sup> Session Manager is provisioned using the Avaya Aura<sup>®</sup> System Manager 6.3.5 platform (referred to in subsequent sections of this document as System Manager). Avaya Communication Server 1000E 7.6 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura<sup>®</sup> Session Manager.

In addition, Avaya Call Pilot<sup>®</sup> is used in conjunction with the Avaya Communication Server 1000E to provide voice mail access, as well as Avaya Aura<sup>®</sup> Contact Center which provide Agents access functionality. While both of these platforms are discussed in the following sections, their provisioning is beyond the scope of this document.

An Avaya Session Border Controller for Enterprise 6.2 is the point of connection between Avaya Aura<sup>®</sup> Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability. In addition, Avaya Aura<sup>®</sup> Contact Center is used to provide Agent access for Avaya Communication Server 1000E

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT<sup>1</sup> transport.

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

## 2. General Test Approach and Test Results

The test environment consisted of:

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

---

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

## 2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2** for examples) between Session Manager, CS1000E, Avaya SBCE, and the AT&T IP Toll Free service.

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

- SIP trunking.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- PBX and AT&T IP Toll Free service features such as hold, resume, conference and transfer.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing were also tested.

## 2.2. Test Results

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

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

### 2.2.1. Known Limitations

1. **CS1000E responds with *ptime:10* in response to *maxptime:30*** – AT&T sends INVITEs with the SIP parameter *maxptime:30*. In response, CS1000E will send *ptime:10* for any UNISTim or Digital stations. This is a known issue. The AT&T AVPN transport service recommends 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 CS1000E respond with *ptime:30* as recommended (see **Sections 5.3.1, 5.3.2, and 8.3.9**).

2. **Removal of SIP Headers** – Depending on the call flow and the endpoints involved, the CS1000E and/or Session Manager may send multiple SIP headers that are not used by AT&T. In addition the AT&T IP Toll Free network does not support the History-Info header. Therefore in the interest of reducing packet overhead, the following headers are removed:
  - MIME type headers are removed by Session Manager Adaptations (see **Section 6.3.2**).
  - The Avaya SBCE is configured to remove the following SIP headers (see **Section 8.4.3**):
    - Alert-Info, x-nt-e164-clid, History-Info, Remote-Party-ID, Resource-Priority, AV-Global-Session-ID, P-AV-Message-ID, and P-Location.
3. **Telephone Events 101 and 111** - The CS1000E uses Telephone Event type 101 by default. This value is changed to the AT&T recommended value of 100 in the CS1000E (see **Section 5.9**). In addition, Telephone event type 111 is also sent by the CS1000E. This value is removed by the Avaya SBCE (see **Section 8.3.9**).
  - Note that the 1140E SIP telephones use a value of 101 for their RFC2833 Telephone Event Type, however no issues were found when 101 was used.
4. **G.726 codec is not supported by CS1000E.**
5. **The CS1000E may not populate the PAI header correctly in response to inbound calls.** In the reference configuration, the AT&T IP Toll Free service sends specific DNIS numbers in the R-URI sent to the Customer Premises Equipment (CPE). The AT&T IP Toll Free service prefers that the PAI and Contact headers sent in any subsequent CPE responses or requests contain these DNIS numbers as well. In addition, while the AT&T IP Toll Free service sends unique DNIS numbers in the INVITE Request URI (R-URI), it will send the same customer billing number in all TO headers. The CS100E Incoming Digit Translation table (IDT) is used to convert these DNIS digits to their associated local extensions. During testing it was found that the CS1000E may populate subsequent PAI headers with the associated destination extension, instead of the desired DNIS digits.
  - The workaround is to have the Avaya SBCE copy the DNIS number from the R-URI and insert it into the TO header prior to sending the INVITE to Session Manager/CS1000E, (the Avaya SBCE reinserts the billing number into the TO header prior to sending the messages back to AT&T). As a result, the CS1000E will populate the PAI with the associated AT&T IP Toll Free DNIS number.
  - It was also found that for inbound calls placed directly to the Call Pilot<sup>®</sup> main extension, the associated DNIS number in the R-URI/TO headers must also be defined in Call Pilot<sup>®</sup> as a Service Directory Number (see **Section 5.10**).
    - A CS1000E MR has been opened.
6. **Avaya SBCE support of T.38** – During testing it was found that the current Avaya SBCE GA load (6.2 Q58) had an issue with T.38 fax. As a result, the use of Avaya SBCE load 6.2 Q48 is recommended at this time, if T.38 fax is required (see **Section 4**).
  - An Avaya SBCE MR was opened.

7. **Fax support** - G.711 and T.38 fax is supported (see **Item 6** above), and the sender and receiver of a fax call may use either Group 3 or Super Group 3 fax machines. However the T.38 fax protocol carries all fax transmissions as Group 3. Fax speeds of 14400, with Error Correction Mode, were observed in the reference configuration.

## 2.3. Support

### 2.3.1. AT&T

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

### 2.3.2. Avaya

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. In the United States, (866) GO-Avaya (866-462-8292) provides access to overall sales and service support menus.

## 3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** and consists of the following:

- The CS1000E system provides the voice communications services for the enterprise site. The system is comprised of:
  - The MG1000E Gateway containing:
    - Call Server (CPPM).
    - Media Gateway Controller (MGC), which provides Digital Signaling Processor (DSP) resources.
    - Meridian Integration Recorded Announcement (MIRAN) card used for Music on Hold.
    - Avaya Call Pilot<sup>®</sup> messaging application.
  - IBM 306M Consumer Off the Shelf (COTS) servers, COTS1 and COTS2.
    - Signaling Server and SIP Gateway (COTS1).
    - SIPLINE and UCM (COTS2).

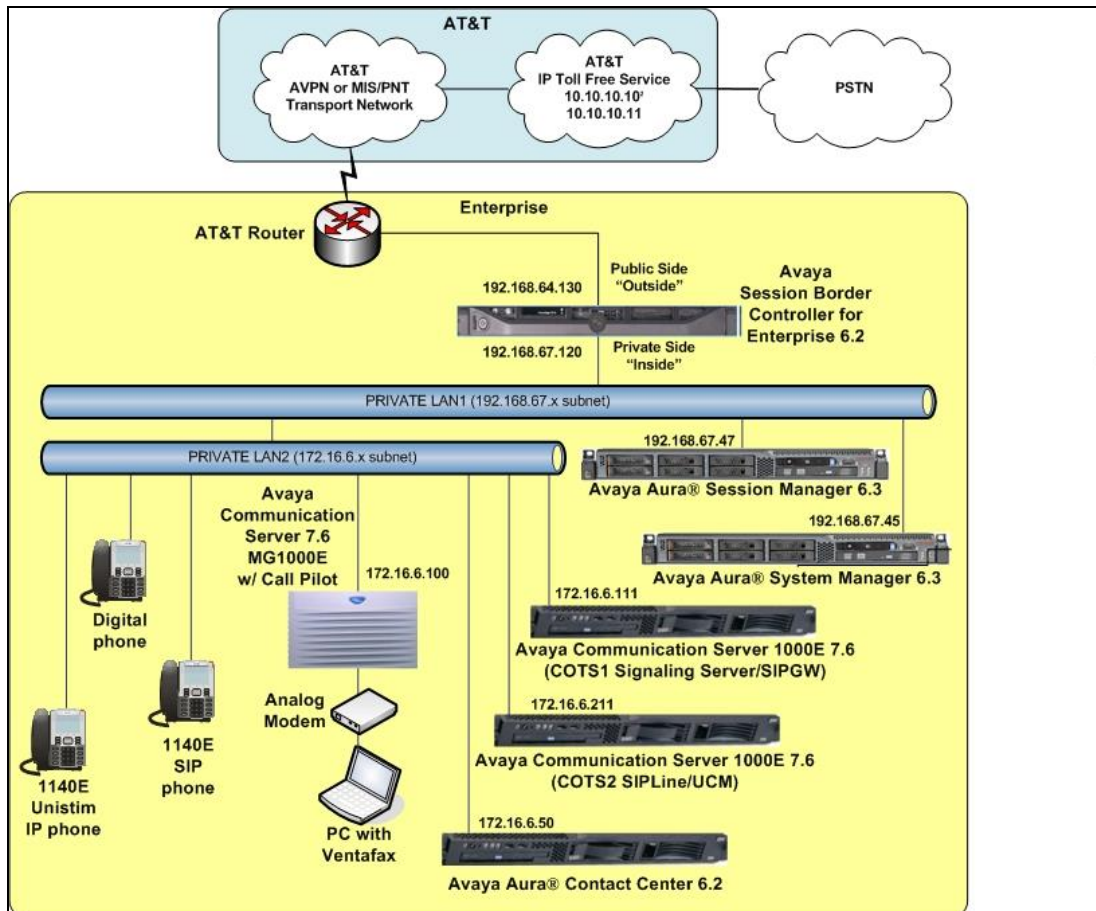
**Note** – Only CS1000E system provisioning providing SIP trunk functionality is described in these application notes. For additional CS1000E system provisioning documentation, see **Section 11**.

- Avaya “desk” phones are represented with Avaya 1140E UNISTim IP, 1140E SIP, and Digital M3904 telephones.
- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements. In the

reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP to communicate with the CS1000E.

- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Avaya SBCE provides address translation and SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network. TCP transport protocol is used between Avaya SBCE and Session Manager. UDP transport protocol is used between Avaya SBCE and the AT&T IP Toll Free service.
- An existing Avaya Call Pilot<sup>®</sup> system provides the corporate voice messaging capabilities in the reference configuration. **Note** - The provisioning of Avaya Call Pilot<sup>®</sup> is beyond the scope of this document (see [5] for more information).

**Note** – Documents used to provision the reference configuration are listed in **Section 11**. Specific references to these documents are indicated in the following sections by the notation [x], where x is the document reference number.



**Figure 1: Avaya Interoperability Reference Configuration**

<sup>2</sup> See the note on the next page regarding the IP addresses.

### 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 configurations.

**Note** – The AT&T IP Toll Free service Border Element IP addresses and DID/DNIS digits are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DID/DNIS digits as part of the AT&T IP Toll Free provisioning process.

Component	Illustrative Value in these Application Notes
<b>CS1000E</b>	
COTS1 SIP Signaling Server IP Address (TLAN)	172.16.6.111
COTS2 SIP Line IP Address (TLAN)	172.16.6.211
MGC Media (DSP) IP Address (TLAN)	172.16.6.100
CS1000E extensions	40xx
<b>Avaya Call Pilot®</b>	
Call Pilot Application	172.16.6.12
Call Pilot Mailboxes	4xxx
<b>Avaya Aura® Contact Center</b>	
	172.16.6.50
<b>Avaya Aura® System Manager</b>	
	192.168.67.45
<b>Avaya Aura® Session Manager</b>	
	192.168.67.47
<b>Avaya SBCE</b>	
IP Address of “Outside” (Public) Interface (connected to AT&T Access Router/IP Toll Free Service)	192.168.64.130
IP Address of “Inside” (Private) Interface (connected to Session Manager)	192.168.67.120
<b>AT&amp;T IP Toll Free Service</b>	
Border Element IP Addresses (Primary & Secondary)	10.10.10.10, 10.10.10.11*

**Table 1: Illustrative Network Values Used in these Application Notes**

**\*NOTE** – The Avaya SBCE Outside interface communicates with AT&T IP Toll Free Border Elements (BEs). For security reasons, the IP addresses of the BEs are not included in this document. However as a placeholder in the following sections, the IP addresses of **10.10.10.10** and **10.10.10.11** are used to represent the AT&T IP Toll Free BE IP addresses where required.

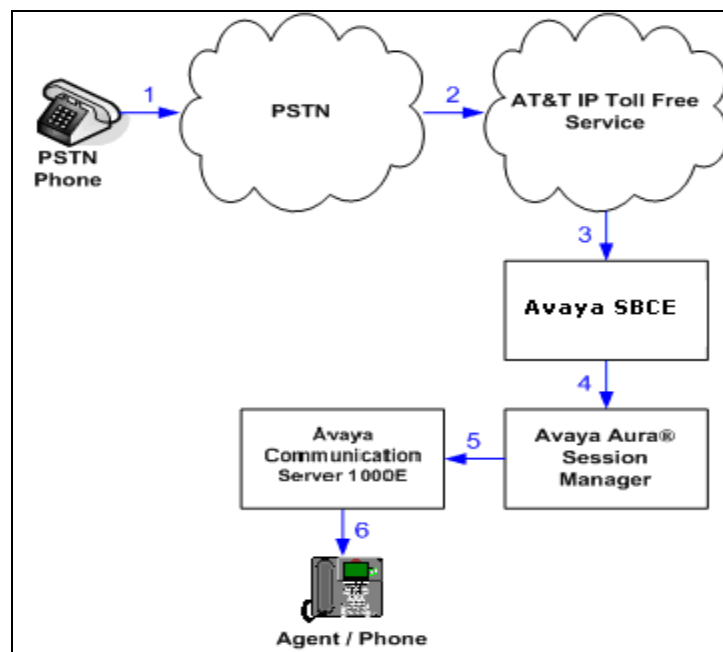
## 3.2. Call Flows

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

### 3.2.1. Inbound Call to the Avaya CS1000E

The first call scenario illustrated in **Figure 2** is an inbound AT&T IP Toll Free service call that arrives on Session Manager and is subsequently routed to CS1000E.

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

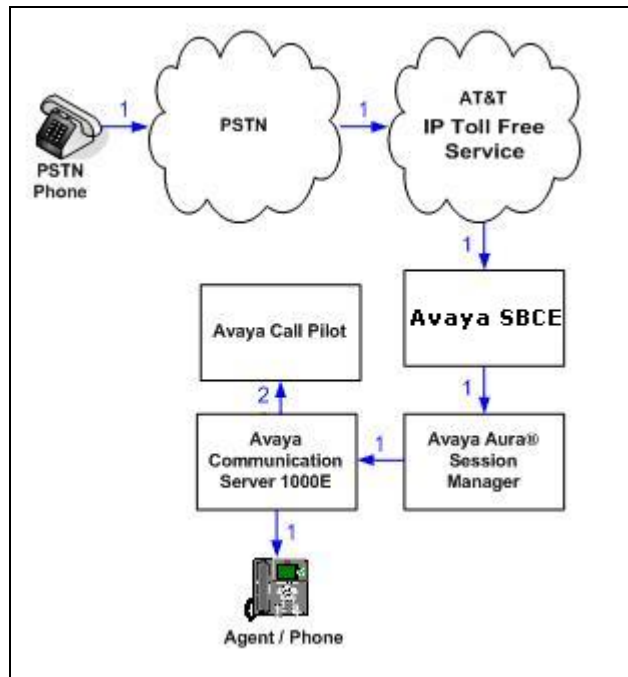


**Figure 2: Inbound AT&T IP Toll Free Service Call to Agent / Telephone**

### 3.2.2. Coverage to Voicemail

The call scenario illustrated in **Figure 3** is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Call Pilot® system connected to CS1000E.

1. Same as the first call scenario shown in **Section 3.2.1**.
2. The called CS1000E Agent/phone does not answer the call, and the call covers to the phone's voicemail. CS1000E forwards the call to Avaya Call Pilot®. Avaya Call Pilot® answers the call and connects the caller to the called phone's voice mailbox.



**Figure 3: Inbound AT&T IP Toll Free Service Call - Coverage to Voicemail**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
HP Proliant DL360 G7 server <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura<sup>®</sup> System Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3.0.0.18002 with patch 6.3.1.08002.0</li> <li>6.3.5_r3501969 with patch 6.3.5_Patch1_r3502017</li> </ul>
IBM 8800 server <ul style="list-style-type: none"> <li>Avaya Aura<sup>®</sup> Session Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3 SP5 (6.3.5.0.635005)</li> </ul>
CS1000E Platform <ul style="list-style-type: none"> <li>Call Pilot</li> </ul>	<ul style="list-style-type: none"> <li>Version 7.6 SP3 (SP_7.6_3)</li> <li>cs1000-patchWeb-7.65.16.21-06.i386.000</li> <li>cs1000-linuxbase-7.65.16.21-08.i386.000</li> <li>cs1000-patchWeb-7.65.16.21-06.i386.000</li> <li>Deplists_CPM_X21_07_65P</li> <li>CP 5.00.41</li> </ul>
Dell R310 <ul style="list-style-type: none"> <li>Avaya Session Border Controller for Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>6.2 Q48<sup>2</sup></li> </ul>
HP DL360 <ul style="list-style-type: none"> <li>Avaya Aura<sup>®</sup> Contact Center</li> </ul>	<ul style="list-style-type: none"> <li>6.2.205</li> </ul>
Avaya 1140E Series IP Deskphones (UNISTim)	<ul style="list-style-type: none"> <li>0625C8Q</li> </ul>
Avaya 1140E Series IP Deskphones (SIP)	<ul style="list-style-type: none"> <li>SIP1140e04.03.12.00.bin</li> </ul>
Avaya M3904 Series Digital Deskphones	-
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none"> <li>6.1.59.144</li> </ul>

**Table 2: Equipment and Software Versions**

<sup>2</sup> See Section 2.2.1, Item 6.

## 5. Configure Avaya Communication Server 1000E

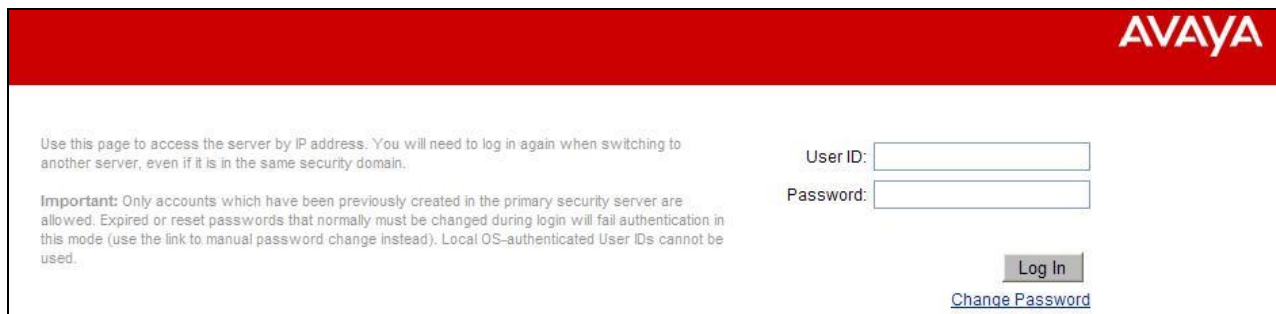
This section describes the CS1000E configuration, focusing on the routing of calls to Session Manager over a SIP trunk. In the sample configuration, CS1000E Release 7.6 was deployed with Call Server applications running on a CPPM server platform with MGC, and utilizing servers running separate Signaling Server and SIP Gateway applications (COTS1), and SIPLINE and UCM applications (COTS2).

Session Manager Release 6.3 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 CS1000E and Session Manager Release 6.3. Therefore NRS was not included in the reference configuration.

This section focuses on the SIP Trunking configurations for the CS1000E. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the CS1000E is configured to support analog, digital, UNISTim and SIP endpoints. For references on how to administer the CS1000E, see **Section 11**.

### 5.1. Logging In and Selecting the System Element

**Step 1** - Unless otherwise noted, all CS1000E provisioning was performed via the Avaya Unified Communication Management (AUCM) web interface. The **AUCM** web interface may be launched directly via **https://<ip address>** where the relevant <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.



**Note** – Although not used in the reference configuration, System Manager may be configured as the Primary Security Server for the Avaya Unified Communications Management application and CS1000E is registered as a member of the System Manager Security framework. The Element Manager then may be accessed via the System Manager **UCM Services** link.

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

The screenshot shows the Avaya Unified Communications Management interface. The left sidebar contains a navigation tree with categories like Network, User Services, Security, and Tools. The main content area is titled 'Elements' and displays a table of registered elements. The table has columns for Element Name, Element Type, Release, Address, and Description. The first row, 'EM on cots1', is highlighted with a red box.

	Element Name	Element Type	Release	Address	Description
1	EM on cots1	CS1000	7.6	192.12.0.100	New element.
2	192.12.0.100	Call Server	7.6	192.12.0.100	New element.
3	CallPilot	Hyperlink	7.6	http://172.16.6.130/cpmgr	
4	cots1.ntlab.com (member)	Linux Base	7.6	172.16.6.111	Base OS element.
5	cots2.ntlab.com (primary)	Linux Base	7.6	172.16.6.211	Base OS element.
6	192.12.0.11	Media Gateway Controller	7.6	192.12.0.11	New element.

## 5.2. Administer Telephony Node

### 5.2.1. Node Information and IP Addresses

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 **1001** is selected.

The screenshot shows the CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and IP Network. The main content area is titled 'IP Telephony Nodes' and displays a table of nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. The first row, '1001', is highlighted with a red box.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1001	1	LTPS, Gateway ( SIPGw )	-	172.16.6.110	-	Synchronized
1004	1	SIP Line	-	172.16.6.210	-	Synchronized

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 a Session Manager SIP Entity for CS1000E in **Section 6.4.2**.

**AVAYA** **CS1000 Element Manager** Help | Logout

---

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

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

Node ID: <input type="text" value="1001"/> * (0-9999)			
Call server IP address: <input type="text" value="192.12.0.100"/> *	TLAN address type: <input checked="" type="radio"/> IPv4 only <input type="radio"/> IPv4 and IPv6		
<b>Embedded LAN (ELAN)</b>		<b>Telephony LAN (TLAN)</b>	
Gateway IP address: <input type="text" value="192.12.0.1"/> *	Node IPv4 address: <input type="text" value="172.16.6.110"/> *		
Subnet mask: <input type="text" value="255.255.255.0"/> *	Subnet mask: <input type="text" value="255.255.255.0"/> *		
Node IPv6 address: <input type="text"/>			

\* Required Value.

**Associated Signaling Servers & Cards**

Scrolling down the Node Details section, the various Node Properties and Applications may be selected.

**AVAYA** **CS1000 Element Manager** Help | Logout

---

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

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

Subnet mask: <input type="text" value="255.255.255.0"/> *	Subnet mask: <input type="text" value="255.255.255.0"/> *
Node IPv6 address: <input type="text"/>	

<b>IP Telephony Node Properties</b> <ul style="list-style-type: none"> <li>• <a href="#">Voice Gateway (VGW) and Codecs</a></li> <li>• <a href="#">Quality of Service (QoS)</a></li> <li>• <a href="#">LAN</a></li> <li>• <a href="#">SNTP</a></li> <li>• <a href="#">Numbering Zones</a></li> <li>• <a href="#">MCDN Alternative Routing Treatment (MALT) Causes</a></li> </ul>	<b>Applications (click to edit configuration)</b> <ul style="list-style-type: none"> <li>• <a href="#">SIP Line</a></li> <li>• <a href="#">Terminal Proxy Server (TPS)</a></li> <li>• <a href="#">Gateway (SIPGw)</a></li> <li>• <a href="#">Personal Directories (PD)</a></li> <li>• <a href="#">Presence Publisher</a></li> <li>• <a href="#">IP Media Services</a></li> </ul>
--	--

\* Required Value.

**Associated Signaling Servers & Cards**

The **Associated Signaling Servers & Cards** information is displayed at the bottom of the screen.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and IP Network. The main content area is titled 'IP Telephony Node Properties' and includes sections for 'Voice Gateway (VGW) and Codecs', 'Quality of Service (QoS)', 'LAN', 'SNTP', 'Numbering Zones', and 'MCDN Alternative Routing Treatment (MALT) Causes'. Below these are 'Applications (click to edit configuration)' including SIP Line, Terminal Proxy Server (TPS), Gateway (SIPGw), Personal Directories (PD), Presence Publisher, and IP Media Services. At the bottom, the 'Associated Signaling Servers & Cards' section is visible, showing a table with columns for Hostname, Type, Deployed Applications, ELAN IP, TLAN IPv4, and Role. The table lists a server named 'cots1' of type 'Signaling\_Server' with various deployed applications and IP addresses. A 'Show: IP/v6 address' checkbox is present, and a note states: '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.'

### 5.2.2. Enable Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, under the **Applications (click to edit configuration)** heading on the **Node Details** page, select the **Terminal Proxy Server (TPS)** application link.

**Step 1** - Check the **UNISim Line Terminal Proxy Server** checkbox to enable proxy service on this node.

**Step 2** - Click on **Save** (not Shown).

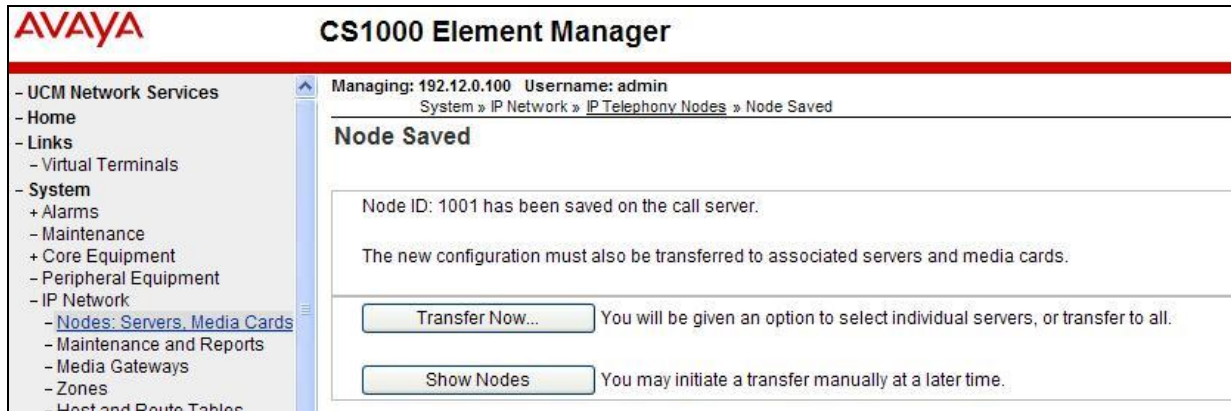
The screenshot shows the AVAYA CS1000 Element Manager interface at the 'UNISim Line Terminal Proxy Server (LTPS) Configuration Details' page. The breadcrumb trail indicates the path: System » IP Network » IP Telephony Nodes » Node Details » UNISim Line Terminal Proxy Server (LTPS) Configuration. The page title is 'Node ID: 1001 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details'. Below the title, there are tabs for 'Firmware', 'DTLS', and 'Network Connect Server'. The 'Firmware' tab is active, showing a section for 'UNISim Line Terminal Proxy Server' with a checkbox labeled 'Enable proxy service on this node' which is checked. Below this, there are fields for 'IP address' (0.0.0.0), 'Full file path' (download/firmwa), 'Server Account/User ID', and 'Password'. The 'DTLS' section is partially visible at the bottom, showing a 'DTLS Policy' dropdown set to 'Off'.

### 5.2.3. Synchronize Configuration

**Step 1** - Scroll to the bottom of the page and click **Save**. This will return the interface to the **Node Details** screen.

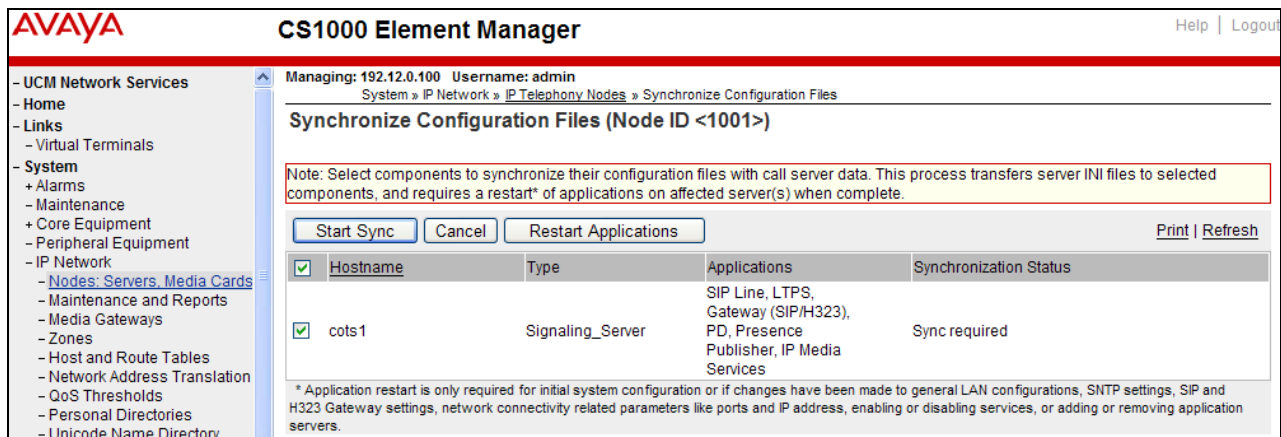
**Step 2** - Click **Save** on the **Node Details** screen (not shown).

**Step 3**- Select **Transfer Now** on the **Node Saved** page as shown below.



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

**Step 4** - Select 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

**AVAYA** **CS1000 Element Manager** Help | Logout

---

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

### Synchronize Configuration Files (Node ID <1001>)

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

Start Sync Cancel Restart Applications Print | Refresh

<input type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input type="checkbox"/>	cots1	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), 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 5** - After synchronization completes, click on the **Refresh** button in the right hand corner, Select the appropriate Hostname (e.g., cots1), and click **Restart Applications**.

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

**AVAYA** **CS1000 Element Manager** Help | Logout

---

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

### Synchronize Configuration Files (Node ID <1001>)

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

Start Sync Cancel Restart Applications Print | Refresh

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cots1	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), 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.

## 5.3. Voice Codecs

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

### 5.3.1. IP Telephony Node Codec Configuration

**Step 1** – As shown in **Section 5.2**, expand **System** → **IP Network**, select **Node, Server, Media Cards**, and select node **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.

The screenshot shows a web-based configuration interface. On the left is a navigation tree with categories like System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes, Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, and Software. The main panel is titled 'General | Voice Codes | Fax' and contains the 'General' tab. The settings include: Echo cancellation (checked, Use canceller, with tail delay: 128), Dynamic attenuation (checked), Voice activity detection threshold: -17 (-20 - +10 DBM), Idle noise level: -65 (-327 - +327 DBM), Signaling options (checked, DTMF tone detection), Low latency mode (unchecked), Remove DTMF delay (squelch DTMF from TDM to IP) (checked), Modem/Fax pass-through (checked), V.21 Fax tone detection (checked), and R factor calculation (unchecked).

**Step 3** - Use the scroll bar on the right to find the area with heading **Voice Codes**. Set the **Voice payload size** to **30**. Note that **Codec G.711** is enabled by default.

The screenshot shows the 'Voice Codes' configuration page. It features a scroll bar on the right. The 'Codec G711' section is expanded, showing: Codec G711: ☒ Enabled (required), Voice payload size: 30 (milliseconds per frame), Voice playback (jitter buffer) delay: 60 120 (milliseconds), Nominal Maximum, Maximum delay may be automatically adjusted based on nominal settings, and ☐ Voice Activity Detection (VAD).

**Step 4** – Scroll down to the G729 codec section 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 should also be enabled in **Section 5.3.2**.

**Note** - On this screen, and the screen shown in **Step 3**, the Voice Payload size is set to 30ms. This is to meet the AT&T IP Toll Free recommendation. However an issue was found where the CS1000E would still send a payload size of 20ms (see **Section 2.2.1, Item 1**).

The screenshot shows the 'Voice Codes' configuration page for Codec G729. It features a scroll bar on the right. The 'Codec G729' section is expanded, showing: Codec G729: ☒ Enabled, Voice payload size: 30 (milliseconds per frame), Voice playback (jitter buffer) delay: 60 120 (milliseconds), Nominal Maximum, Maximum delay may be automatically adjusted based on nominal settings, and ☐ Voice Activity Detection (VAD).

**Step 5** - Scrolling further down, note that T.38 fax is enabled by default. Verify the **Maximum Rate** is set to **14400**.

Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

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

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

Packet size: 30 (bps)

**Step 6** – Click on **Save** and then follow **Steps 1** through **5** in **Section 5.2.3** to synchronize the configuration.

### 5.3.2. Media Gateway Codec Configuration

**Step 1** - Expand **System** → **IP Network** on the left panel and select **Media Gateways**. Click on the IPMG ID (e.g., **000 01**).

AVAYA

CS1000 Element Manager

Help | Log

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Managing: 192.12.0.100 Username: admin

System » IP Network » Media Gateways

Media Gateways

Add...

Digital Trunking...

Reboot

Delete

Virtual Terminal

More Actions

Refresh

	IPMG	IP Address	Zone	Type
	000 01	192.12.0.11	1	MGC

This will open the **Property Configuration** screen (not shown). Click on **Next** (not shown). This will open the **Media Gateway Controller (MGC) Configuration** screen.

**Step 2** - 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 \*

+ VGW and IP phone codec profile

+ QoS

+ Media Based CLID

**Step 3** - 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** (see the note in **Section 5.3.1** regarding payload size).

- 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 4** – Scroll down, click on and expand the **Codec G729A** field. Check the selection box and set the **Voice payload size** (PTIME) to **30** (see the note in **Section 5.3.1** regarding payload size).

**Note** – Although not shown, annexB=yes may be enabled by selecting the **VAD** (Voice Activity Detection) box. However, if enabled here, it should also be enabled in **Section 5.3.1**.

- 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

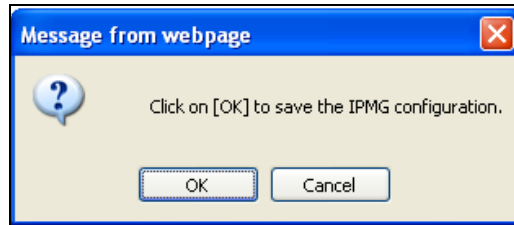
VAD

**Step 5** – Scroll down and click on **Codec T.38 FAX**. Note that T.38 is enabled by default.

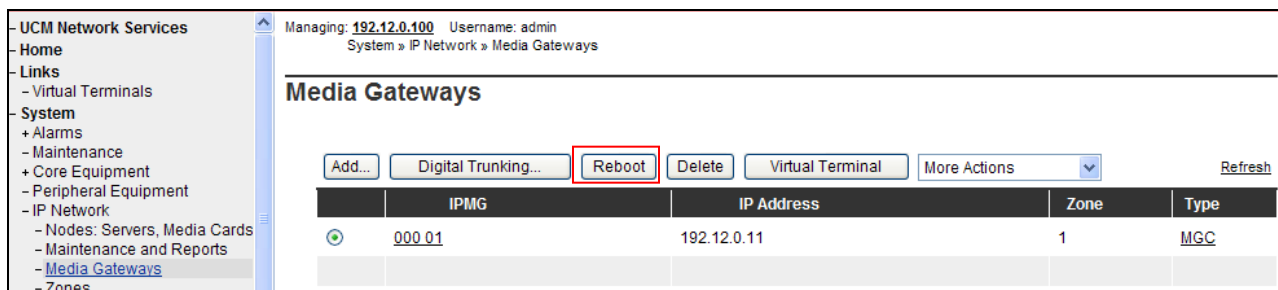
- Codec	T38 FAX	Select <input checked="" type="checkbox"/>
Codec name T38 FAX		

**Step 6** – If changes are made to any of these settings, click on **Save** (not shown).

**Step 7** – A dialog box will open. Click on **Ok**.



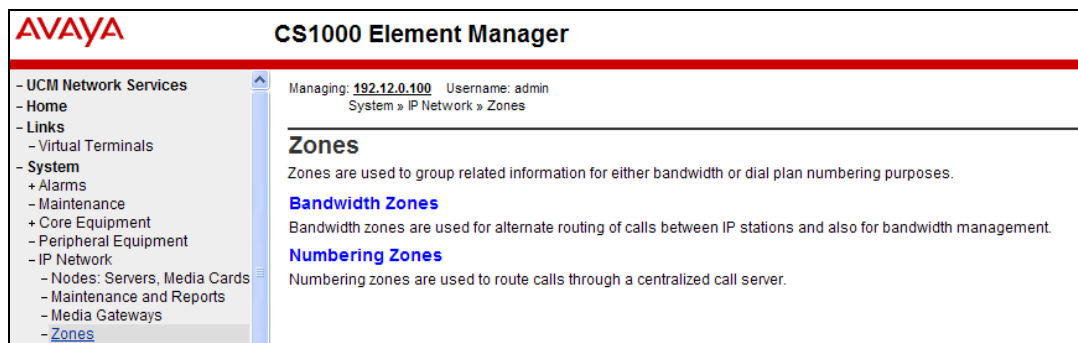
**Step 8** –Select the Media Gateway ID (e.g., 000 01), and click on the **Reboot** button. The Media Gateway will reboot and deploy the new configuration.



## 5.4. Zones and Bandwidth Management

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

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



**Step 2** - Select **Bandwidth Zones**. In the reference configuration, two zones are configured as shown below. **Zone 3** is for the IP telephones and **Zone 5** is for the SIP trunk. Additional zones may be added by selecting the **Add** button.

#### 5.4.1. Zone 5 – SIP Trunk

**Step 1** – Continuing from **Section 5.4, Step 2**, select the zone associated with the virtual trunk to Session Manager (e.g., zone 5) and click **Edit** as shown below.

Bandwidth Zones								
Add...			Edit...	Import...	Export	Maintenance...	Delete	Refresh
	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 2** – Select **Zone Basic Property and Bandwidth Management** for Zone 5.

### 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 Toll Free service.

### Zone Basic Property and Bandwidth Management

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

Submit Refresh Cancel

### 5.4.2. Zone 3 – IP Telephones

Following the steps in **Section 5.4.1**, these are the values used for **Zone 3** (IP Telephones), in the reference configuration.

Input Description	Input Value
Zone Number (ZONE):	3 ( 1 - 8000 )
Intrazone Bandwidth (INTRA_BW):	10000 ( 0 - 10000000 )
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ) ▼
Interzone Bandwidth (INTER_BW):	10000 ( 0 - 10000000 )
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	MO (MO) ▼
Description (ZDES):	PHONES
Location Name (ZNAME):	
Reserved BW Block Size (RESERVED_BW_SIZE):	0 ( 200 - 9999999 )

## 5.5. SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Session Manager.

### 5.5.1. Provision SIP Gateway

**Step 1** – As shown in **Section 5.2.1**, expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**. Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw)** link to view or edit the SIP Gateway configuration.

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

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

Gateway IP address: 192.12.0.1 *	Node IPv4 address: 172.16.0.110 *
Subnet mask: 255.255.255.0 *	Subnet mask: 255.255.255.0 *
Node IPv6 address:	

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

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

\* Required Value.

Save Cancel

**Step 2** - 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 (see **Section 6.1**).
- **Local SIP port:** Enter “**5060**”
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter “<Node id>”. In the sample configuration, Node “**1001**” was used matching the node shown in **Section 5.2.1**.
- **VTrk gateway application:** select “**SIP Gateway (SIPGw)**”.

The values defined for the sample configuration are shown below.

**Step 3** - 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, “**192.168.67.47**” was used.
- **Port:** Enter “**5060**”
- **Transport protocol:** Select “**TCP**”

**Note** - The Secondary TLAN IP address was not used.

**AVAYA** **CS1000 Element Manager** Help | Log

---

Managing: 192.12.0.100 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

**Node ID: 1001 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

Port:  (1 - 65535)

Transport protocol:

Shared Bandwidth Management:  
☐ Enable Shared Bandwidth Management

Proxy Or Redirect Server:  
Proxy Server Route 1:

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

Port:  (1 - 65535)

Transport protocol:

Options: ☐ Support registration  
☐ Primary CDS proxy

**Step 4** - Scroll down and repeat these steps for the **Proxy Server Route 2** (not shown).

**Step 5** - Scroll down to the **SIP URI Map** section. Under the **Public E.164 domain names** and **Private domain names** sections, leave the fields blank. Use the defaults for all other values.

**AVAYA** **CS1000 Element Manager** Help | Log

---

Managing: 192.12.0.100 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

**Node ID: 1001 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

Number translation: Strip: Prefix: CLID display format:

Subscriber (SN):   <CCC><Area code><SN>

National (NN):   <CCC><NN>

International:   <International number>

**SIP URI Map:**

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

**SIP Gateway Services**

SIP Converged Desktop: ☐ Enable CD service

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

**Step 6** – Select **Save** and follow the synchronization steps shown in **Section 5.2.3**.

## 5.5.2. Integrated Services Digital Network (ISDN)

**Step 1** - Select **Customers** in the left pane.

**Step 2** - Click on the link associated with the appropriate customer, (e.g., **00**, not shown). The **Customer 00 Edit** page will appear (not shown).

**Step 3** - Select the **Feature Packages** option from **Customer 00 Edit** page (not shown).

The screen is updated with a listing of available **Feature Packages**.

**Step 4** - Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the **Save** button (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like Core Equipment, IP Network, Interfaces, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'Customers' category is selected. The main area displays a list of feature packages with their respective package numbers. The 'Integrated Services Digital Network' package (Package: 145) is highlighted. Below this, there are input fields for 'Integrated Services Digital Network' (checked), 'Virtual private network identifier' (0), and 'Private network identifier' (1). The top right corner has a 'Help' link.

## 5.5.3. Virtual D-Channel Configuration

**Step 1** - Expand **Routes and Trunks** on the left navigation panel and select **D-Channels**. In the sample configuration, **Channel 15** is associated with the Signaling Server. Channel 20 is associated with the SIP Line. Click on **Edit** to view/change settings. Click on the **To Add** button, to add additional D-Channels.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation tree has 'Routes and Trunks' expanded, and 'D-Channels' is selected. The main area shows the 'D-Channels' configuration page. At the top, it says 'Managing: 192.12.0.100 Username: admin' and 'Routes and Trunks » D-Channels'. Below this, there are sections for 'Maintenance' (listing D-Channel Diagnostics, Network and Peripheral Equipment, MSDI Diagnostics, TMDI Diagnostics, and D-Channel Expansion Diagnostics) and 'Configuration'. The 'Configuration' section has a 'Choose a D-Channel Number' dropdown (set to 0) and a 'Type' dropdown (set to DCH), followed by a 'to Add' button. Below this, there is a table of existing D-Channels:

Channel	Type	Card Type	Description	Action
Channel: 15	Type: DCH	Card Type: DCIP	Description: VDCH	Edit
Channel: 20	Type: DCH	Card Type: DCIP	Description: SIPLINE	Edit

**Step 2** – Click on **Edit** to display the associated D-Channel information used in the reference configuration for the Signaling Server (e.g., channel 15). The **D-Channels 100 Property Configuration** screen is displayed. In the **Basic Configuration** section, the following settings are used.

- Basic Configuration	
Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	VDCH
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1) ▼
Country:	ETS 300 =102 basic protocol (ETSI) ▼
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> <a href="#">more PRI</a>
Secondary PRI2 loops:	<input type="text"/>
Meridian 1 node type:	Slave to the controller (USR) ▼
Release ID of the switch at the far end:	25 ▼
Central Office switch type:	100% compatible with Bellcore standard (STD) ▼
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	1800 Range: 0 - 3700

**Step 3** – Scrolling down, in the **Basic Options (BSCOPT)** section, the following settings are used.

- Basic options (BSCOPT)	
Primary D-channel for a backup DCH:	<input type="text"/> Range: 0 - 254
- PINX customer number:	▼
- Progress signal:	▼
- Calling Line Identification :	▼
- Output request Buffers:	32 ▼
- D-channel transmission Rate:	56 kb/s when LCMT is AMI (56K) ▼
- Channel Negotiation option:	No alternative acceptable, exclusive. (1) ▼
- Remote Capabilities:	<a href="#">Edit</a>

**Step 4** – Scrolling down, in the **Advanced Options (ADVOPT)** section, the following settings are used.

- Advanced options (ADVOPT)	
- Layer 3 call control message count per 5 second time interval:	300 Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms:	1 ▼
- Map channel number to timeslots on a PRI2 loop:	<input checked="" type="checkbox"/>

**Step 5** – Click on **Submit** (not shown).

**Step 6** – Repeat **Steps 1-5** to create the D-channel (e.g., **20**) for the SIP Line.

#### 5.5.4. SIP Routes Configuration

**Step 1** - Select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In the reference configuration, **Customer 0** is used. Click on **Customer:0** to display defined routes, or click on **Add route**, to add additional routes.

**Step 2** – In the reference configuration, **Route 16** is used for SIP trunking. Click on the **Edit** button to display the Route 16 settings.

AVAYA CS1000 Element Manager			
Managing: 192.12.0.100 Username: admin Routes and Trunks » Routes and Trunks			
Routes and Trunks			
Customer: 0	Total routes: 9	Total trunks: 60	Add route
+ Route: 15	Type: TIE	Description: H323	Edit Add trunk
+ Route: 16	Type: TIE	Description: SIP	Edit Add trunk
+ Route: 17	Type: TIE	Description: SIP VTRK TTY	Edit Add trunk
+ Route: 18	Type: TIE	Description: SIPLINE	Edit Add trunk
+ Route: 26	Type: DID	Description: MIRAN	Edit Add trunk
+ Route: 27	Type: MUS	Description: MUSIC	Edit Add trunk
+ Route: 28	Type: RAN	Description: RAN1	Edit Add trunk

The following screen shows **Basic Configuration** settings for Route 16.

**- Basic Configuration**

Route data block (RDB) (TYPE):

Customer number (CUST):

Route number (ROUT):

Designator field for trunk (DES):

Trunk type (TKTP):

Incoming and outgoing trunk (ICOG):

Access code for the trunk route (ACOD):

Trunk type M911P (M911P): ☐

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

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

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

- Protocol ID for the route (PCID):

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

- Enable Shared Bandwidth Management for the route (SBWM): ☐

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE):

- D channel number (DCH):  (0 - 254)

- Interface type for route (IFC):

- Private network identifier (PNI):  (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):

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

- 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):

- Mobile extension timer (MBXT):  (0 - 8000 milliseconds)

Calling number dialing plan (CNDP):

**Step 3** – Scrolling down, click on **Basic Route Options**. The following settings are used in the reference configuration.

**- Basic Route Options**

Attendant announcement (ATAN):

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):  (0 - 254)

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

- Display external dialed digits (DEXT): ☐

Multifrequency compelled or MFC signaling (MFC):

Process notification networked calls (PNNC): ☐

### 5.5.5. SIP Trunk Configuration to Session Manager

**Step 1** - Select **Routes and Trunks** → **Routes and Trunks** on the left navigation panel and expand the **Customer 0**. Select **Route 16**, to display the 10 trunks used in the reference configuration (**Trunk:1 – 10**), or click **Add Trunk** to add additional trunks to the route.

The screenshot displays the AVAYA CS1000 Element Manager interface. The top status bar shows 'Managing: 192.12.0.100' and 'Username: admin'. The left navigation pane is expanded to 'Routes and Trunks'. The main content area, titled 'Routes and Trunks', shows a table of routes for 'Customer: 0'. The table has columns for 'Route', 'Type', and 'Description'. The 'Route' column is expanded, showing a list of routes from 15 to 30. The 'Route: 16' is selected, and a sub-table shows the trunks associated with it, including 'Trunk: 1 - 10'. The 'Trunk: 1 - 10' is highlighted with a red box. The sub-table also shows 'Total trunks: 10'.

Customer: 0	Total routes: 9	Total trunks: 60		
+ Route: 15	Type: TIE	Description: H323	Edit	Add trunk
- Route: 16	Type: TIE	Description: SIP	Edit	Add trunk
+ Trunk: 1 - 10	Total trunks: 10			
+ Route: 17	Type: TIE	Description: SIP VTRK TTY	Edit	Add trunk
+ Route: 18	Type: TIE	Description: SIPLINE	Edit	Add trunk
+ Route: 26	Type: DID	Description: MIRAN	Edit	Add trunk
+ Route: 27	Type: MUS	Description: MUSIC	Edit	Add trunk
+ Route: 28	Type: RAN	Description: RAN1	Edit	Add trunk
+ Route: 29	Type: RAN	Description: RAN2	Edit	Add trunk
- Route: 30	Type: RAN	Description: RAN3	Edit	Add trunk

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

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

**Step 3** – Click on the **Edit** button for **Trunk: 1**, to display the trunk configuration. In the reference configuration, Trunk 1 uses **Channel 16**. Therefore, each subsequent trunk allocated to this route will use channel  $16+(n-1)$ , where n is the trunk number. For example, Trunk 9 will use channel 24 ( $16+9-1 = 24$ ).

### Customer 0, Route 16, Trunk 1 Property Configuration

**- Basic Configuration**

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:  \*

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

**Step 4** – Going back to the screen shown in **Step 1**, select the **Edit** button next to **Route 16** to verify the configuration, as shown below. Verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.2**. 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 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.

**Note** – Although the AT&T IP Toll Free service is an inbound only service, the trunks are configured for outbound as well, to facilitate SIP trunk calls to other destinations in the CPE via Session Manager (if needed).

**AVAYA CS1000 Element Manager**

Managing: 192.12.0.100 Username: admin  
Routes and Trunks » Routes and Trunks » Customer 0, Route 16 Property Configuration

### Customer 0, Route 16 Property Configuration

**- Basic Configuration**

Route data block (RDB) (TYPE): 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 5.5.3** (e.g., 15).

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Links, System, IP Network, Interfaces, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main area displays the configuration for the 'Integrated services digital network option (ISDN)'. A red box highlights the '- D channel number (DCH)' field, which contains the value '15'. Other visible fields include 'Mode of operation (MODE)' set to 'Route uses ISDN Signaling Link (ISLD)', 'Interface type for route (IFC)' set to 'Meridian M1 (SL1)', 'Private network identifier (PNI)' set to '00000', 'Network calling name allowed (NCNA)' checked, 'Network call redirection (NCRD)' checked, 'Trunk route optimization (TRO)' unchecked, 'Recognition of DTI2 ABCD FALT signal for ISL (FALT)' unchecked, 'Channel type (CHTY)' set to 'B-channel (BCH)', 'Call type for outgoing direct dialed TIE route (CTYP)' set to 'Unknown Call type (UKWN)', 'Insert ESN access code (INAC)' unchecked, 'Integrated service access route (ISAR)' unchecked, 'Display of access prefix on CLID (DAPC)' unchecked, 'Mobile extension route (MBXR)' unchecked, 'Mobile extension outgoing type (MBXOT)' set to 'National number (NPA)', 'Mobile extension timer (MBXT)' set to '0', and 'Calling number dialing plan (CNDP)' set to 'Unknown (UKWN)'.

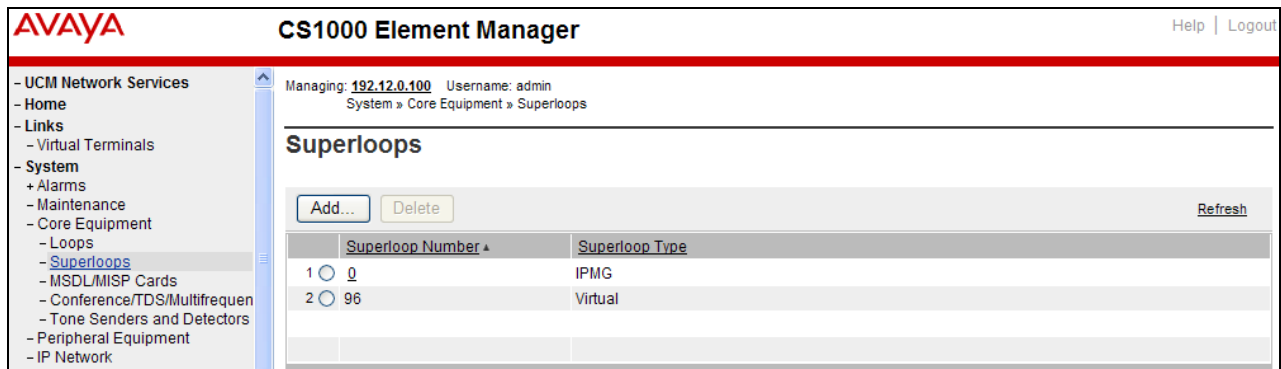
**Step 6** - Scrolling down, open **Basic Route Options** and verify that the DCNO number specified (e.g., 1), matches the **Digit Conversion Tree Number** specified in **Section 5.6, Step 3**.

The screenshot shows the 'Basic Route Options' configuration window. It contains several fields with checkboxes or dropdown menus. A red box highlights the '- Day IDC tree number (DCNO)' field, which contains the value '1'. Other visible fields include 'Attendant announcement (ATAN)' set to 'No Attendant Announcement. (NO)', 'Billing number required (BILN)' unchecked, 'Call detail recording (CDR)' unchecked, 'North American toll scheme (NATL)' checked, 'Controls or timers (CNTL)' unchecked, 'Conventional (Tie trunk only) (CNVT)' unchecked, 'Incoming DID digit conversion on this route (IDC)' checked, '- Night IDC tree number (NDNO)' set to '1', '- Display external dialed digits (DEXT)' unchecked, and 'MFC feature options (MFC\_FEAT)' unchecked. At the bottom, there are expandable sections for '+ Network Options', '+ General Options', and '+ Advanced Configurations'.

**Step 7** – After any changes or additions, click on **Submit** (not shown).

### 5.5.6. Administer Virtual Super-Loop

Select **System** → **Core Equipment** → **Superloops** from the left pane to display the **Superloops** screen. In the reference configuration, Superloops 0 and 96 are used.



## 5.6. Routing of Inbound Numbers to CS1000E

PSTN callers will dial AT&T IP Toll Free DID numbers to reach stations on CS1000E. The AT&T will then send associated DNIS digits in the Request-URI of the inbound SIP INVITES. These DNIS digits are converted to their associated extensions by the CS1000E Incoming Digit Translation (IDT) table.

**Note** – The DNIS digits might not be the same as the dialed DID number<sup>3</sup>.

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

**Step 2** – Select the appropriate **Customer ID** (e.g., 00) 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 trunk provisioning shown in **Section 5.5.5**.

<sup>3</sup> See the issue described in Section 2.2.1, Item 5.

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 (not shown). In the **Incoming Digits** field, enter an AT&T IP Toll Free DNIS number sent in the R-URI (e.g., **7325554383**), and in the **Converted Digits** field, enter the associated CS1000E extension (e.g., **4094**). Click on **Save**.

### Add Incoming Digits

Incoming Digits:

Converted digits:  (0 - 99999999)

Force storage or removal of data: ☐

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

[Save](#) [Cancel](#)

**Step 5** – Repeat **Step 4** for all AT&T IP Toll Free DNIS numbers and their associated destination extensions. For example, a CS1000E Agent phone (e.g., 4014, see **Section 5.7**), an Agent skill queue (e.g., 4013, see **Section 5.7**), and the Call Pilot main access number (e.g., 2090, see **Section 5.10**).

### Digit Conversion Tree 1 Configuration

Regular IDC tree 4013  
Send calling party DID disabled

[Add...](#) [Delete IDC](#) [Delete IDC tree](#) [Refresh](#)

	Incoming Digits ▲	Converted Digits	CPND Name	CPND language
33	<a href="#">7325553166</a>	4013		
34	<a href="#">7325553167</a>	4095		
35	<a href="#">7325553168</a>	4099		
36	<a href="#">7325553169</a>	4009		
37	<a href="#">7325553170</a>	4014		
38	<a href="#">7325553179</a>	4096		
39	<a href="#">7325553180</a>	2090		

## 5.7. CS1000E Agent Access Provisioning

This section is not intended to be prescriptive, but simply illustrates a sampling of defining Agent access on the CS1000E in the sample configuration. Inbound IP Toll Free numbers are mapped to the Agent extensions (or queues) as shown in **Section 5.6**.

The following Directory Numbers (DN) are defined:

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

### 5.7.1. CS1000E IP Agent Phone

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

#### 5.7.1.1 General Properties

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

**Step 2** – Click on the TN value displayed (e.g., **096 0 01 17**). The **Phone Details** form will open. Note that in this example the telephone type is an 1150 and that it is defined in Zone 3. A call between this telephone and another telephone in Zone 3 will use a “best bandwidth” strategy (see **Section 5.4**) and therefore can use G.711MU. If this same telephone connects to the PSTN via the SIP trunk, the call would use a “best bandwidth” strategy, and the call would use G.729A.

The screenshot shows the 'CS1000 Element Manager' interface. On the left is a navigation tree with categories like Zones, Interfaces, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The 'Phones' category is selected. The main area is titled 'Phone Details' and contains a small image of a phone. To the right of the image, it says 'System: EM on cots1', 'Phone Type: 1150', and 'Sync Status: TRN'. Below this is a tabbed interface with 'General Properties', 'Features', 'Keys', and 'User Fields'. The 'General Properties' tab is active, showing fields for 'Customer Number' (0), 'Terminal Number' (096 0 01 17), 'Designation' (AGENT2), 'Zone' (3), and 'Key Expansion Modules' (0). A 'Custom View' dropdown is set to 'All'.

### 5.7.1.2 Features

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

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

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

### 5.7.1.3 Keys

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

#### 5.7.1.3.1 Key 0

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

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

Key No.	Key Type	Key Value								
0	ACD - Auto. Call Distribution	<table><tr><td>ACD Directory Number</td><td>4012</td></tr><tr><td>CLID</td><td></td></tr><tr><td>Numeric/D&lt;space&gt;ACD Position ID</td><td>0 2003</td></tr><tr><td>ANIE Entry</td><td></td></tr></table>	ACD Directory Number	4012	CLID		Numeric/D<space>ACD Position ID	0 2003	ANIE Entry	
ACD Directory Number	4012									
CLID										
Numeric/D<space>ACD Position ID	0 2003									
ANIE Entry										

#### 5.7.1.3.2 Key 3 - Single Call Appearance

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

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

3	SCR - Single Call Ringing	<table><tr><td>Directory Number</td><td>4014</td></tr><tr><td colspan="2"><input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)</td></tr><tr><td>First Name</td><td>Last Name</td><td>Display Format</td><td>Language</td></tr><tr><td>Agent2</td><td></td><td>First, Last</td><td>Roman</td></tr><tr><td colspan="2">CLID Entry (Numeric or D)</td><td colspan="2">0</td></tr><tr><td colspan="2">ANIE Entry</td><td colspan="2"></td></tr></table>	Directory Number	4014	<input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)		First Name	Last Name	Display Format	Language	Agent2		First, Last	Roman	CLID Entry (Numeric or D)		0		ANIE Entry			
Directory Number	4014																					
<input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)																						
First Name	Last Name	Display Format	Language																			
Agent2		First, Last	Roman																			
CLID Entry (Numeric or D)		0																				
ANIE Entry																						

### 5.7.1.3.3 LD 20 Overlay Command for Agent Configuration Display

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

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

```

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

```

### 5.7.2. CS1000E Auto Call Distribution (ACD)

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

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

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

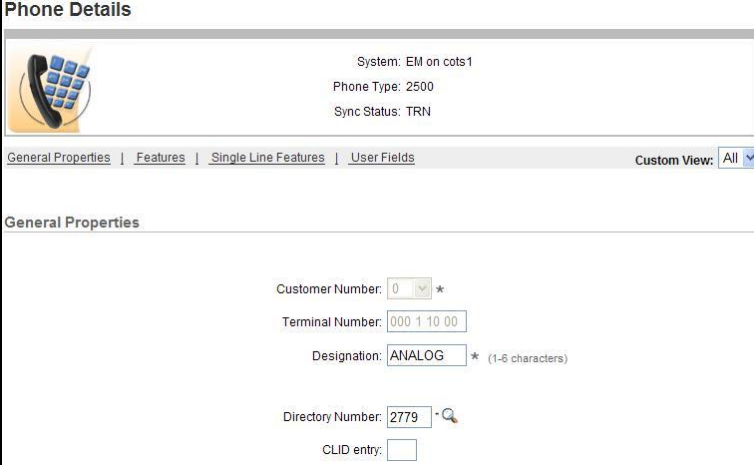
### 5.7.3. CS1000E Control DN (CDN)

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

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

### 5.7.4. Analog Fax Line

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



The 'Phone Details' configuration screen shows a phone icon and system information: 'System: EM on cots1', 'Phone Type: 2500', and 'Sync Status: TRN'. Below this is a tabbed interface with 'General Properties' selected. The 'General Properties' section contains the following fields:

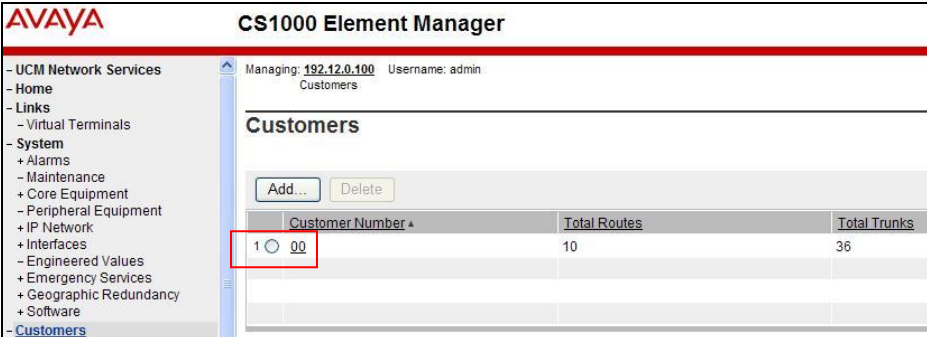
- Customer Number: 0
- Terminal Number: 000 1 10 00
- Designation: ANALOG (1-6 characters)
- Directory Number: 2779
- CLID entry: (empty)

## 5.8. Customer Information

In the reference configuration, specific calling number information is required based on the destination of the call.

### 5.8.1. Caller ID Provisioning

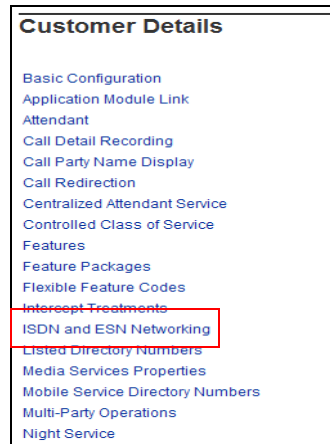
**Step 1** - Select **Customers** from the left navigation menu, click on the appropriate **Customer Number** (e.g., 00)



The 'CS1000 Element Manager' interface shows the 'Customers' section. The left navigation menu includes: UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, and Customers. The main area displays a table of customers with columns for Customer Number, Total Routes, and Total Trunks. The first row is highlighted with a red box around the '1' and '00' in the Customer Number column.

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

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

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

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

This will display all defined Call Ids. For example **CLID 0** will use **732-555-4383**.

**Calling Line Identification Entries**

Search for CLID

Start range :

End range :

'End range' should not exceed the CLID size specified

**Calling Line Identification Entries**

<input type="checkbox"/>	Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
<input type="checkbox"/>	0	732	5554383			NO	
<input type="checkbox"/>	1	732	5554384			NO	
<input type="checkbox"/>	2	732	5554385			NO	

Click on any Entry ID to view or change further details (e.g., **Entry ID 0**). Note that the **Use DN as DID** is set to **NO**. This means that the local extension will not be used for the calling number. Call IDs are then associated with specific telephone directory numbers (DNs) assigned to stations (see **Section 5.7.1.3.2**).

Managing: **192.12.0.100** Username: admin  
[Customers](#) » [Customer 00](#) » [Customer Details](#) » [ISDN and ESN Networking](#) » [Calling Line Identification Entries](#) » Edit Calling Line Identification 0

**Edit Calling Line Identification 0**

**General Properties**

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

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

Local Steering Code:  (1-7 digits)

Use DN as DID :

**Emergency Services Access**

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

Emergency Options: ☐ Home national number for emergency services access calls

Roman characters: ☒

CPND Name:   
first name, last name

Expected Length:

Display Format:

## 5.9. Changing RFC2833 DTMF Telephone Event Type

The CS1000E uses RFC2833 DTMF Telephone Event type 101. The AT&T IP Toll Free service recommends the value 100. While having asymmetric telephone event types is permitted, this may cause issues in some call scenarios. Therefore the CS1000E value may be changed to 100 as follows:

**Step 1** – From an CS1000E console connection, press the ctrl key and enter “**pdt**”. The system will return:

```
PDT login on /tyCo/0
Username:
```

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

```
Password:
```

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

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

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

```
pdt> setRFC2833PT 100
```

The system will respond with the pdt> prompt.

```
pdt>
```

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

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

## 5.10. Inbound Calls to Call Pilot®

PSTN callers may wish to access Call Pilot® to retrieve messages. In addition to defining an entry in the CS1000E IDT table for routing calls to the main Call Pilot® access number (e.g., 2090, see **Section 5.6**), the customers Billing Number (that the AT&T IP Toll Free service inserts in SIP INVITE Request-URI and TO headers, see **Section 2.2.1, Item 5**), must be defined to Call Pilot® as well. This is required because Call Pilot® uses the contents of the TO header for admission control.

**Note** – The provisioning of Call Pilot® is beyond the scope of this document. Refer to [5] for more information.

**Step 1** – Log into the Call Pilot® manager GUI using the appropriate credentials.

> CALLPILOT MANAGER

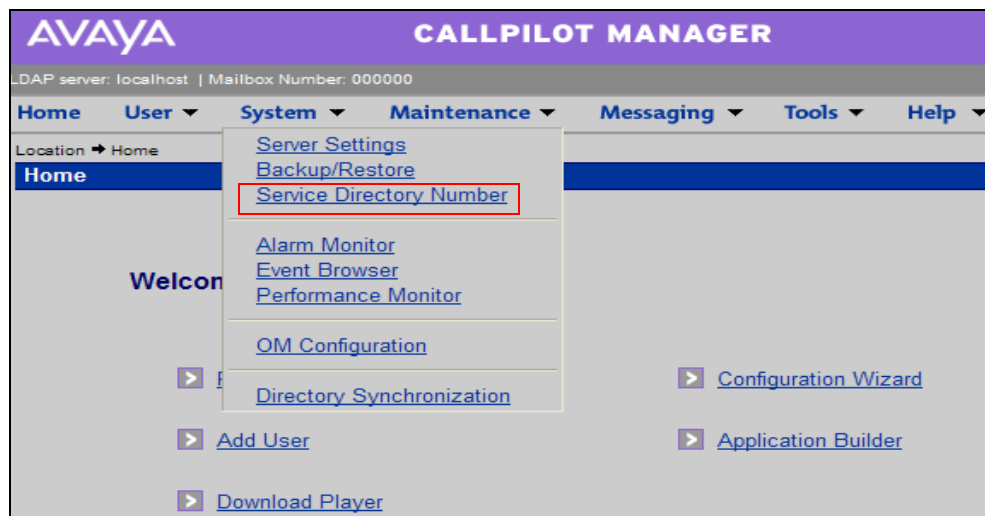
AVAYA

**Selecting a CallPilot Server:**  
Select a server and location from the list of preset servers, or enter the server name (or IP address). The location field is required only if the indicated server has Network Message Service (NMS). In this case enter the name of the location where your mailbox resides.

User:  
Mailbox Number:   
Password:

Server:  
Preset server list: Enter data manually   
Server:  [security](#)  
Location:

**Step 2** – Navigate to **System** → **Service Directory Number**



**Step 3** – Click on **New** (not shown). Populate the form as shown below, where **1234567890** is the AT&T IP Toll Free customer Billing Number. Click on **Save**.

The screenshot shows the AVAYA CALLPILOT MANAGER web interface. At the top, there's a purple header with the AVAYA logo and 'CALLPILOT MANAGER'. Below it, a status bar shows 'LDAP server: localhost | Mailbox Number: 000000'. A navigation menu includes 'Home', 'User', 'System', 'Maintenance', 'Messaging', 'Tools', and 'Help'. A breadcrumb trail reads 'Location → System → Service Directory Number → SDN Details'. The main title bar says 'SDN Details: 1234567890'. Below this are 'Save', 'Cancel', 'Print', and 'Help' buttons. The 'General' section contains the following fields: 'Service DN' (text box with '1234567890'), 'Application Name' (dropdown menu with 'Voice Messaging'), 'Media Type' (dropdown menu with 'Voice'), 'Minimum Channels' (text box with '0'), 'Maximum Channels' (checkbox 'Use Default' is checked, followed by an empty text box), 'Remote Activation Password' (text box), 'Password Confirmation' (text box), 'Comments' (text area), and 'Ring-back type' (dropdown menu with 'USA').

## 5.11. Configuration Backup

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

The screenshot shows the 'Call Server Backup' form. On the left is a navigation tree with 'Tools' expanded and 'Call Server' selected. The main area has the title 'Call Server Backup'. Below it, the 'Action' dropdown menu is set to 'Backup'. To the right of the dropdown are 'Submit' and 'Cancel' buttons.

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.
```

## 6. Configure Avaya Aura® Session Manager

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 11**.

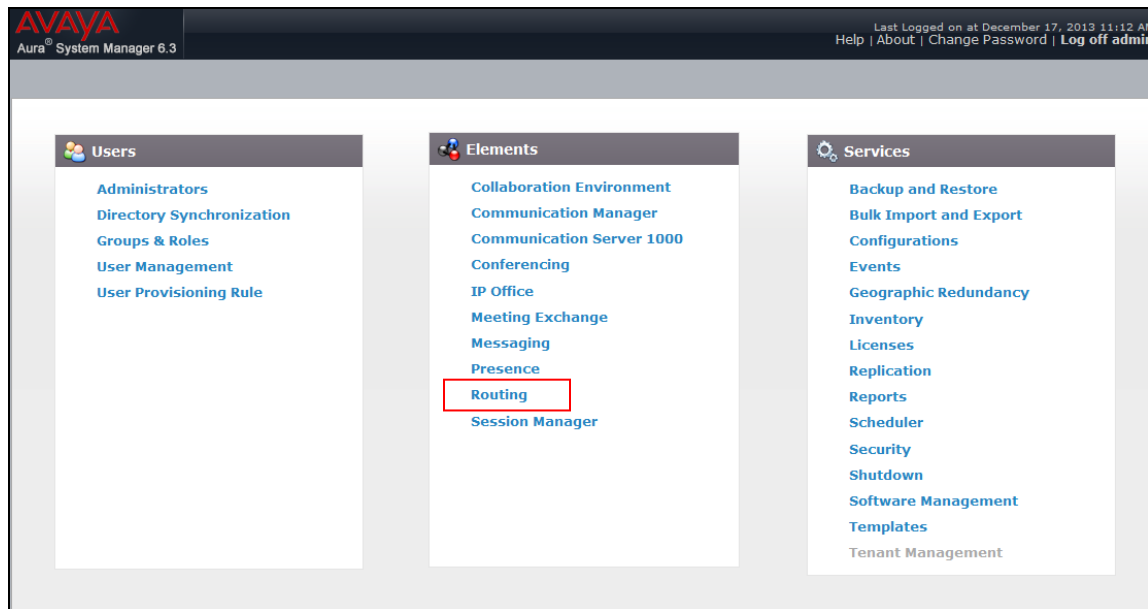
The following administration activities will be described:

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

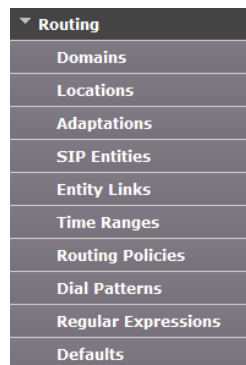
**Step 1** - Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “<http://<ip-address>/SMGR>”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.

**Step 2** - From the **Log On** screen enter appropriate **User ID** and **Password** and press the **Log On** button.

**Step 3** - Once logged in, a Release 6.3.5 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.



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



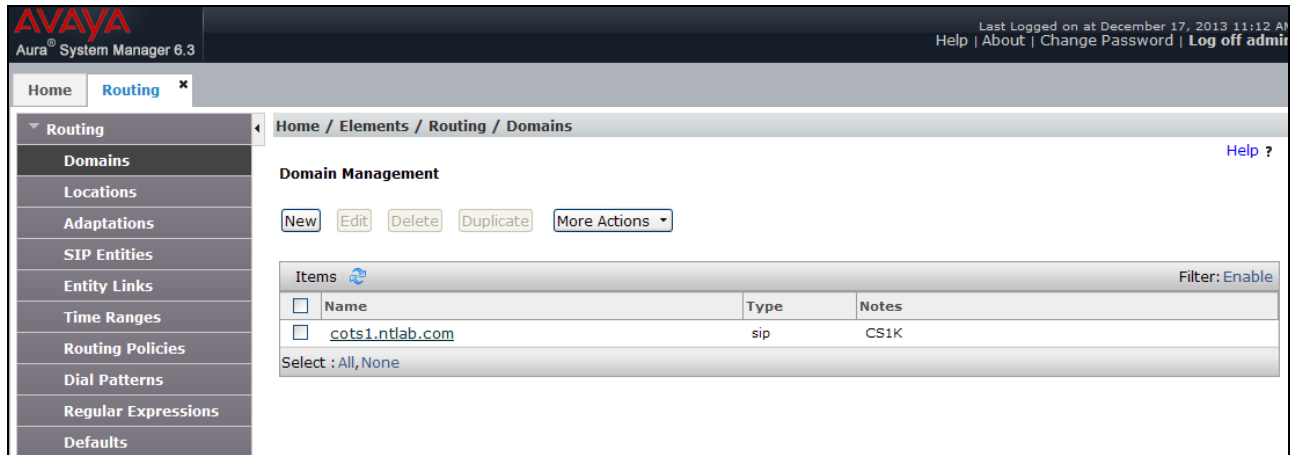
## 6.1. SIP Domain

**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 shown below and use default values for remaining fields.

- **Name** = **cots1.ntlab.com** (see **Section 5.5.1**).
- **Type** = SIP
- Add **Notes** if desired.

**Step 3** - Click **Commit** to save (not shown). 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., 172.16.6.x for all devices on a particular subnet), or individual devices (e.g., 172.16.6.10 for a specific device's IP address). In the reference configuration the CS1000E is located in subnet 172.16.6.x). The rest of the CPE equipment, (including Session Manager, System Manager and the Avaya SBCE), were located in subnet 192.168.67.x. Therefore a Location was created for each subnet.

### 6.2.1. Location for CS1000E Subnet

**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 (e.g., **CS1K**).
- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern** Enter the IP Address or IP Address pattern used to identify the CS1000E location (e.g., **172.16.6.\***).
- **Notes** Add a brief description. [Optional]

**Step 3** – Leave all other default values, and click **Commit** to save.

AVAYA

Aura System Manager 6.3

Last Logged on at December 17, 2013 11:12 AM

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

Home

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations

Location Details

Commit

Cancel

Help ?

General

\* Name:

CS1K

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

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

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

\* Latency before Overall Alarm Trigger:

5

Minutes

\* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 172.16.6.*	

Select : All, None

Commit

Cancel

### 6.2.2. Location for Customer Premises Equipment Subnet.

Repeat **Steps 1-3** in **Section 6.2.1** to create a location called **Main** for the rest of the CPE, including Session Manager, System Manager, and the Avaya SBCE, using address **192.168.67.\***.

Location Pattern		
<input type="button" value="Add"/> <input type="button" value="Remove"/>		
1 Item <input type="button" value="Refresh"/>		
<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*192.168.67.*	
Select : All, None		
		<input type="button" value="Commit"/> <input type="button" value="Cancel"/>

The completed Locations form is shown below.

AVAYA  
Aura® System Manager 6.3

Last Logged on at December 17, 2013 11:12 /  
Help | About | Change Password | Log off adm

Home Routing

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

Home / Elements / Routing / Locations

Location

2 Items  Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CS1K	
<input type="checkbox"/>	Main	

Select : All, None

## 6.3. Configure Adaptations

Adaptations are pre-configured modules, designed for the CS1000E, that Session Manager can use to replace, modify, or remove SIP headers. In the reference configuration the following adaptations are used.

- **CS1000Adapter** – This adaptation is used to provide translation of certain CS1000E generated SIP headers into formats used by other Avaya products and endpoints.
- **DigitConversionAdapter** – This adaptation is used in conjunction with the CS1000Adapter to modify digit strings in the SIP Request-URI. Note that this adaptation's functionality is included in all other adaptations.

In addition, Module Parameters **fromto=true** (used to modify the From and To headers for inbound calls to Call Pilot), and **MIME=no** (to remove CS1000E Mime headers not supported by AT&T), are also specified.

### 6.3.1. Adaptation for Traffic to CS1000E

**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., “**To\_CS1K**”).
- **Module Name:** Select “**CS1000Adapter**” from drop-down menu (or enter “**CS1000Adapter**” if not previously defined in the menu).
- **Module Parameter:** Select **Name-Value Parameter** from the drop-down menu.
  - Click on **Add**, then enter:
    - **Name** = **fromto**
    - **Value** = **true**

**Step 2** - Click on **Commit**.

The screenshot shows the AVAYA Aura System Manager 6.3 interface. The left navigation pane is open to 'Routing' > 'Adaptations'. The main content area shows the 'Adaptation Details' for a new adaptation. The 'General' tab is selected. The 'Adaptation Name' is 'To\_CS1K', 'Module Name' is 'CS1000Adapter', and 'Module Parameter Type' is 'Name-Value Parameter'. Below this, there is a table with one row: 'fromto' with value 'true'. There are also fields for 'Egress URI Parameters' and 'Notes'. At the bottom, there are two sections for 'Digit Conversion' (Incoming and Outgoing), both showing '0 Items'.

**Note** – No entries are required in the **Digit Conversion for Incoming Calls to SM** or the **Digit Conversion for Outgoing Calls from SM** sections.

### 6.3.2. Adaptation for Traffic from CS1000E to AT&T

The message body of Re-INVITE messages sent from the CS1000E may 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. Since AT&T has no use for this information, the Module Parameter **MIME=no** was used in the reference configuration to remove these headers. Note that the Avaya SBCE is used to remove additional Avaya SIP headers (see **Section 8.4.3**).

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

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., “CS1K\_to\_ATT”).
- **Module Name:** Select “**DigitConversionAdapter**” from drop-down menu (or add an adapter with name “**DigitConversionAdapter**” if not previously defined)
- **Module Parameter Type:** Select **Name-Value Parameter** from the drop-down menu.
  - Click on **Add**, then enter:
    - **Name** = **MIME**
    - **Value** = **no**

**Step 2** - Click **Commit**.

AVAYA  
Aura® System Manager 6.3  
Last Logged on at December 18, 2013 4:59 | Help | About | Change Password | Log off adm

Home Routing x

Home / Elements / Routing / Adaptations

Adaptation Details [Commit] [Cancel]

General

\* Adaptation Name: CS1K\_to\_ATT

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

[Add] [Remove]

Name	Value
MIME	no

Select : All, None

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

[Add] [Remove]

0 Items

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

[Add] [Remove]

0 Items

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

**Note** – No entries are required in the **Digit Conversion for Incoming Calls to SM** or the **Digit Conversion for Outgoing Calls from SM** sections.

## 6.4. SIP Entities

SIP Entities must be added for 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.

In addition, a SIP Entity is also created for Session Manager itself, during the System Manager installation process. While installation procedures are beyond the scope of this document, the Session Manager Entity form is shown below for completeness. Consult [6-8] for further information on Session Manager Installation.

### 6.4.1. SIP Entity for Session Manager

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 6.3', and a user status bar indicating 'Last Logged on at December 18, 2013 4:59 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar contains a menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / SIP Entities' and shows the 'SIP Entity Details' form for 'sm63'. The form includes fields for Name, FQDN or IP Address, Type (set to 'Session Manager'), Notes, Location (set to 'Main'), Outbound Proxy, Time Zone (set to 'America/New\_York'), and Credential name. Below this is the 'SIP Link Monitoring' section, which is set to 'Use Session Manager Configuration'. The 'Entity Links' section shows a table with two entries: one linking 'sm63' to 'CS1K' and another linking 'sm63' to 'A-SBCE', both using TCP on port 5060 with a 'trusted' connection policy. The 'Port' section shows two entries: '5060' for TCP and '5061' for TLS, both with the default domain 'cots1.ntlab.com'. The 'SIP Responses to an OPTIONS Request' section is currently empty.

**SIP Entity Details**

**General**

\* Name: sm63

\* FQDN or IP Address: 192.168.67.47

Type: Session Manager

Notes:

Location: Main

Outbound Proxy:

Time Zone: America/New\_York

Credential name:

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

**Entity Links**

Add Remove

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
sm63	TCP	* 5060	CS1K	* 5060	trusted	<input type="checkbox"/>
sm63	TCP	* 5060	A-SBCE	* 5060	trusted	<input type="checkbox"/>

Select : All, None

**Port**

TCP Failover port:

TLS Failover port:

Add Remove

Port	Protocol	Default Domain	Notes
5060	TCP	cots1.ntlab.com	
5061	TLS	cots1.ntlab.com	

Select : All, None

**SIP Responses to an OPTIONS Request**

Add Remove

Response Code & Reason Phrase	Mark Entity Up/Down	Notes
-------------------------------	---------------------	-------

## 6.4.2. SIP Entity for CS1000E

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

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

- **Name:** Enter an identifier for the SIP Entity (e.g., “CS1K”).
- **FQDN or IP Address:** Enter the TLAN IP address of the CS1000E SIP GW.
- **Type:** Select “SIP Trunk”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the **To\_CS1K** Adaptation Module defined in **Section 6.3.1**.
- **Location:** Select the **CS1K** 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**.

AVAYA  
Aura® System Manager 6.3

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

\* Name: CS1K

\* FQDN or IP Address: 172.16.6.110

Type: SIP Trunk

Notes:

Adaptation: To\_CS1K

Location: CS1K

Time Zone: America/New\_York

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

### 6.4.3. SIP Entity for Avaya SBCE

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

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

- **Name:** Enter an identifier for the SIP Entity (e.g., “**A-SBCE**”).
- **FQDN or IP Address:** Enter the IP Address of the Avaya SBCE private side (A1) interface.
- **Type:** Select “**Other**”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the **CS1K\_to\_ATT** Adaptation Module defined in **Section 6.3.2**.
- **Location:** Select the Location **Main** 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).

**Step 4** - Click **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane is expanded to 'Routing', and 'SIP Entities' is selected. The main content area is titled 'SIP Entity Details' and has a 'General' section. The 'Name' field is 'A-SBCE', 'FQDN or IP Address' is '192.168.67.120', 'Type' is 'Other', 'Adaptation' is 'CS1K\_to\_ATT', 'Location' is 'Main', and 'Time Zone' is 'America/New\_York'. The 'SIP Timer B/F (in seconds)' is '4'. The 'SIP Link Monitoring' section is set to 'Use Session Manager Configuration'. There are also checkboxes for 'Supports Call Admission Control' and 'Shared Bandwidth Manager', and dropdowns for 'Primary Session Manager Bandwidth Association' and 'Backup Session Manager Bandwidth Association'.

## 6.5. Entity Links

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

### 6.5.1. Entity Link to CS1000E

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

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

**Step 3** - Click **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation menu is expanded to 'Entity Links'. The main content area shows the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons. Below them is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The row shows: \*CS1K\_5060\_TCP, \*sm63, TCP, \*5060, \*CS1K, a checkbox, \*5060, trusted, a checkbox, and an empty Notes field. Below the table is a 'Select' dropdown set to 'All, None'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
*CS1K_5060_TCP	*sm63	TCP	*5060	*CS1K	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

### 6.5.2. Entity Link to Avaya SBCE

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

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

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation menu is expanded to 'Entity Links'. The main content area shows the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons. Below them is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The row shows: \*A-SBCE\_5060\_TCP, \*sm63, TCP, \*5060, \*A-SBCE, a checkbox, \*5060, trusted, a checkbox, and an empty Notes field. Below the table is a 'Select' dropdown set to 'All, None'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
*A-SBCE_5060_TCP	*sm63	TCP	*5060	*A-SBCE	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

## 6.6. Routing Policies

Routing Policies describe the conditions under which calls will be routed by Session Manager to CS1000E, or Avaya SBCE.

### 6.6.1. Routing Policy to 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 (e.g., “**To\_CS1K**”).
- **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 **CS1K** SIP Entity associated with CS1000E (see **Section 6.4.2**) and click **Select**, and the display returns to the **Routing Policy Details** page.

**Step 3** - In the **Time of Day** section, add an appropriate time of day entry. 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.

AVAYA  
Aura System Manager 6.3  
Last Logged on at December 18, 2013 8:44 A  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

\* Name: To\_CS1K

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K	172.16.6.110	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

**Note** – The Dial Pattern portion of this form will be populated when the Dial Patterns in **Section 6.7** are defined.

## 6.6.2. Routing Policy to 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 (e.g., “A-SBCE\_to\_ATT”).
- **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 **A-SBCE** SIP Entity associated with Avaya SBCE (see **Section 6.4.3**) and click **Select**, and the display returns to the **Routing Policy Details** page.

**Step 3** - In the **Time of Day** section, add an appropriate time of day entry. 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.

AVAYA  
Aura® System Manager 6.3

Last Logged on at December 18, 2013 8:44  
Help | About | Change Password | Log off adm

Home Routing x

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

\* Name: A-SBCE\_to\_ATT

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
A-SBCE	192.168.67.120	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

**Note** – The Dial Pattern portion of this form will be populated when the Dial Patterns in **Section 6.7** are defined.

## 6.7. Dial Patterns

Dial patterns are used to route calls to the appropriate Routing Policies, and ultimately to the appropriate SIP Entities.

**Note** - 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 DNIS numbers used in the Request-URIs are the numbers to be defined here in the **Pattern** fields. In the examples below, an inbound 10 digit DNIS pattern of **732555xxxx** is used. These patterns are also matched, and converted to local extensions, by the CS1000E IDT table (see **Section 5.6**).

### 6.7.1. Inbound AT&T calls to CS1000E Extensions

**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 a matching dial pattern for calls to the CS1000E (e.g., **732555**)
- **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 **Main**, (which covers the Avaya SBCE IP address), defined in **Section 6.2.2**.
- In the **Routing Policies** table, select the **To\_CS1K** Routing Policy defined in **Section 6.6.1**.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

**Step 4** - Click **Commit** to save.

**Step 5** - Repeat **Steps 1-4** as needed for any additional inbound AT&T DNIS number patterns.

**Note** – No **Denied Originating Locations** were specified.

**Note** – The AT&T IP Toll Free service is inbound only, so no outbound dial patterns are specified.



## 7. Avaya Aura® Contact Center

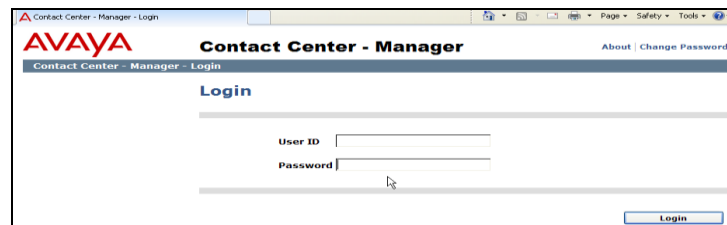
In the reference configuration, Avaya Aura® Contact Center is used to manage Agent functionalities and integrate these functions to the CS1000E.

**Note** - In the reference configuration, Application Module Link (AML) protocol is used between the CS1000E and Avaya Aura® Contact Center. The provisioning and establishment of the AML connection between Avaya Aura® Contact Center and the CS1000E is assumed to be completed. However, SIP based connections are also supported.

**Note** – The installation and initial provisioning of Avaya Aura® Contact Center is beyond the scope of this document (see [11-14] for more information). Only the Agent provisioning supporting the AT&T IP Toll Free solution testing, is shown below.

### 7.1. Create Avaya Aura® Contact Center Agent

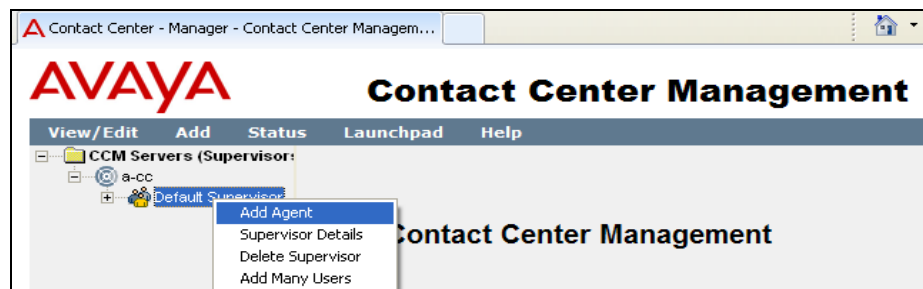
**Step 1** – Log into the Avaya Aura® Contact Center Manager web interface.



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



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



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

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

---

**User Details**

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

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

[Associate User Account](#)

---

**Agent Information**

Primary Supervisor: **Default Supervisor**      Call Presentation: **Call\_Centre\_Administrator**  
 Agent Key:       Threshold: **Agent\_Template**  
 Login Status:       Tn Name:

---

**Contact Types**

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

---

**Skillssets**

Skillset Name (2)	Contact Type	Priority
Default_Skillset	Voice	5
<b>SK2</b>	Voice	<b>1</b>

[Assign Skillssets](#)

---

[Partitions](#)

**Step 5** – Click **Submit** (not shown). Repeat **Steps 1-5** for additional Agents/Skills.

## 7.2. Verify Control DN (CDN) and Agent Connection Status

### 7.2.1. CDN Connection status

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

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

**Step 2** – Select **Configuration**.

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

The screenshot shows the Avaya Configuration web interface. The left-hand menu is expanded to show 'CDNs (Route Points)'. The main content area displays a table titled 'CDNs (Route Points)' with columns: Name, Number, Call Type, Acquired?, and Status. A red box highlights the 'Acquired?' and 'Status' columns for the 'CS1K' entry, which shows 'Acquired' in both fields. A 'Refresh Status' button is visible to the right of the table.

Name	Number	Call Type	Acquired?	Status
CS1K	4013	Local	<input checked="" type="checkbox"/>	Acquired
*			<input type="checkbox"/>	

### 7.2.2. Agent Connection status

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

**Step 2** – Select **Configuration**.

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

The screenshot shows the Avaya Configuration web interface. The left-hand menu is expanded to show 'Phonesets and Voice Ports'. The main content area displays a table titled 'Phonesets/Voice Ports' with columns: Name, Type, Address, Channel, IVR Name, Acquired?, and Status. A red box highlights the 'Acquired?' and 'Status' columns for 'Agent1' and 'Agent2', both of which show 'Acquired' in both fields. A 'Refresh Status' button is visible to the right of the table.

Name	Type	Address	Channel	IVR Name	Acquired?	Status
Agent1	Agent	96-0-1-16			<input checked="" type="checkbox"/>	Acquired
Agent2	Agent	96-0-1-17			<input checked="" type="checkbox"/>	Acquired
*					<input type="checkbox"/>	

## 8. Configure Avaya Session Border Controller for Enterprise

### 8.1. Initial Installation/Provisioning

**Note:** The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [9-10] for additional information.

**IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.**


In the reference configuration, the Avaya SBCE interface B1 (192.168.64.130) was used for the public interface (toward AT&T), and interface A1 (192.168.67.120) was the private network interface.

### 8.2. Log into the Avaya SBCE

The follow provisioning is performed via the Avaya SBCE GUI interface.

**Step 1** - Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).

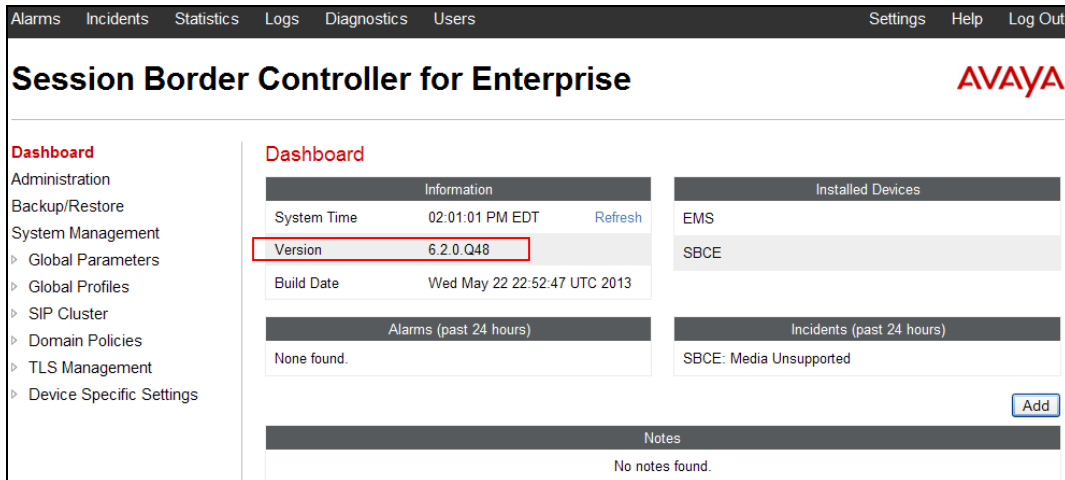
**Step 2** – Enter the appropriate credentials, and click on **Log In**.



The Avaya SBCE Dashboard screen is displayed. All platform navigation is performed from the menu area on the left of the screen. This menu is displayed for all screens.

The platform version used in the reference configuration is displayed in the center of the display (e.g., **6.2.0 Q48**).

**Note** – See **Section 2.2.1, Item 6**, regarding the Avaya SBCE platform version.



## 8.3. Global Profiles

### 8.3.1. Server Interworking – Avaya Side

**Step 1** - Select **Global Profiles** → **Server Interworking** (not shown).

**Step 2** - Select the **Add** button (not shown).

**Step 3** - Enter a profile name (e.g., “Avaya\_SI”) and click on **Finish**. The new profile name will appear on the profile list.

**Step 4** - Select the profile name created above, and then select the **General** Tab (not shown). Scroll down and click on **Edit** (not shown):

- Check **T38 Support** → **Yes**
- All other options on the General Tab can be left at default
- Select **Next**

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

**Next**

**Step 5** - Accept default values on all remaining tabs, then click **Finish** (not shown).

### 8.3.2. Server Interworking – AT&T Side

Repeat the steps shown in **Section 8.3.1** to add an Interworking Profile for the connection to AT&T.

**Step 1** - On the **General** Tab:

- Enter a profile name: (e.g., “**ATT\_SI**”).
- Check **T38 Support**.
- All other options on the General Tab can be left at default.
- Select **Next**.

**Step 2** - Accept default values on all remaining tabs, then click **Finish** (not shown).

### 8.3.3. Routing – Avaya Side

**Step 1** - Select **Global Profiles** → **Routing** from the menu on the left-hand side (not shown).

**Step 2** - Select **Add Profile** (not shown).

**Step 3** - Enter Profile Name: (e.g., “**To\_SM\_RP**”).

**Step 4** - Click **Next** and enter the following:

- Leave **URI Group** with the default \* value.
- Set **Next Hop Server 1**: to **192.168.67.47** (Session Manager IP address).
- Select **Routing Priority Based on Next Hop Server**.
- Set **Outgoing Transport**: to **TCP**.

**Step 5** - Click **Finish**.

The screenshot shows a configuration window titled "Next Hop Routing" with a close button (X) in the top right corner. A blue banner at the top states "Each URI group may only be used once per Routing Profile." The form contains the following fields and options:

- URI Group**: A dropdown menu showing the asterisk (\*) symbol.
- Next Hop Server 1**: A text field containing "192.168.67.47", which is highlighted with a red rectangular box. Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Next Hop Server 2**: An empty text field with the label "IP, IP:Port, Domain, or Domain:Port" below it.
- Routing Priority based on Next Hop Server**: A checkbox that is checked (indicated by a green checkmark).
- Use Next Hop for In Dialog Messages**: An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog**: An unchecked checkbox.
- NAPTR**: An unchecked checkbox.
- SRV**: An unchecked checkbox.
- Outgoing Transport**: Three radio buttons labeled "TLS", "TCP" (which is selected), and "UDP".

A "Finish" button is located at the bottom center of the window.

### 8.3.4. Routing – AT&T Side

Repeat the steps in **Section 8.3.3** to add a Routing Profile for the AT&T primary Border Element.

**Note** – See **Appendix 1** for provisioning a route to the AT&T IP Toll Free service secondary Border Element, if applicable.

**Step 1** - Select **Add Profile**.

**Step 2** - Enter Profile Name: (e.g., “**To\_ATT\_RP**”).

**Step 3** - Click **Next**, then following the procedures shown in **Section 8.3.3**, enter the following:

- Set **Next Hop Server 1**: to **10.10.10.10<sup>4</sup>** (AT&T Border Element IP address).
- Select **Routing Priority Based on Next Hop Server**.
- Set **Outgoing Transport**: to **UDP**.

**Step 4** - Click **Finish**. The completed form is shown below.

The screenshot shows a web interface for configuring Routing Profiles. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, and Routing. The main area is titled 'Routing Profiles: To\_ATT\_RP' and contains a table of profiles. The 'To\_ATT\_RP' profile is selected and expanded, showing a table with one entry: Priority 1, URI Group \*, Next Hop Server 1 10.10.10.10, and Next Hop Server 2. There are buttons for 'Add', 'Rename', 'Clone', and 'Delete' at the top right of the profile list.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	10.10.10.10	

### 8.3.5. Server Configuration –Session Manager

**Step 1** - Select **Global Profiles → Server Configuration** from the menu on the left-hand side (not shown).

**Step 2** - Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., “**SM\_SC**”) and select **Next**.

**Step 3** - The **Add Server Configuration Profile - General** window will open (not shown). Enter the following:

- Set **Server Type**: to **Call Server**.
- Set **IP Address**: to **192.168.67.47** (Session Manager IP Address).
- For **Supported Transports**: check **UDP** and **TCP**.
- Set **TCP Port**: to **5060**.
- Set **UDP Port**: to **5060**.
- Select **Next**.

**Step 4** - The **Authentication** window will open (not shown). Select **Next** to accept default values.

**Step 5** - The **Heartbeat** window will open (not shown). Select **Next** to accept remaining default values.

<sup>4</sup> See the note in **Section 3.1** regarding this address

**Step 6** - The **Advanced** window will open.

- Select **Enable Grooming**.
- For **Interworking Profile** select **Avaya\_SI** created in **Section 8.3.1**.
- For the **Signaling Manipulation Script** select the **CS1K\_headers** script defined in **Section 8.3.9**.
- Select **Finish**, accepting remaining default values.

The following screen shots show the completed **General** and **Advanced** tabs.

The screenshot shows the 'Server Configuration: SM\_SC' window with the 'General' tab selected. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main area displays the following configuration:

Property	Value
Server Type	Call Server
IP Addresses / FQDNs	192.168.67.47
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060
TLS Port	

Buttons: Add, Rename, Clone, Delete, Edit.

The screenshot shows the 'Server Configuration: SM\_Trunk\_SC' window with the 'Advanced' tab selected. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main area displays the following configuration:

Property	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya_SI
TLS Client Profile	
Signaling Manipulation Script	CS1K_headers
TCP Connection Type	SUBID
UDP Connection Type	SUBID
TLS Connection Type	SUBID

Buttons: Add, Rename, Clone, Delete, Edit.

### 8.3.6. Server Configuration –AT&T Primary Border Element

**Note** – See **Appendix 1** for configuration of a Secondary AT&T IP Toll Free order Element, if applicable.

Repeat the steps in **Section 8.3.5** to create a Server Configuration for the connection to the AT&T primary Border Element, using the following entries:

**Step 1** - In the **Profile Name** window enter a Profile Name (e.g., “**ATT\_Primary\_SC**”) and select **Next**.

**Step 2** – In the **Add Server Configuration Profile - General** window for **Server Type**: select **Trunk Server**.

- Enter **IP Address: 10.10.10.10<sup>5</sup>** (AT&T IP Toll Free primary border element).
- For **Supported Transports**: check **UDP**
- For **UDP Port**: enter **5060**
- Select **Next**

**Step 3** - Accept default values for the **Add Server Configuration Profile - Authentication** and **Heartbeat** windows (not shown).

**Step 4** – The **Add Server Configuration Profile - Advanced** window will open.

- Select **ATT\_SI** for **Interworking Profile** (created in **Section 8.3.2**).
- For the **Signaling Manipulation Script** select the **CS1K\_TO\_Header\_and\_Maxptime** script that was defined in **Section 8.3.9**.

**Step 5** - Select **Finish**.

The following screens show the completed **General** and **Advanced** tabs.

The screenshot shows the 'Server Configuration: ATT\_Primary\_SC' window with the 'General' tab selected. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main content area shows the following configuration:

Field	Value
Server Type	Trunk Server
IP Addresses / FQDNs	10.10.10.10
Supported Transports	UDP
UDP Port	5060

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

The screenshot shows the 'Server Configuration: ATT\_Secondary\_SC' window with the 'Advanced' tab selected. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main content area shows the following configuration:

Field	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	CS1K_TO_Header_and_Maxptime
UDP Connection Type	SUBID

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

### 8.3.7. Topology Hiding – Avaya Side

**Step 1** - Select **Global Profiles → Topology Hiding** from the menu on the left-hand side (not shown).

**Step 2** - Click **default** profile and select **Clone Profile**.

**Step 3** - Enter Profile Name: (e.g., “**Avaya\_TH**”). Enter the following:

- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**

<sup>5</sup> See the note in **Section 3.1** regarding this address

- In the **Replace Action** column select: **Overwrite**
- In the **Overwrite Value** column: **cots1.ntlab.com**
- Repeat for the Header **From**
- Repeat for the Header **Request Line**

**Step 4** - Click **Finish** (not shown).

Dashboard  
Administration  
Backup/Restore  
System Management  
Global Parameters  
Global Profiles  
Domain DoS  
Fingerprint  
Server Interworking  
Phone Interworking  
Media Forking  
Routing  
Server Configuration  
**Topology Hiding**  
Signaling Manipulation  
URI Groups

Topology Hiding Profiles: Avaya\_TH

Add

Topology Hiding Profiles: default

Avaya\_TH

Click here to add a description.

Topology Hiding

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

Edit

### 8.3.8. Topology Hiding – AT&T Side

Create a **Topology Hiding Profile** for the connection to AT&T, by repeating the steps in **Section 8.3.7** with the following changes:

- Enter **Profile Name**: (e.g., “**ATT\_TH**”).
- Use the default **Replace Action** setting of **Auto**.
- Click **Finish**.

Dashboard  
Administration  
Backup/Restore  
System Management  
Global Parameters  
Global Profiles  
Domain DoS  
Fingerprint  
Server Interworking  
Phone Interworking  
Media Forking  
Routing  
Server Configuration  
**Topology Hiding**  
Signaling Manipulation  
URI Groups

Topology Hiding Profiles: default

Add

Topology Hiding Profiles: default

ATT\_TH

Avaya\_TH

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Topology Hiding

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

Edit

### 8.3.9. Signaling Manipulation

The Avaya SBCE can manipulate inbound and outbound SIP headers. In the reference configuration, two signaling manipulation scripts are used; **CS1K\_TO\_Header\_and\_Maxptime** and **CS1K\_headers**.

**Note** – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 8.4.3**) does not meet the desired result. Refer to **[10]** for information on the Avaya SBCE scripting language.

#### 8.3.9.1 CS1K\_TO\_Header\_and\_Maxptime

Calls can be made directly into Call Pilot® (e.g., to check/retrieve messages, or access an Auto Attendant). Call Pilot® checks the contents of the INVITE TO header as part of admission control. However while AT&T sends the unique DNIS number in the INVITE R-URI, it will send the customers Billing Number in the TO header of all INVITES. Therefore the Avaya SBCE is used to copy the contents of the R-URI, into the TO header, so that Call Pilot® can apply admission control successfully (see **Section 2.2.1, Item 5**). The script then returns the TO header back to the Billing number in messages sent back to AT&T. See **Section 5.10** for additional provisioning required in Call Pilot® to accept call to check/retrieve messages.

In addition, as described in **Section 2.2.1, Item 1**, AT&T sends INVITES with the SIP parameter *maxptime:30*. In response, Avaya CS1000E will send *ptime:10* for any UNISim or digital stations. The Avaya SBCE is used to change the *maxptime:30* parameter to *ptime:30*, thereby making Avaya CS1000E respond with *ptime:30* as required.

**Step 1** - Select **Global Profiles → Signaling Manipulation** from the menu on the left-hand side of the screen (not shown).

**Step 2** - Click **Add Script** (not shown) and the script editor window will open.

Enter a name for the script in the **Title** box (e.g., “**CS1K\_TO\_Header\_and\_Maxptime**”). Enter the script body as shown below.

**Step 3** - Click on **Save**. The script editor will test for any errors, and the Edit window will close. This script is applied to the AT&T Server Configuration in **Section 8.3.6, Step 4**.

The completed script is shown below.

```
// Replace inbound TO header billing number with RURI DNIS number for CS1K.
Apply to AT&T side.

within session "ALL"
{
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{
// Replace Billing number in "TO" with "REQUEST-LINE" number

%touser = %HEADERS["To"][1].URI.USER;

%HEADERS["To"][1].URI.USER = %HEADERS["Request_Line"][1].URI.USER;
}
}
// Return ?TO? header to original form
within session "ALL"
{
act on response where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%HEADERS["To"][1].URI.USER = %touser;
}
}

// 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");
}
}
}
```

### 8.3.9.2 CS1K\_headers

As described in **Section 2.2.1, Item 5**, the Avaya CS1000E inserts a telephone event type of 111 which AT&T does not support. This value is removed via the following script. In addition, in some call scenarios the Avaya CS1000E may insert a leading + in the calling/called number fields. This is also not required by AT&T, and is removed.

- Select **Global Profiles → Signaling Manipulation** from the menu on the left-hand side of the screen (not shown).
- Click **Add Script** (not shown) and the script editor window will open.
- Enter a name for the script in the **Title** box (e.g., “**CS1K\_headers**”). Enter the script body as shown below.
- Click on **Save**. The script editor will test for any errors, and the Edit window will close. This script is applied to the Avaya Server Configuration in **Section 8.3.5, Step 6**.

```
// Removes 111 telephone event. Apply to CPE side.
// Remove 111 from CS1K requests

within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %BODY[1].regex_replace("100 111","100");
    %BODY[1].regex_replace("a=rtpmap:111","");
    %BODY[1].regex_replace("101 111","101");
  }
}

// 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","");
    %BODY[1].regex_replace("101 111","101");
  }
}

// Remove plus sign from From, Contact, and PAI

within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %HEADERS["Request_Line"][1].regex_replace("\+", "");
    %HEADERS["From"][1].regex_replace("\+", "");
    %HEADERS["Contact"][1].regex_replace("\+", "");
    %HEADERS["P-Asserted-Identity"][1].regex_replace("\+", "");
  }
}
}
```

The screen below shows the completed Signaling Manipulations form.

The screenshot shows a web application interface for managing signaling manipulation scripts. On the left is a sidebar with a navigation menu. The main content area is titled 'Signaling Manipulation Scripts: CS1K\_headers'. It features a list of scripts on the left and a large text area on the right for editing a script. The script being edited is 'CS1K\_headers' and contains the same code as shown in the previous block. The interface includes buttons for 'Upload', 'Add', 'Download', 'Clone', and 'Delete'.

## 8.4. Domain Policies

### 8.4.1. Application Rules

**Step 1** - Select **Domain Policies** → **Application Rules** from the menu on the left-hand side menu (not shown).

**Step 2** - Select the **default** Rule

**Step 3** - Select **Clone Rule** button

- For **Name**: enter “**SIP\_Trunk\_AR**”
- Click **Finish**

**Step 4** - Highlight the rule **SIP\_Trunk\_AR** just created, and click the **Edit** button.

- In the **Voice** row:
  - Change the **Maximum Concurrent Sessions** to an appropriate amount (e.g., **2000**)
  - Change the **Maximum Sessions per Endpoint** to an appropriate amount (e.g.,**2000**)
  - Set **CDR Support** to **None**.
  - Click on **Finish**.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	<input checked="" type="radio"/> None <input type="radio"/> CDR w/ RTP <input type="radio"/> CDR w/o RTP
RTCP Keep-Alive	<input type="checkbox"/>

Finish

### 8.4.2. Media Rules

#### 8.4.2.1 Avaya Media Rule

**Step 1** - Select **Domain Policies** → **Media Rules** from the menu on the left-hand side menu (not shown).

**Step 2** - From the Media Rules menu, select the **default-low-med** rule

**Step 3** - Select **Clone Rule** button

- Name: **Avaya\_trunk\_low\_med**
- Click **Finish**

**Step 4** - Highlight the **Avaya\_trunk\_low\_med** rule just created, select the **Media QOS** tab, and click the **Edit** button.

- Check the **Media QoS Marking - Enabled**
- Select the **DSCP** box
- **Audio:** Select **AF11** from the drop-down
- **Video:** Select **AF11** from the drop-down

**Step 5** - Click **Finish** (not shown).

#### 8.4.2.2 AT&T Media Rule

**Step 1** – Repeat the steps in **Section 8.4.2.1** with the following changes:

- Name: **ATT\_low\_med**

**Step 2** - Click **Finish** (not shown).

#### 8.4.3. Signaling Rules

As described in **Section 2.2.1, Item 2**, the Avaya SBCE is used to help reduce packet size by removing SIP headers not required by AT&T.

##### 8.4.3.1 Avaya - Requests

**Step 1** - Select **Domain Policies** → **Signaling Rules** from the menu on the left-hand side menu (not shown).

**Step 2** - From the Signaling Rules menu, select the **default** rule.

**Step 3** - Select **Clone Rule** button

- Enter a name: **CS1K\_SR\_with\_SM**
- Click **Finish**

**Step 4** - Select the **CS1K\_SR\_with\_SM** rule and do the following:

- Select the **Request Headers** tab (not shown), and select the **Add In Header Control** button (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open (not shown).
- Check the **Proprietary Request Header** box.

- From the **Header Name** menu select **P-Location**.
- From the **Method Name** menu select **All**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**

**Step 5** - Repeat **Step 4** to create a rule to remove the **P-AV-Message-ID**, **P-Location**, and **x-nt.E164-clid** proprietary headers.

**Step 6** - Repeat **Step 4** to remove the **Alert-Info**, **History-Info**, and **Remote-Party-ID** non proprietary headers.

- Do not check the **Proprietary Request Header** box.

The completed form is shown below. Note that all the entries in the **Direction** column says **In**.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	AV-Global-Session-Id	ALL	Forbidden	Remove Header	Yes	IN
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN
3	History-Info	ALL	Forbidden	Remove Header	No	IN
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN
6	Remote-Party-ID	ALL	Forbidden	Remove Header	No	IN
7	x-nt-e164-clid	ALL	Forbidden	Remove Header	Yes	IN

### 8.4.3.2 Avaya - Responses

Following the steps shown in **Section 8.4.3.1**, Response Signaling Rules are defined to remove **AV-Global-Session-ID**, **History-Info**, **P-AV-Message-ID**, **Remote-Party-ID**, and **P-Location** headers for both **1xx** and **2xx** responses.

**Step 1** - Highlight the **CS1K\_SR\_with\_SM** rule created in **Section 8.4.3.1** and enter the following to remove the **AV-Global-Session-ID** proprietary header from **1XX** responses.

- Select the **Response Headers** tab (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- From the **Header Name** menu enter **AV-Global-Session-ID**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **All**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**

**Step 2** - Repeat **Step 1** to create rules to remove the **P-AV-Message-ID**, **Remote-Party-ID**, and **P-Location** proprietary headers for **1xx** responses.

**Step 3** - Repeat **Step 2** to create rules to remove the **History-Info** and **Remote-Party-ID** *non-proprietary* headers for **1xx** responses.

- Do *not* check the **Proprietary Request Header** box.

**Step 4** - Repeat **Step 1** to create rules to remove **AV-Global-Session-ID**, **P-AV-Message-ID**, and **P-Location** proprietary headers for **2xx** responses

- From the **Response Code** menu select **2xx**.

**Step 5** - Repeat **Step 4** to create rules to remove **History-Info**, and **Remote-Party-ID** non-proprietary headers for **2xx** responses

- Do *not* check the **Proprietary Request Header** box.

The completed form is shown below. Note that all the entries in the **Direction** column says **In**.

**Signaling Rules: CS1K\_SR\_with\_SM**

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Click here to add a description.

Tabs: General, Requests, Responses, Request Headers, **Response Headers**, Signaling QoS

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	History-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
4	History-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	Remote-Party-ID	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
10	Remote-Party-ID	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

### 8.4.3.3 AT&T – Requests

**Step 1** – Follow the steps in **Section 8.4.3.1**, and create a Request rule called **ATT\_SR**.

**Step 2** - Select the **ATT\_SR** rule and do the following:

- Select the **Request Headers** tab (not shown), and select the **Add In Header Control** button (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open (not shown).
- Do *not* check the **Proprietary Request Header** box.
- From the **Header Name** menu select **Resource-Priority**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**

Dashboard  
Administration  
Backup/Restore  
System Management  
  > Global Parameters  
  > Global Profiles  
  > SIP Cluster  
  4 Domain Policies  
    Application Rules  
    Border Rules  
    Media Rules  
    Security Rules  
    **Signaling Rules**

**Signaling Rules: ATT\_SR**

Add Filter By Device... Rename Clone Delete

Signaling Rules  
default  
CS1K\_SR\_with\_SM  
**ATT\_SR**

Click here to add a description.

General Requests Responses **Request Headers** Response Headers Signaling QoS

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Resource-Priority	INVITE	Forbidden	Remove Header	No	IN	Edit Delete

#### 8.4.3.4 Avaya – Signaling QOS

**Step 1** - Highlight the **CS1K\_SR\_with\_SM** rule created in **Section 8.4.3.1** and enter the following:

- Select the **Signaling QOS** tab (not shown).
- Click the **Edit** button and the **Signaling QOS** window will open.
- Select the **Enabled** option.
- Select **DCSP**.
- Select **Value = AF11**.
- Click **Finish**.

**Signaling QoS**

Signaling QoS

Enabled ☒

ToS

Precedence

ToS

DSCP

Value

Finish

#### 8.4.3.5 AT&T – Signaling QOS

**Step 1** - Highlight the **ATT\_SR** rule created in **Section 8.4.3.3** and repeat the procedure in **Section 8.4.3.4**.

#### 8.4.4. Endpoint Policy Groups – Avaya

**Step 1** - Select **Domain Policies → End Point Policy Groups** from the menu on the left-hand side (not shown).

**Step 2** - Select **Add** (not shown).

- For **Name**: enter “**Avaya\_default\_low\_PG**”, then click **Next**.
- For **Application Rule**: select **SIP\_Trunk\_AR** (see **Section 8.4.1**).
- For **Border Rule**: select **default**.
- For **Media Rule**: select **Avaya\_Trunk\_low\_med** (see **Section 8.4.2**).
- For **Security Rule**: select **default-low**.

- For **Signaling Rule**: select **CS1K\_SR\_with\_SM** (see Section 8.4.3).
- For **Time of Day**: select **default**.

**Step 3** - Select **Finish**.

Application Rule	SIP_Trunk_AR
Border Rule	default
Media Rule	Avaya_Trunk_low_med
Security Rule	default-low
Signaling Rule	CS1K_SR_with_SM
Time of Day Rule	default

Finish

### 8.4.5. Endpoint Policy Groups – AT&T

**Step 1** – Repeat the steps in Section 8.4.4 with the following setting changes:

- For **Name**: enter “**ATT\_default\_low\_PG**”
- For **Signaling Rule**: select **ATT\_SR** (see Section 8.4.3).

**Step 2** - Select **Finish** (not shown).

**Policy Groups: ATT\_default-low\_PG**

Filter By Device...

Click here to add a description.

Click here to add a row description.

**Policy Group**

Order	Application	Border	Media	Security	Signaling	Time of Day
1	SIP_Trunk_AR	default	ATT_low_med	default-low	ATT_SR	default

## 8.5. Device Specific Settings

### 8.5.1. Network Management

**Step 1** - Select **Device Specific Settings** → **Network Management** from the menu on the left-hand side.

**Step 2** – Select the **Network Configuration** tab. The network interfaces were provisioned during installation. However if these values need to be modified, do so via this tab. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab.

The screenshot displays the 'Network Management: SBCE' web interface. On the left is a navigation menu with categories like Dashboard, Administration, System Management, and Device Specific Settings. The 'Network Management' option is highlighted. The main content area has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: '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.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.0), and 'B2 Netmask'. An 'Add' button is present. Below these fields is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains two rows of data. The first row shows IP Address 192.168.67.120, Gateway 192.168.67.1, and Interface A1. The second row shows IP Address 192.168.64.130, Gateway 192.168.64.254, and Interface B1. Each row has a 'Delete' button next to the interface name.

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

### 8.5.2. Media Interface

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 recommended by AT&T.

**Step 1** - Select **Device Specific Settings** → **Media Interface** from the menu on the left-hand side, click on **Add**, and enter the following:

- For **Name**: enter “**Inside\_Trunk\_MI**”
- For **Media IP**: enter **192.168.67.120** (Avaya SBCE internal address toward Session Manager).
- For **Port Range**: enter **16384 - 32767**

**Step 2** - Click **Finish** (not shown)

**Step 3** – Repeat **Step 1** with the following changes:

- For **Name**: enter “**Outside\_Trunk\_MI**”
- For **Media IP**: enter **192.168.64.130** (Avaya SBCE external address toward AT&T)

**Step 4** - Click **Finish** (not shown)

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface

Media Interface: SBCE

Devices
SBCE

Media Interface

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

Add

Name	Media IP	Port Range		
Inside_Trunk_MI	192.168.67.120	16384 - 32767	Edit	Delete
Outside_Trunk_MI	192.168.64.130	16384 - 32767	Edit	Delete

### 8.5.3. Signaling Interface

**Step 1** - Select **Device Specific Settings** → **Signaling Interface** from the menu on the left-hand side.

**Step 2** - Select **Add** , and enter the following:

- For **Name**: enter “**Inside\_Trunk\_SI**”
- For **Media IP**: enter **192.168.67.120** (Avaya SBCE internal address toward Session Manager)
- For **TCP Port**: enter **5060**
- For **UDP Port**: enter **5060**

**Step 3** - Click **Finish** (not shown).

**Step 4** – Repeat Step 2 with the following changes:

- For **Name**: enter “**Outside\_Trunk\_SI**”
- For **Media IP**: enter **192.168.64.130** (Avaya SBCE external address toward AT&T).
- For **UDP Port**: enter **5060**

**Step 3** - Click **Finish** (not shown).

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface

Signaling Interface: SBCE

Devices
SBCE

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Inside_Trunk_SI	192.168.67.120	5060	5060	---	None	Edit	Delete
Outside_Trunk_SI	192.168.64.130	---	5060	---	None	Edit	Delete

### 8.5.4. Endpoint Flows – Avaya (Session Manager)

**Step 1** - Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side.

**Step 2** - Select the **Server Flows** tab

**Step 3** - Select **Add**, and enter the following:

- For **Name**: enter “**Avaya\_Trunk**”
- For **Server Configuration**: select **SM\_SC** (see **Section 8.3.5**)
- For **URI Group**: enter \* (default)

- ### Step 4 - Click **Finish** (not shown)

**Note** – See **Appendix 1** for provisioning an Endpoint Flow for the AT&T IPFR-EF service secondary Border Element, if applicable.

- For **Name**: enter “ATT\_Primary”
- For **Server Configuration**: select ATT\_Primary\_SC (see Section 8.3.6)
- For **Received Interface**: select Inside\_Trunk\_SI (see Section 8.5.3)
- For **Signaling Interface**: select Outside\_Trunk\_SI (see Section 8.5.3)
- For **Media Interface**: select Outside\_Trunk\_MI (see Section 8.5.2)
- For **End Point Policy Group**: select ATT\_default\_low\_PG (see Section 8.4.5)
- For **Routing Profile**: select To\_SM\_RP (see Section 8.3.3)
- For **Topology Hiding Profile**: select ATT\_TH (see Section 8.3.8)

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
**End Point Flows**
Session Flows
Relay Services
SNMP

## End Point Flows: SBCE

Devices

SBCE

Subscriber Flows

Server Flows

Click here to add a row description.

Server Configuration: ATT\_Primary\_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ATT_Primary	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default_low_PG	default	View Clone Edit Delete

Server Configuration: SM\_SC

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default_low_PG	To_ATT_VIT	View Clone Edit

## 9. Verification Steps

The following steps may be used to verify the configuration.

### 9.1. General

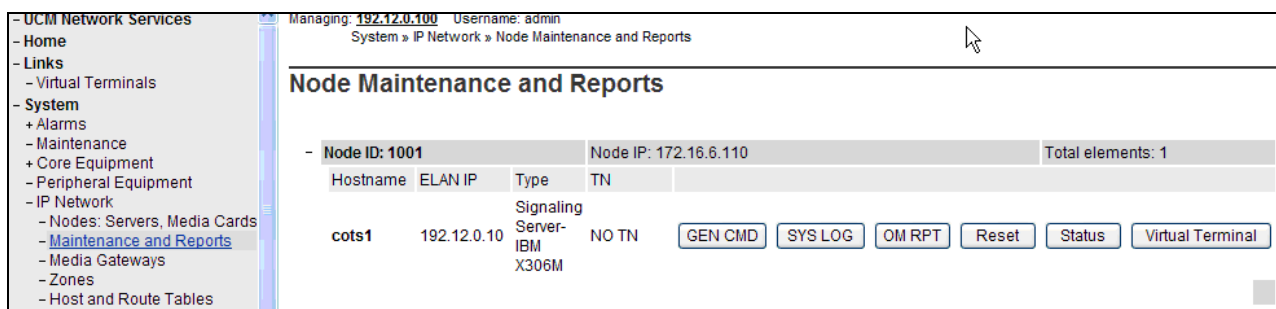
- [1] Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly.
- [2] Place an inbound call to an agent or telephone, but do not answer the call. Verify that the call covers to Call Pilot<sup>®</sup>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

### 9.2. Avaya CS1000E Verifications

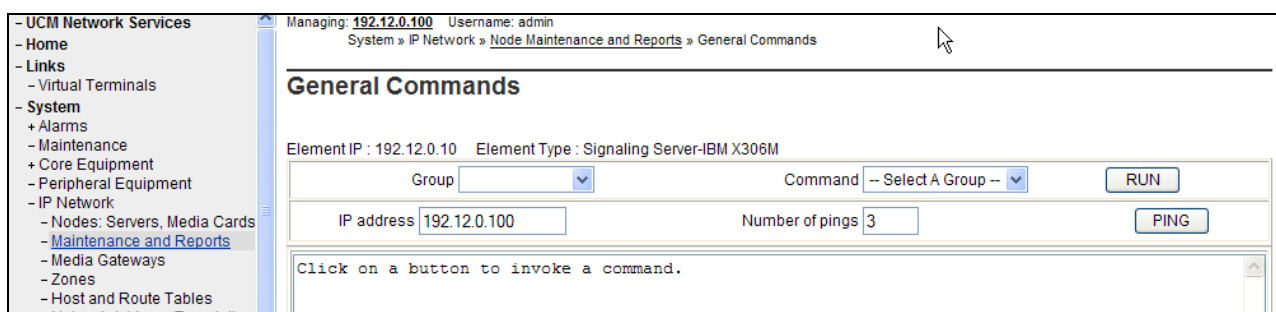
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

#### 9.2.1. IP Network Maintenance and Reports Commands

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



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



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

For example, 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 (192.168.67.47, port 5060, TCP) has “SIPNPM Status” Active.

**General Commands**

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

Group **Sip** Command **SIPGwShow** **Sip** **RUN**

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

```

SIPNPM Status           : Active
Primary Proxy IP address : 192.168.67.47
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 : 192.168.67.47
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
  
```

The following screen shows a method to view IP UNISim telephone status. The screen shows the output of the **Command** “isetShow” in **Group** “Iset”. At the time this screen was captured, the first UNISim telephone listed was involved in an active call with PSTN via the AT&T IP Toll Free service.

**General Commands**

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

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

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

Set Information

IP Address	NAT	Model Name	Type	RegType	State	Up
172.16.6.107		1140E IP Deskphone	1140	Regular	busy	2
172.16.6.108		2004 Phase 2 IP Deskphone	2004P2	Regular	online	2
172.16.6.104		1150E IP Deskphone	1150	Regular	online	2
172.16.6.109		1140E IP Deskphone	1140	Regular	online	2

Total sets = 4

## 9.2.2. System Maintenance Commands

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

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-Channels **15** (SIP GW) and **20** (SIPLINE), show as established (**EST**) and active (**ACTV**).

**D-Channel Diagnostics**

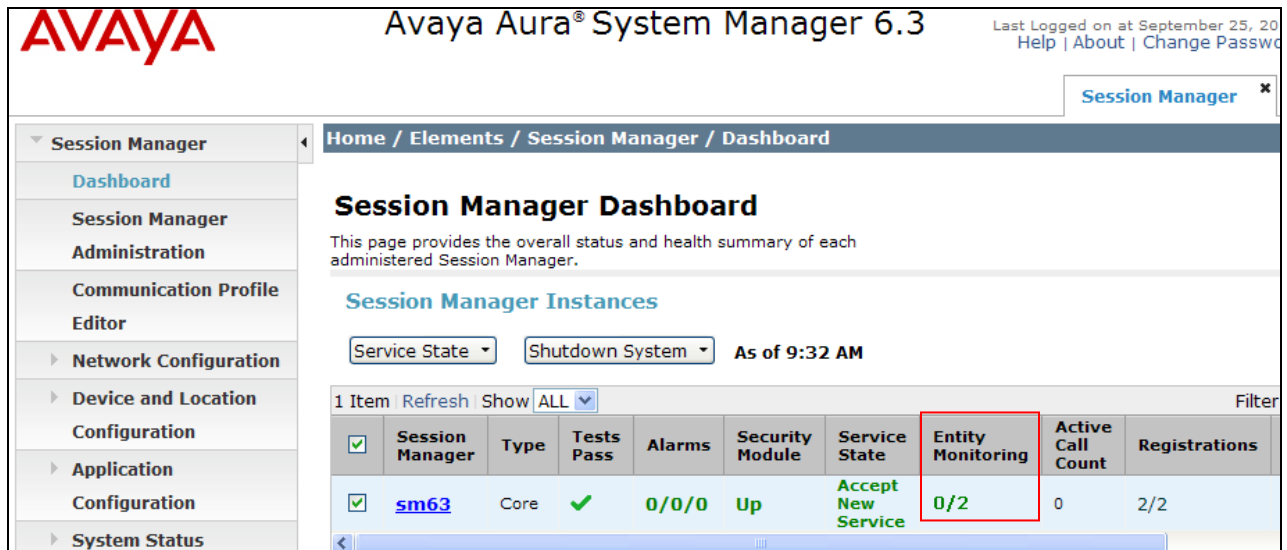
Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	<input type="button"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

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_REC	PDCH	BDCH
<input type="radio"/> 015	VDCH	OPER	EST	ACTV	AUTO	
<input type="radio"/> 020	SIPLINE	OPER	EST	ACTV	AUTO	

## 9.3. System Manager / Session Manager Verification

### 9.3.1. Verify Service State and Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** and the Dashboard screen is displayed. Verify that the **Service State** column shows “Accept New Service”, and the **Entity Monitoring** column shows “0” Entities are down.



Avaya Aura® System Manager 6.3

Last Logged on at September 25, 2014  
Help | About | Change Password

Session Manager

Session Manager Dashboard

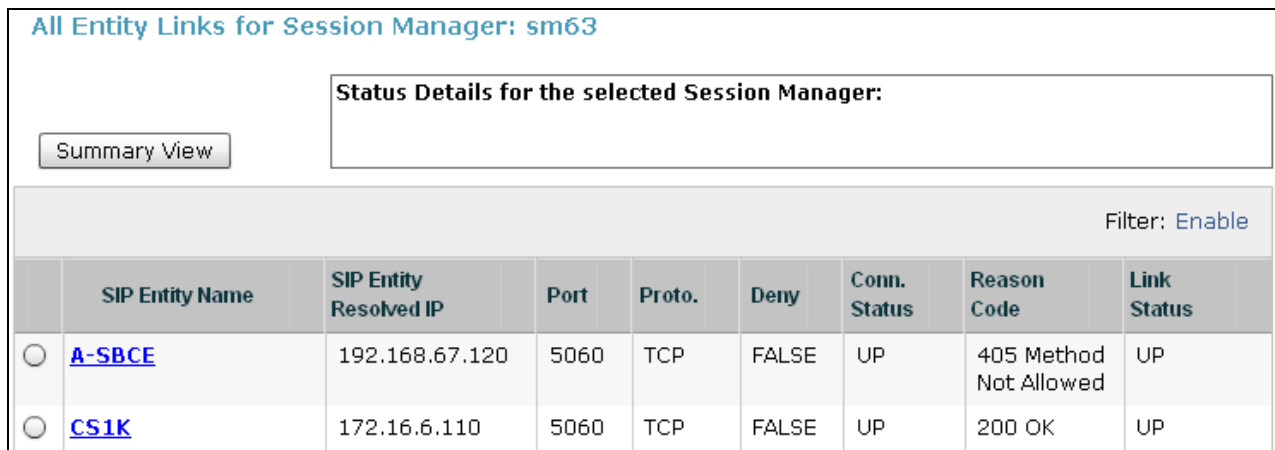
This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State Shutdown System As of 9:32 AM

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations
sm63	Core	✓	0/0/0	Up	Accept New Service	0/2	0	2/2

Click on the **Entity Monitoring** display (e.g., 0/2), and a list of all the provisioned SIP Entities, and their states, are displayed. Under normal operating conditions, the **Conn. Status** should be “Up” as shown in the example screen below. The **Reason Code** column indicates that the Avaya SBCE 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.



All Entity Links for Session Manager: sm63

Status Details for the selected Session Manager:

Summary View

Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	A-SBCE	192.168.67.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP
<input type="radio"/>	CS1K	172.16.6.110	5060	TCP	FALSE	UP	200 OK	UP

### 9.3.2. Call Routing Test

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

The following screen shows an example call routing test for an inbound call to the Avaya CS1000E from PSTN/AT&T.

### 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**  
sm63

**Calling Party Address**  
192.168.67.125

**Session Manager Listen Port**  
5060

**Transport Protocol**  
TCP

Execute Test

#### Routing Decisions

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

#### Routing Decision Process

NRP Adaptations: CS1K\_AT&T\_AA-SBC applied.  
BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.  
Originating Location is AA-SBC. Using digits < 7325554383 > and host < cots1.ntlab.com > for routing.  
NRP Dial Patterns: No matches for digits < 7325554383 > and domain < cots1.ntlab.com >.  
NRP Dial Patterns: No matches for digits < 7325554383 > and domain < ntlab.com >.  
NRP Dial Patterns: Found a Dial Pattern match for pattern < 732555 > Min/Max length 10/10 and domain < null >.  
NRP Routing Policies: Ranked destination NRP Sip Entities: CS1K  
NRP Routing Policies: Removing disabled routes.  
NRP Routing Policies: Ranked destination NRP Sip Entities: CS1K  
END EMERGENCY CALL CHECK: This is not an emergency call.  
Adapting and proxying for SIP Entity CS1K.  
NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.  
NRP Adaptations: CS1K applied.  
NRP Adaptations: Request-URI set to sip:4094@cots1.ntlab.com  
NRP Adaptations: Request URI set to sip:4094@cots1.ntlab.com  
Route < sip:4094@cots1.ntlab.com > to SIP Entity CS1K (172.16.6.110). Terminating Location is CS1K.

## 9.4. Protocol Traces

This section illustrates an example inbound call from PSTN/AT&T IP Toll Free service to DNIS 7325551234 (this number is associated with a CS1000E Directory Number 4096).

1. The following Wireshark trace was captured on the **public** side of the Avaya SBCE (to AT&T), filtered on SIP messages. The INVITE message sent by AT&T to the Avaya SBCE is selected. As can be observed in the example below:
  - The AT&T IP Toll Free service sends the INVITE with the DNIS number **7325551234** in the R-URI; however the Billing number **8885555821** is in the TO header, (used for all calls to this customer).
  - Note that the **maxptime=30** parameter is specified with no ptime parameter.

No.	Time	Source	Destination	Protocol	Info
11	27.229	10.10.10.10	192.168.64.130	SIP/SDP	Request: INVITE sip:7325551234@192.168.64.130:5060, with
* Frame 11: 1082 bytes on wire (8656 bits), 1082 bytes captured (8656 bits)					
+ Ethernet II, Src: Cisco_29:e4:a0 (a4:93:4c:29:e4:a0), Dst: Intel_31:1b:e9 (90:e2:ba:31:1b:e9)					
+ Internet Protocol Version 4, Src: 135.25.29.74 (135.25.29.74), Dst: 135.16.170.55 (135.16.170.55)					
+ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)					
+ Session Initiation Protocol					
+ Request-Line: INVITE sip:7325551234@192.168.64.130:5060 SIP/2.0					
+ Message Header					
+ Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK9rekqi00400h1rgeu070.1					
+ MIME-Version: 1.0					
+ Supported: replaces					
+ Allow: INVITE, BYE, ACK, CANCEL, PRACK, INFO, REFER					
+ Accept: application/sdp					
+ Accept: application/isup					
+ Accept: application/dtmf					
+ Accept: application/dtmf-relay					
+ Accept: multipart/mixed					
+ Privacy: none					
+ P-Asserted-Identity: <sip:7325551000@10.10.10.10 >					
+ From: <sip:8185551111@10.10.10.10 >;isup-oli=00;tag=905771306713283_c1b09.1.1.1379097345250.0_296_1141					
+ To: <sip:8885551111@192.168.64.130>					
+ Call-ID: 47033942349966296@c1b09_1_1					
+ Max-Forwards: 66					
+ CSeq: 2 INVITE					
+ Content-Type: application/sdp					
+ Content-Length: 309					
+ Contact: <sip:10.10.10.10 :5060;transport=udp>					
+ Message Body					
+ Session Description Protocol					
+ Session Description Protocol Version (v): 0					
+ Owner/Creator, Session Id (o): Sonus_UAC 13439 1270 IN IP4 10.10.10.10					
+ Session Name (s): SIP Media Capabilities					
+ Connection Information (c): IN IP4 10.10.10.10					
+ Time Description, active time (t): 0 0					
+ Media Description, name and address (m): audio 17950 RTP/AVP 18 0 2 100					
+ Media Attribute (a): rtpmap:18 G729/8000					
+ Media Attribute (a): fmtp:18 annexb=no					
+ Media Attribute (a): rtpmap:0 PCMU/8000					
+ Media Attribute (a): rtpmap:2 G726-32/8000					
+ Media Attribute (a): rtpmap:100 telephone-event/8000					
+ Media Attribute (a): fmtp:100 0-15					
+ Media Attribute (a): sendrecv					
+ Media Attribute (a): maxptime:30					

2. The following trace captured on the **private** side of the Avaya SBCE (to the CPE), filtered on SIP messages. The same INVITE message sent by AT&T is selected, though it is now sent by the Avaya SBCE to Session Manager (then to the CS1000E). As can be observed in the example below:

- The contents of the R-URI (**7325551234**) have been copied into the TO header, and the **maxptime=30** parameter has been changed to **ptime=30** by the signaling manipulation defined in **Section 8.3.9**.

No.	Time	Source	Destination	Protocol	Length	Info
111	11.448091	192.168.67.120	192.168.67.47	SIP/SDP	1131	Request: INVITE sip:0000011051@
Frame 111: 1131 bytes on wire (9048 bits), 1131 bytes captured (9048 bits)						
Ethernet II, Src: Intel_31:1b:ed (90:e2:ba:31:1b:ed), Dst: Ibm_40:56:90 (e4:1f:13:40:56:90)						
Internet Protocol Version 4, Src: 192.168.67.120 (192.168.67.120), Dst: 192.168.67.47 (192.168.67.47)						
Transmission Control Protocol, Src Port: 13486 (13486), Dst Port: sip (5060), Seq: 2, Ack: 1, Len: 1077						
Session Initiation Protocol						
Request-Line: INVITE sip:7325551234@cots1.ntlab.com>IP/2.0						
Message Header						
From: <sip:8185551111@cots1.ntlab.com>isup-oli=00;tag=905771306713283_c1b09.1.1.1379097345250.0_296_1141						
To: <sip:7325551234@cots1.ntlab.com>						
CSeq: 2 INVITE						
Call-ID: 49717a26ace85b720d87c06955e0d647						
Contact: <sip:192.168.67.120:5060;transport=tcp>						
Record-Route: <sip:192.168.67.120:5060;ipcs-line=10425;lr;transport=tcp>						
Allow: INVITE, BYE, ACK, CANCEL, PRACK, INFO, REFER						
Supported: replaces						
Max-Forwards: 65						
Via: SIP/2.0/TCP 192.168.67.120:5060;branch=z9hG4bK-s1632-002139069330-1--s1632-						
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay, multipart/mixed						
MIME-Version: 1.0						
Privacy: none						
P-Asserted-Identity: <sip:7325551000@cots1.ntlab.com>						
Content-Type: application/sdp						
Content-Length: 291						
Message Body						
Session Description Protocol						
Session Description Protocol Version (v): 0						
Owner/Creator, Session Id (o): Sonus_UAC 13439 1270 IN IP4 192.168.67.120						
Session Name (s): SIP						
Connection Information (c): IN IP4 192.168.67.120						
Time Description, active time (t): 0 0						
Media Description, name and address (m): audio 16988 RTP/AVP 18 0 2 100						
Media Attribute (a): rtpmap:18 G729/8000						
Media Attribute (a): fmtp:18 annexb=no						
Media Attribute (a): rtpmap:0 PCMU/8000						
Media Attribute (a): rtpmap:100 telephone-event/8000						
Media Attribute (a): fmtp:100 0-15						
Media Attribute (a): sendrecv						
Media Attribute (a): ptime:30						

3. The following trace captured on the **private** side of the Avaya SBCE, shows the CS1000E 200 OK response being sent by Session Manager to the Avaya SBCE. As can be observed in the example below:
  - The CS1000E IDT table has an entry for the DNIS number **7325551234** (which converted it to its corresponding CS1000E extension 4096), therefore the CS1000E sends the DNIS number in the P-Asserted-Identity header and the Contact header, (see **Section 2.2.1, Item 5**).
  - Session Manager has added **P-Location**, **AV-Global-Session-ID**, and **P-AV-Message-ID-ID** headers.
  - The CS1000E is sending RFC2833 Telephone event types **100** and **111**.
  - Note that the CS1000E is responding with **ptime:30**.

No.	Time	Source	Destination	Protocol	Length	Info
156	13.629308	192.168.67.47	192.168.67.120	SIP/SDP	322	Status: 200 OK, with session description
Frame 156: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits)						
Ethernet II, Src: Ibm_40:56:90 (e4:1f:13:40:56:90), Dst: Intel_31:1b:ed (90:e2:ba:31:1b:ed)						
Internet Protocol Version 4, Src: 192.168.67.47 (192.168.67.47), Dst: 192.168.67.120 (192.168.67.120)						
Transmission Control Protocol, Src Port: sip (5060), Dst Port: 13486 (13486), Seq: 3517, Ack: 1079, Len: 268						
[2 Reassembled TCP Segments (1728 bytes): #155(1460), #156(268)]						
Session Initiation Protocol						
Status-Line: SIP/2.0 200 OK						
Message Header						
P-Location: SM;origlocname="Main";origsiglocname="Main";origmediaLocname="Main";termlocname="CS1K";termsiglocname="CS1K"						
P-AV-Message-ID: 1_2						
Server: AVAYA-SM-6.3.5.0.635005						
AV-Global-Session-ID: fca550b0-6bfc-11e3-acaf-e41f13326f60						
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE						
Contact: <sip:7325551234;phone-context=UnknownUnknown@cots1.ntlab.com:5060;maddr=172.16.6.110;transport=tcp;user=phone;						
Record-Route: <sip:rw-5aabea25@192.168.67.47;lr;transport=TCP>						
Record-Route: <sip:192.168.67.46:15060;transport=tcp;lr;ibmsid=local.1386195439845_843122_843354>						
Record-Route: <sip:rw-5aabea25@192.168.67.47;lr;transport=TCP>						
Record-Route: <sip:192.168.67.120:5060;transport=tcp;lr;ipcs-line=10425>						
Privacy: none						
P-Asserted-Identity: <sip:7325551234;phone-context=UnknownUnknown@cots1.ntlab.com;user=phone>						
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.65.16						
Supported: 100rel, x-nortel-sipvc, replaces						
To: <sip:7325551234@customera.com>;tag=3a95078-6e0610ac-13c4-55013-53325-42275032-53325						
From: <sip:8185551111@customera.com>;tag=905771306713283_c1b09.1.1.1379097345250.0_296_1141;isup-oli=00						
Call-ID: 49717a26ace85b720d87c06955e0d647						
CSeq: 2 INVITE						
Via: SIP/2.0/TCP 192.168.67.120:5060;branch=z9hg4bk-s1632-002139069330-1--s1632-						
Content-Type: application/sdp						
Content-Length: 254						
Message Body						
Session Description Protocol						
Session Description Protocol Version (v): 0						
Owner/Creator, Session Id (o): - 2 2 IN IP4 172.16.6.110						
Session Name (s): -						
Connection Information (c): IN IP4 172.16.6.115						
Time Description, active time (t): 0 0						
Media Description, name and address (m): audio 5574 RTP/AVP 18 100 111						
Connection Information (c): IN IP4 172.16.6.115						
Media Attribute (a): ptime:30						
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): sendrecv						

4. The following trace captured on the **public** side of the Avaya SBCE, shows the subsequent 200 OK message sent by the Avaya SBCE to AT&T.
  - The Avaya SBCE has removed the following headers (**Section 8.4.3**):
    - **P-Location**, **AV-Global-Session-ID**, and **P-AV-Message-ID**
  - Removed the **Telephone Event Type 111** (**Section 8.3.9**).
  - The Avaya SBCE has set the TO header back to the customers Billing number **8885551111** (**Section 8.3.9**).

No.	Time	Source	Destination	Protocol	Info
17	29.413	192.168.64.130	10.10.10.10	SIP/SDP	Status: 200 OK, with session description
Frame 17: 1224 bytes on wire (9792 bits), 1224 bytes captured (9792 bits)					
Ethernet II, Src: Intel_31:1b:e9 (90:e2:ba:31:1b:e9), Dst: Cisco_29:e4:a0 (a4:93:4c:29:e4:a0)					
Internet Protocol Version 4, Src: 192.168.64.130 (192.168.64.130), Dst: 10.10.10.10 (10.10.10.10)					
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)					
Session Initiation Protocol					
Status-Line: SIP/2.0 200 OK					
Message Header					
From: <sip:8185551111@10.10.10.10>;tag=905771306713283_c1b09.1.1.1379097345250.0_296_1141;isup-oli=00 To: <sip:8885551111@192.168.64.130>;tag=3a95078-6e0610ac-13c4-55013-53325-42275032-53325					
CSeq: 2 INVITE					
Call-ID: 47033942349966296@c1b09_1_1					
Contact: <sip:7325551234;phone-context=UnknownUnknown@192.168.64.130:5060;transport=udp;user=phone;gsid=fca					
Record-Route: <sip:192.168.64.130:5060;ipcs-line=10425;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-7.65.16					
Via: SIP/2.0/UDP 10.10.10.10 :5060;branch=z9hg4bk9rekqf00400h1rgeu070.1					
Server: AVAYA-SM-6.3.5.0.635005					
Privacy: none					
P-Asserted-Identity: <sip:7325551234;phone-context=UnknownUnknown@192.168.64.130;user=phone>					
Content-Type: application/sdp					
Content-Length: 222					
Message Body					
Session Description Protocol					
Session Description Protocol Version (v): 0					
Owner/Creator, Session Id (o): - 2 2 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 16900 RTP/AVP 18 100					
Connection Information (c): IN IP4 192.168.64.130					
Media Attribute (a): ptim:30					
Media Attribute (a): fmtp:18 annexb=no					
Media Attribute (a): rtpmap:100 telephone-event/8000					
Media Attribute (a): fmtp:100 0-15					
Media Attribute (a): sendrecv					

Changing the display filter to **rtp**, the media streams for this call are displayed. Note that the UDP ports used are within the range defined in **Section 8.5.2**. Also note that G.729 was the codec used.

No.	Time	Source	Destination	Protocol	Info
190	8.769	192.168.64.130	10.10.10.10	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9508, Time=
191	8.792	10.10.10.10	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=93, Time=
192	8.796	192.168.64.130	10.10.10.10	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9509, Time=
193	8.822	10.10.10.10	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=94, Time=
194	8.827	192.168.64.130	10.10.10.10	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9510, Time=
195	8.852	10.10.10.10	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=95, Time=
196	8.859	192.168.64.130	10.10.10.10	RTP	PT=ITU-T G.729, SSRC=0x5B3A3A28, Seq=9511, Time=
197	8.882	10.10.10.10	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x4B3C23F7, Seq=96, Time=

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: 10.10.10.1074 (10.10.10.1074), 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					

## 9.5. Avaya Session Border Controller for Enterprise Verification

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

Verify that SIP trunk connection from Avaya SBCE (192.168.64.130) to AT&T IP Toll Free border element (10.10.10.10<sup>6</sup>) is up and communicating with SIP OPTIONS and response messages. In the example below, AT&T has sent an OPTIONS and Session Manager (via the Avaya SBCE) has responded with 200 OK.

No.	Time	Source	Destination	Protocol	Info
9	6.776	10.10.10.10	192.168.64.130	SIP	Request: OPTIONS sip:192.168.64.130:5060
10	6.781	192.168.64.130	10.10.10.10	SIP	Status: 200 OK

### 9.5.2. Internal Tracing

**Step 1** – Using the left hand column menu described in **Section 8**, navigate to **Device Specific Settings → Troubleshooting → Trace**.

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

- Select the desired **Interface** from the drop-down menu. If “**Any**” is selected, then the Avaya SBCE will trace traffic from both the A1 and B1 interfaces.
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**)
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Click **Start Capture** to begin the trace.

<sup>6</sup> See the note in **Section 3.1**.

Domain Policies

- TLS Management
- Device Specific Settings
  - Network Management
  - Media Interface
  - Signaling Interface
  - Signaling Forking
  - End Point Flows
  - Session Flows
  - Relay Services
  - SNMP
  - Syslog Management
  - Advanced Options
  - Troubleshooting
    - Debugging
    - Trace**
    - DoS Learning

Trace: SBCE

Devices

SBCE

Call Trace Packet Capture Captures

Packet Capture Configuration

Status: Ready

Interface: Any

Local Address: All :

Remote Address: \*

Protocol: All

Maximum Number of Packets to Capture: 5000

Capture Filename: TEST.pcap

Start Capture Clear

The capture process will initialize, (with the message “Please wait while your settings are saved and the capture is started” displayed), and then the **Status** field will change to “**In Progress**”.

Trace: SBCE

Devices

SBCE

Call Trace Packet Capture Captures

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

Packet Capture Configuration

Status: In Progress

Interface: Any

Local Address: All :

Remote Address: \*

Protocol: All

Maximum Number of Packets to Capture: 5000

Capture Filename: TEST.pcap

Stop Capture

**Step 3** – Run the test.

**Step 4** – Click on the **Stop Capture** button.

**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.

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

Trace: SBCE

Devices

SBCE

Call Trace Packet Capture **Captures**

Last Modified Descending Sort Reset Refresh

File Name	File Size (bytes)	Last Modified	
TEST_20130925093634.pcap	147,456	September 25, 2013 9:36:53 AM EDT	Delete

## 10. Conclusion

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

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

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

## 11. References

### 11.1. Avaya

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

#### Avaya Communication Server 1000E

- [1] *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013.
- [2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013.
- [3] *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.
- [4] *SIP Line Fundamentals Avaya Communication Server 1000*, Release 7.6, NN43001-508, Issue 04.01
- [5] *Avaya CallPilot® Communication Server 1000 and Avaya CallPilot Server Configuration 5.1*, NN44200-312, 02.01, October 2012

#### Avaya Aura® Session Manager/System Manager

- [6] *Administering Avaya Aura® Session Manager*, Release 6.3, December, 2012
- [7] *Implementing Avaya Aura® Session Manager*, Release 6.3, March, 2013
- [8] *Implementing Avaya Aura® System Manager*, Release 6.3, Issue 1, December, 2012

#### Avaya Session Border Controller for Enterprise

- [9] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2013
- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013

#### Avaya Aura® Contact Center

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

[15] *Avaya Aura® Contact Center Commissioning*, Release 6.2, NN44400-312, 03.02, 24 August 2011

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

**AT&T IP Toll Free Service:**

[17] AT&T IP Toll Free Service description -

<http://www.business.att.com/enterprise/Service/voice-services/contact-center-solutions/ip-toll-free/>

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

The AT&T IP Toll Free service may provide multiple network border elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundancy configuration.

Given two AT&T border elements **10.10.10.10<sup>7</sup>** and **10.10.10.11**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to 10.10.10.11 (the primary trunk connection to 10.10.10.10 is defined in **Sections 8.3.4** and **8.3.6**).

### 12.1.1. Configure the Secondary Border Element Server Configuration

Repeat the steps in **Section 8.3.6** to create a Server Configuration for the connection to the AT&T secondary Border Element, using the following entries:

**Step 1** - In the **Profile Name** window enter a Profile Name (e.g., “**ATT\_Secondary\_SC**”) and select **Next**.

**Step 2** – In the **Add Server Configuration Profile - General** window for **Server Type**: select **Trunk Server**.

- Enter **IP Address: 10.10.10.11**.
- For **Supported Transports**: check **UDP**
- For **UDP Port**: enter **5060**
- Select **Next**

**Step 3** - Accept default values for the **Add Server Configuration Profile - Authentication** and **Heartbeat** windows (not shown).

**Step 4** – The **Add Server Configuration Profile - Advanced** window will open.

- Select **ATT\_SI** for **Interworking Profile** (created in **Section 8.3.2**).
- For the **Signaling Manipulation Script** select the **CS1K\_TO\_Header\_and\_Maxptime** script that was defined in **Section 8.3.9**.

**Step 5** - Select **Finish**.

The following screen shots show the completed **General** and **Advanced** tabs.

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
 Domain DoS  
 Fingerprint  
 Server Interworking  
 Phone Interworking  
 Media Forking  
 Routing  
**Server Configuration**

**Server Configuration: ATT\_Secondary\_SC**

Add Rename Clone Delete

Server Profiles  
ATT\_Primary\_SC  
SM\_Trunk\_SC  
**ATT\_Secondary\_SC**

General Authentication Heartbeat Advanced

Server Type	Trunk Server
IP Addresses / FQDNs	10.10.10.11
Supported Transports	UDP
UDP Port	5060

Edit

<sup>7</sup> See the note in **Section 3.1**.

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration

### Server Configuration: ATT\_Secondary\_SC

Add
Rename
Clone
Delete

Server Profiles
ATT\_Primary\_SC
SM\_Trunk\_SC
ATT\_Secondary\_SC

General
Authentication
Heartbeat
Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	CS1K_TO_Header_and_Maxptime
UDP Connection Type	SUBID

Edit

### 12.1.2. Add Secondary Border Element IP Address to Routing

Repeat the steps in **Section 8.3.4** to add a Routing Profile for the AT&T secondary Border Element.

**Step 1** – Select the profile created in **Section 8.3.4** (e.g., **To\_ATT\_RP**).

**Step 2** - Click **Next**, then enter the following:

- Set **Next Hop Server 2:** to **10.10.10.11**.

**Step 3** - 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
IP, IP:Port, Domain, or Domain:Port
10.10.10.10

Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port
10.10.10.11

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

Finish

### 12.1.3. Configure Secondary AT&T Border Element End Point Flow

**Step 1** – Repeat the steps in **Section 8.5.5**, with the following changes, to add an Endpoint Flow for the AT&T secondary Border Element:

- For **Name**: enter “**ATT\_Secondary**”

**Step 4** - Click **Finish** (not shown)

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ SIP Cluster

▸ Domain Policies

▸ TLS Management

▸ Device Specific Settings

Network Management

Media Interface

Signaling Interface

Signaling Forking

**End Point Flows**

Session Flows

Relay Services

SNMP

Syslog Management

Advanced Options

▸ Troubleshooting

End Point Flows: SBCE

Devices

SBCE

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: ATT\_Primary\_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ATT_Primary	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

Server Configuration: ATT\_Secondary\_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ATT_Secondary	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

Server Configuration: SM\_Trunk\_SC

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default-low_PG	To_ATT_VIT	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

When completed the Avaya SBCE will issue OPTIONS messages to the primary (**10.10.10.10** and secondary (**10.10.10.11**) border elements.

---

©2014 Avaya Inc. All Rights Reserved.

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

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