



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3, and the Avaya Session Border Controller for Enterprise 6.3, with the AT&T IP Toll Free SIP Trunk service using either AVPN or MIS/PNT transport connections.

Avaya Aura® 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 1000 7.6 is a telephony server, and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Session Border Controller for Enterprise 6.3 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service, and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

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
2.3	Support	8
3	Reference Configuration	8
3.1	Illustrative Configuration Information	10
3.2	Call Flows	11
4	Equipment and Software Validated	12
5	CS1000 Provisioning	13
5.1	Logging In and Selecting the System Element	13
5.2	Administer Telephony Node	14
5.2.1	Node Information and IP Addresses	14
5.2.2	Enable Terminal Proxy Server.....	16
5.2.3	Synchronize Configuration	17
5.3	Voice Codecs.....	18
5.3.1	IP Telephony Node Codec Configuration.....	18
5.3.2	Media Gateway Codec Configuration	20
5.4	Zones and Bandwidth Management.....	22
5.4.1	Zone 5 – SIP Trunk.....	23
5.4.2	Zone 3 – IP Telephones	24
5.5	SIP Trunk Gateway	24
5.5.1	Provision SIP Gateway	24
5.5.2	Integrated Services Digital Network (ISDN).....	27
5.5.3	Virtual D-Channel Configuration	27
5.5.4	SIP Routes Configuration	29
5.5.5	SIP Trunk Configuration.....	30
5.6	Routing of Inbound Numbers to CS1000.....	33
5.7	Enabling Plug-Ins for Call Transfer Scenarios	34
5.8	CS1000 Agent Access Provisioning	35
5.8.1	CS1000 IP Agent Phone	36
5.8.2	Analog Fax Line	37
5.9	Changing RFC2833 DTMF Telephone Event Type	38
5.10	Inbound Calls to Call Pilot®	38
5.11	CS1000 Configuration Backup.....	40
6	Configure Avaya Aura® Session Manager	41
6.1	SIP Domain	42
6.2	Locations	42
6.3	Configure Adaptations	43
6.3.1	Adaptation to the CS1000.....	44
6.3.2	Adaptation for calls from the CS1000 to AT&T	45
6.4	SIP Entities	46
6.4.1	SIP Entity for the CS1000.....	46

6.4.2	SIP Entity for the Avaya SBCE	47
6.4.3	SIP Entity for Session Manager	48
6.5	Entity Links	49
6.5.1	Entity Link to CS1000 Entity	49
6.5.2	Entity Link to the Avaya SBCE	49
6.6	Routing Policies	50
6.6.1	Routing Policy to the CS1000	50
6.6.2	Routing Policy to the Avaya SBCE	50
6.7	Dial Patterns	51
7	Configure Avaya Session Border Controller for Enterprise	52
7.1	System Management/Status	53
7.2	Global Profiles	54
7.2.1	Server Interworking – Avaya	54
7.2.2	Server Interworking – AT&T	57
7.2.3	Signaling Manipulation	57
7.2.4	Server Configuration – Session Manager	58
7.2.5	Server Configuration – AT&T	59
7.2.6	Routing – To Session Manager	60
7.2.7	Routing – To AT&T	61
7.2.8	Topology Hiding – Avaya Side	61
7.2.9	Topology Hiding – AT&T Side	62
7.3	Domain Policies	63
7.3.1	Application Rules	63
7.3.2	Media Rules	63
7.3.3	Signaling Rules	64
7.3.4	Endpoint Policy Groups – Avaya Connection	67
7.3.5	Endpoint Policy Groups – AT&T Connection	68
7.4	Device Specific Settings	68
7.4.1	Network Management	68
7.4.2	Advanced Options	69
7.4.3	Media Interfaces	70
7.4.4	Signaling Interface	70
7.4.5	Endpoint Flows	71
8	Configure Avaya Aura® Contact Center	73
8.1	Create Avaya Aura® Contact Center Agent	73
8.2	Verify Control DN (CDN) and Agent Connection Status	74
8.2.1	CDN Connection status	74
8.2.2	Agent Connection status	75
9	AT&T IP Toll Free Service	75
10	Verification Steps	76
10.1	General	76
10.2	CS1000 Verifications	76
10.2.1	IP Network Maintenance and Reports Commands	76
10.2.2	System Maintenance Commands	77

10.3	Avaya Aura® Session Manager	78
10.4	Avaya Session Border Controller for Enterprise	79
10.4.1	System Status	79
10.4.2	Protocol Traces.....	80
11	Conclusion	81
12	References.....	82
13	Addendum 1 – Redundancy to Multiple AT&T Border Elements	83
13.1	Configure the Secondary Border Element Server Configuration	83
13.2	Add Secondary Border Element IP Address to Routing	84
13.3	Configure Secondary AT&T Border Element End Point Flow.....	84

1 Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 Release 7.6 (CS1000), Avaya Aura® Session Manager Release 6.3 (Session Manager), and the Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE), with the AT&T IP Toll Free SIP trunk service (IPTF) for PSTN access.

Avaya Aura® 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 1000 7.6 is a telephony server, and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Session Border Controller for Enterprise 6.3 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service, and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

In addition, Avaya Call Pilot® (Call Pilot®) is used in conjunction with the Avaya Communication Server 1000 to provide voice mail access, as well as Avaya Aura® Contact Center 6.4 (ACC) which provide Agents access functionality (queues, skill levels, etc). While both of these platforms are discussed in the following sections, their provisioning is beyond the scope of this document.

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

Note - These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. That solution is *not* supported by the CS1000.

2 General Test Approach and Test Results

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPTF and the Customer Premises Equipment (CPE) containing the CS1000, Session Manager, and the Avaya SBCE (see **Section 3.2** for call flow examples).

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

The test environment consisted of:

- A simulated enterprise including the CS1000 (including Call Pilot[®]), Session Manager, System Manager (for Session Manager provisioning), the Avaya SBCE, ACC, Avaya phones, and fax machine emulation software (Ventafax application).
- A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise was connected via AVPN transport.

2.1 Interoperability Compliance Testing

Note – Documents used to provision the test environment are listed in **Section 12**. In the following sections, references to these documents are indicated by the notation [x], where *x* is the document reference number.

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 IPTF network. Calls were made between the PSTN, via the IPTF network, and the CPE.

The following SIP trunking VoIP features were tested with the IPTF service:

- Inbound voice calls between PSTN, the IPTF service, the Avaya SBCE, Session Manager, and the CS1000/ACC. Avaya 1140E and 1150E UniStim IP telephones, as well as M3904 Digital telephones, were used.
- Inbound fax calls using T38 or G.711.
- Requests for privacy (i.e., caller anonymity) for inbound calls to the CS1000/ACC.
- SIP OPTIONS messages used to monitor the health of the SIP trunks between the CPE and AT&T.
- Incoming calls using the G.729(A) and G.711 ULAW codecs.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful IPTF, Call Pilot[®], and ACC voice menu navigation.
- CS1000 telephony features such as Hold, Transfer, and Conference.
- Proper UDP port ranges for RTP media (16384-32767) were verified.
- Passing of inbound DTMF events and their recognition by ACC automated menus.
- IPTF network features such as Legacy Transfer Connect (network Hold, Transfer, and Conference via outbound DTMF), and Alternate Destination Routing were also tested.

2.2 Test Results

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

1. **Maxptime:30 and Ptime:10** – For inbound calls, the IPTF service sends Invites with the SIP parameter *maxptime:30*. In response, the CS1000 will send *ptime:10* for any UNISim or digital stations. This is known CS1000 behavior. However, the AT&T AVPN transport service specifies the use of *ptime:30* for best bandwidth utilization. An Avaya SBCE script is used to change the IPTF *maxptime:30* parameter, to *ptime:30*, thereby making CS1000 respond with *ptime:30* as required (see **Section 7.2.3**).

2. **Removal of SIP Headers** – Depending on the call flow and the endpoints involved, the CS1000 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:
 - The CS1000 may include MIME type headers in some messages. These are removed by a Session Manager Adaptation (see **Section 6.3.2**).
 - The Avaya SBCE is configured to remove the following SIP headers that may also be added by the CPE (see **Section 7.4.4**):
 - Alert-Info, x-nt-e164-clid, History-Info, Remote-Party-ID, Resource-Priority, AV-Global-Session-ID, P-AV-Message-ID, and P-Location.
 - a. Note that AT&T does not support History-Info.
3. **The Avaya SBCE issues a Remote-Address header even though the option to do so is disabled** - During testing it was found that the Avaya SBCE was including a Remote-Address header to SIP Invite messages leaving the Avaya SBCE (inbound or outbound, depending on call direction), even though the option was disabled.
 - a. No issues were caused by the inclusion of this header; however the Avaya SBCE was provisioned to remove this header for calls to AT&T, to reduce overall packet size (see **Section 7.3.3**).
4. **CS1000 Telephone Events 101 and 111** - The CS1000 uses Telephone Event type 101 by default. This value is changed to the AT&T recommended value of 100 in the CS1000 (see **Section 5.9**). Telephone event type 111 is also sent by the CS1000. This value is removed by the Avaya SBCE (see **Section 7.2.3**).
5. **The IPTF service offers the G.726-32 codec (Dynamic Payload 98). This codec is not supported by the CS1000.**
6. **The CS1000 may not populate the PAI header correctly.** In certain call conditions, the CS1000 Incoming Digit Translation (IDT) table (**Section 5.6**), may populate PAI headers with the associated CS1000 extension and/or the inbound IPTF DNIS digits, instead of the desired IPTF DID digits.
 - a. The workaround is to have Session Manager modify the PAI headers prior to sending the subsequent CS1000 call responses back to the IPTF service (see **Section 6.3.1**).
7. **Fax support** - G.711 and T.38 fax is supported by the IPTF service, 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. Note that the fax test results obtained during the CS1000 7.6/Session Manager 6.3/Avaya SBCE 6.3/AT&T IP Flexible Reach-Enhanced Features testing were used as the benchmark validation for the AT&T IP Toll Free service as well. Successful fax speeds of 14400, with Error Correction Mode, were observed during that testing.

8. **IPTF Landline/Mobility test cases could not be executed.** The AT&T supplied IPTF test plan specifies test cases to verify the transmission of Landline/Mobility data by the IPTF service. Due to network provisioning issues, these test cases could not be executed.
9. **Call Pilot® uses the contents of the SIP To header for admission control.** The IPTF service Invite messages populate the SIP To header with the customers billing number. When inbound calls are placed directly to the Call Pilot® main extension, this billing number must be defined provisioned in Call Pilot® as a Service Directory Number (see **Section 5.10**), otherwise Call Pilot® will reject the call.

2.3 Support

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

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 CS1000 system provides the voice communications services for the enterprise site. The system is comprised of:
 - The MG1000 Gateway containing:
 - Call Server (CPPM).
 - Media Gateway Controller (MGC), which provides Digital Signaling Processor (DSP) resources.
 - Meridian Integration Recorded Announcement (MIRAN) card used for Music on Hold.
 - Avaya Call Pilot® messaging application.
 - IBM 306M Consumer Off the Shelf (COTS) servers, COTS1 and COTS2.
 - Signaling Server and SIP Gateway (COTS1).
 - SIPLINE and UCM (COTS2).
- Avaya desk phones are represented with Avaya 1140E and 1150E UNISTim IP and M3904 Digital telephones.
- Session Manager provides core SIP routing and integration services that enable communication between the CS1000 and the Avaya SBCE/IPTF service. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP to communicate with the CS1000.
- System Manager 6.3 provides the provisioning/management interface for Session Manager.
- Avaya SBCE provides address translation and SIP header manipulation between the IPTF 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 IPTF service.

- An Avaya Aura® Contact Center system provides the Agent capabilities in the reference configuration. The provisioning of Avaya Aura® Contact Center is beyond the scope of this document (see [12-14] for more information).

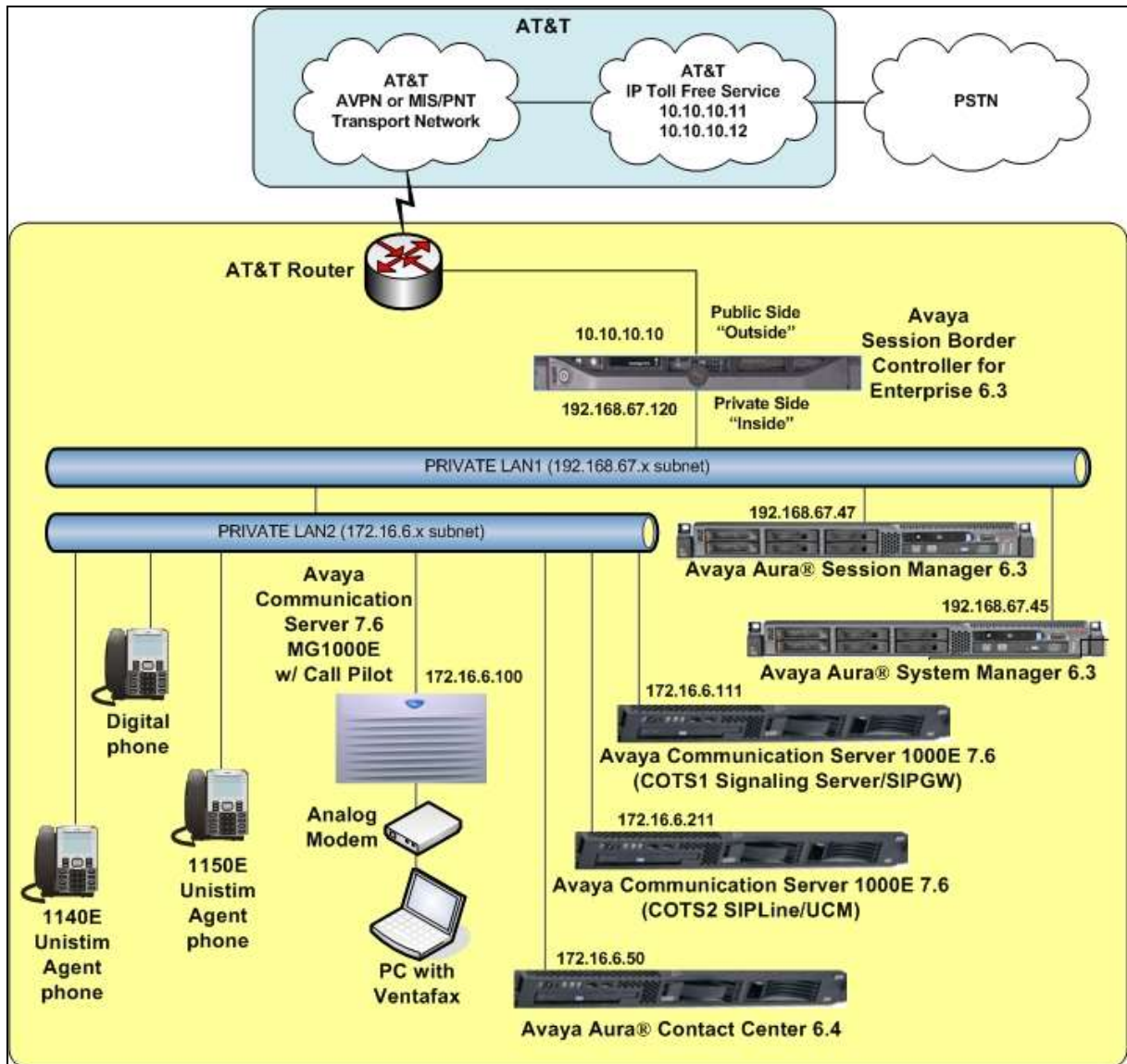


Figure 1: Avaya Interoperability Reference Configuration

3.1 Illustrative Configuration Information

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

Note – The IPTF 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 IPTF provisioning process.

Component	Illustrative Value in these Application Notes
CS1000	
COTS1 SIP Signaling Server (TLAN)	172.16.6.110
COTS2 SIP Line (TLAN)	172.16.6.210
Call Pilot [®]	172.16.6.130
MGC Media (DSP) (TLAN)	172.16.6.115
Avaya Contact Center	
Contact Center Application	172.16.6.50
Avaya SBCE	
“Outside” (Public) Interface (connected to AT&T Access Router/IP Toll Free Service)	10.10.10.10 (see note below)
“Inside” (Private) Interface (connected to Session Manager)	192.168.67.120
AT&T IP Toll Free Service	
Border Element	10.10.10.11 (see note below)

Table 1: Illustrative Network Values Used in these Application Notes

NOTE – The Avaya SBCE Outside interface communicates with AT&T Border Elements (BEs) located in the AT&T IP Toll Free network. For security reasons, the IP addresses of the AT&T BE are not included in this document. However as placeholders in the following configuration sections, the IP address of **10.10.10.10** (Avaya SBCE public interface), and **10.10.10.11** (AT&T BE IP address), are specified.

3.2 Call Flows

To understand how inbound IPTF service calls are processed by Session Manager and CS1000, two general call flows are described in this section.

The first call scenario illustrated in **Figure 2** is an inbound IPTF service call that arrives on Session Manager and is subsequently routed to CS1000.

1. A PSTN telephone originates a call to an IPTF service number.
2. The PSTN routes the call to the IPTF service network.
3. The IPTF 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 CS1000.
6. Depending on the called number, CS1000 routes the call to an Agent (via Avaya Contact Center) or CS1000 telephone.

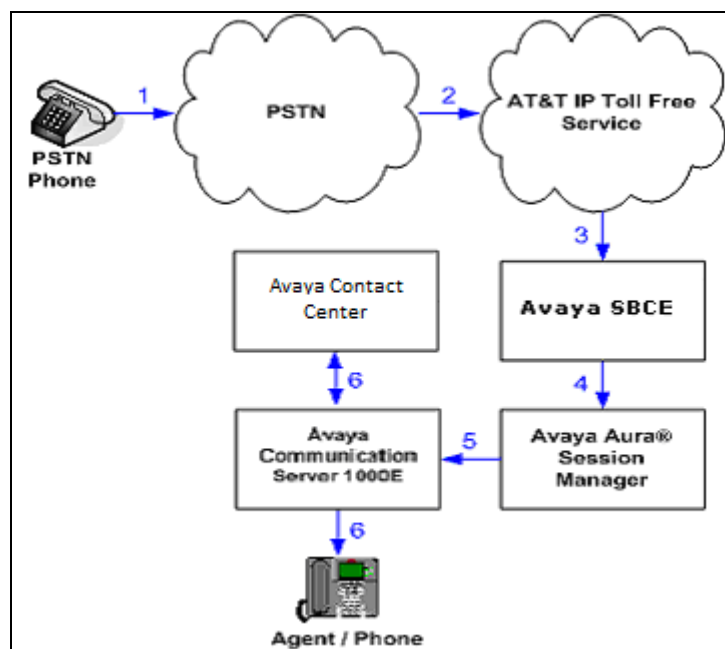


Figure 2: Inbound IPTF Service Call to Agent / Telephone

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">• System Platform• Avaya Aura® System Manager	<ul style="list-style-type: none">• 6.3.6.1005.0• 6.3.13.10.3336 (SP13)
IBM 8800 server <ul style="list-style-type: none">○ Avaya Aura® Session Manager	<ul style="list-style-type: none">• 6.3.13.0.631304 (SP13)
CS1000 Platform	<ul style="list-style-type: none">• Version 4021, Release 765P+• Service Pack 5 (CPM_7.65.16.00)• CP 5.00.41
HP DL360 G7 <ul style="list-style-type: none">○ Avaya Aura® Contact Center	<ul style="list-style-type: none">• 6.4.212.0
Dell R210 <ul style="list-style-type: none">• Avaya Session Border Controller for Enterprise	<ul style="list-style-type: none">• 6.3.2-08-5478 (SP2)
Avaya 1140E and 1150E Series IP Telephones (UNISTim)	<ul style="list-style-type: none">• 0625C8Q
Avaya M3904 Series Digital Deskphones	-
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none">• 7.0.202.494

Table 2: Equipment and Software Versions

5 CS1000 Provisioning

Note – Only CS1000 system provisioning providing SIP trunk functionality is described in these application notes. For additional CS1000 system provisioning documentation, see **Section 12**.

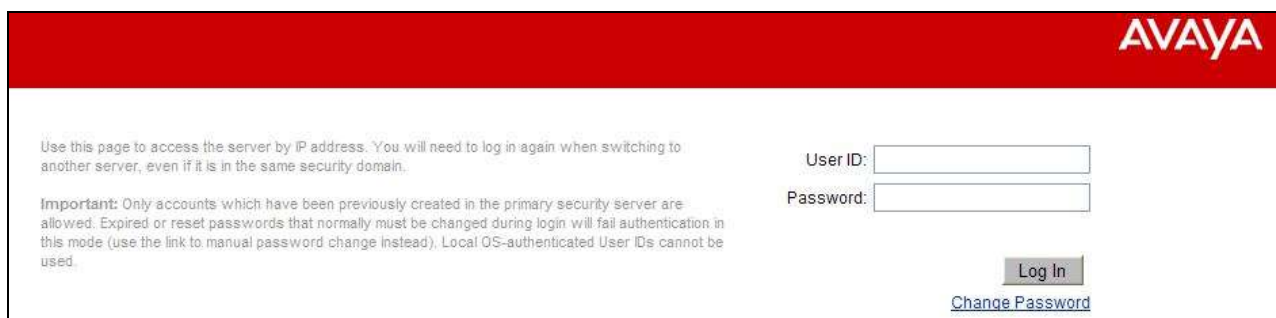
This section describes the CS1000 configuration, focusing on the routing of calls to Session Manager over a SIP trunk. In the sample configuration, CS1000 Release 7.6 was deployed with Call Server applications running on a CPPM server platform with MGC, and utilizing servers running separate Signaling 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 CS1000 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 CS1000. 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 CS1000 is configured to support analog, digital, UNISTim and SIP endpoints. For references on how to administer the CS1000, see **Section 12**.

5.1 Logging In and Selecting the System Element

Step 1 - Unless otherwise noted, all CS1000 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.

The screenshot shows the Avaya login interface. At the top right is the AVAYA logo. Below it, a message states: "Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain." To the right of this message are two input fields labeled "User ID:" and "Password:". Below the "Important:" text, it says: "Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used." At the bottom right, there is a "Log In" button and a "Change Password" link.

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 CS1000 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**.

Avaya Unified Communications Management

Host Name: cots2.ntlab.com Software Version: 02.30.0066.00(6406) User Name admin

Elements

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

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	EM on cots1	CS1000	7.6	192.12.0.100	New element.
<input type="checkbox"/>	192.12.0.100	Call Server	7.6	192.12.0.100	New element.
<input type="checkbox"/>	CallPilot	Hyperlink	7.6	http://172.16.6.130/cpmgr	
<input type="checkbox"/>	cots1.ntlab.com (member)	Linux Base	7.6	172.16.6.111	Base OS element.
<input type="checkbox"/>	cots2.ntlab.com (primary)	Linux Base	7.6	172.16.6.211	Base OS element.
<input type="checkbox"/>	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.

CS1000 Element Manager

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

IP Telephony Nodes

Click the Node ID to view or edit its properties.

<input type="checkbox"/>	Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/>	1001	1	LTPS, Gateway (SIPGw)	-	172.16.6.110	-	Synchronized
<input type="checkbox"/>	1004	1	SIP Line	-	172.16.6.210	-	Synchronized

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

The **Node Details** screen is displayed with additional details as shown below.

Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPv4 address**. In the sample screen below, the **Node IPv4 address** is 172.16.6.110. This IP address will be needed when configuring a Session Manager SIP Entity for CS1000 in **Section 6.4.1**.

AVAYA CS1000 Element Manager

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

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

Node ID: 1001 * (8-9995)

Call server IP address: 192.12.0.100 *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 192.12.0.1 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 172.16.6.110 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

* Required Value.

Save Cancel

Associated Signaling Servers & Cards

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

AVAYA CS1000 Element Manager

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

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

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

Associated Signaling Servers & Cards

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

AVAYA CS1000 Element Manager

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]

Associated Signaling Servers & Cards

Select to add [Add] [Remove] [Make Leader] [Print] [Refresh]

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cots1	Signaling_Server	SIP Line, LTPS, Gateway (SIPH323), PD, Presence Publisher, IP Media Services	192.12.0.10	172.16.6.111	Leader

Show: ☐ IPv6 address

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

5.2.2 Enable Terminal Proxy Server

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server (TPS)** application link as shown above.

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

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

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » UNISTim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 1001 - UNISTim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware | DTLS | Network Connect Server

UNISTim Line Terminal Proxy Server: ☒ **Enable proxy service on this node**

Firmware

IP address: 0.0.0.0

Full file path: download/firmwa

Server Account/User ID:

Password:

DTLS

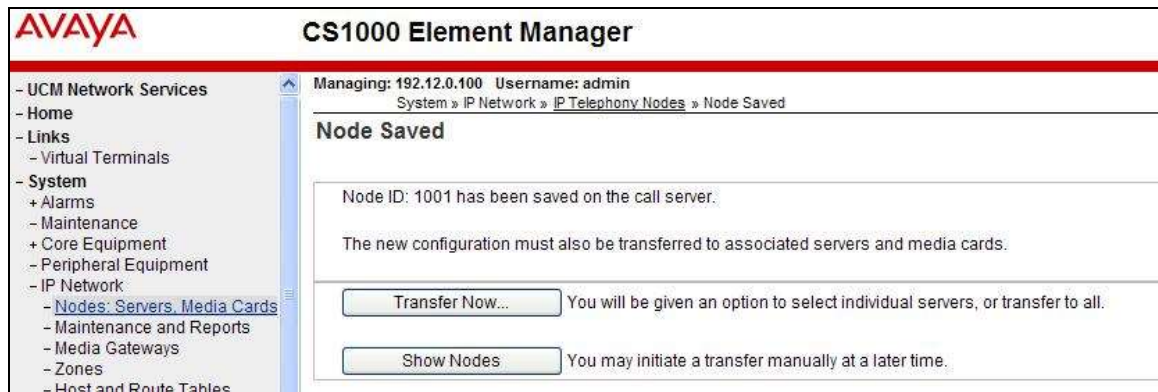
DTLS Scaling: Off

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.

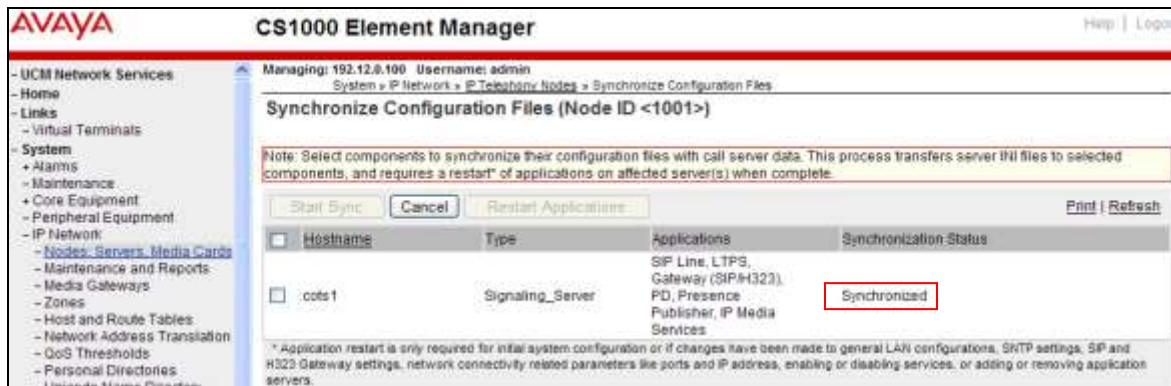


Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

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.



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.



5.3 Voice Codecs

The following section describes how to set codec preferences as well as setting Packet Interval (PTIME) values. Note that the CS1000 always specifies G.711 regardless of the additional selected codes. Codecs are defined in the **IP Telephony Node** for IP (e.g., UNISTIM) 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**.

AVAYA **CS1000 Element Manager**

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

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

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)
Gateway IP address: *
Subnet mask: *

Telephony LAN (TLAN)
Node IPv4 address: *
Subnet mask: *
Node IPv6 address:

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

The Voice Gateway (VGW) and Codecs form will open.

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

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: (milliseconds per frame)

Voice playout (jitter buffer) delay: (milliseconds)

Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☐ 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**.

Codec G729: ☒ Enabled

Voice payload size: (milliseconds per frame)

Voice playout (jitter buffer) delay: (milliseconds)

Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☐ 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 configuration window showing the following settings:

- 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 8** through **12** 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**).

CS1000 Element Manager - Media Gateways

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**.

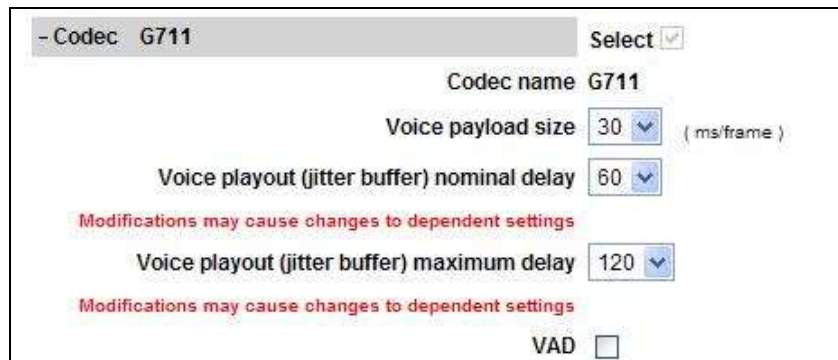
MGC Configuration screen showing the following settings:

- Hostname: DB1
- 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

Profiles list:

- + VGW and IP phone codec profile
- + QoS
- + Media Based CLID

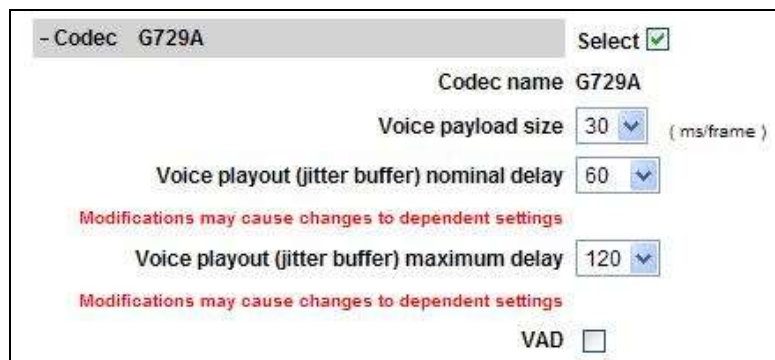
Step 3 - The **VGW and IP phone codec profile** section will expand. Scroll down, click on and expand the **Codec G711** field. Note that the **Select** box is checked by default. Set the **Voice payload size (PTIME)** to **30**.



The screenshot shows the configuration for the G711 codec. At the top, there is a dropdown menu labeled '- Codec' with 'G711' selected, and a 'Select' button with a checkmark. Below this, the 'Codec name' is 'G711'. The 'Voice payload size' is set to '30' with a unit of '(ms/frame)'. The 'Voice playout (jitter buffer) nominal delay' is set to '60'. A red warning message 'Modifications may cause changes to dependent settings' appears below the nominal delay. The 'Voice playout (jitter buffer) maximum delay' is set to '120'. Another red warning message 'Modifications may cause changes to dependent settings' appears below the maximum delay. At the bottom, there is a 'VAD' checkbox which is currently unchecked.

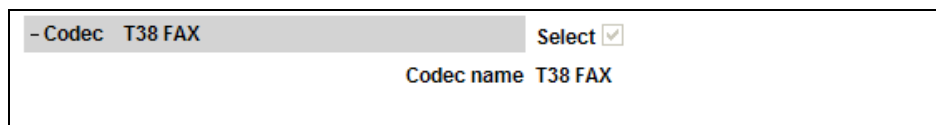
Step 4 – Scroll down , click on and expand the **Codec G729A** field. Check the selection box and set the **Voice payload size (PTIME)** to **30**.

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**.



The screenshot shows the configuration for the G729A codec. At the top, there is a dropdown menu labeled '- Codec' with 'G729A' selected, and a 'Select' button with a checkmark. Below this, the 'Codec name' is 'G729A'. The 'Voice payload size' is set to '30' with a unit of '(ms/frame)'. The 'Voice playout (jitter buffer) nominal delay' is set to '60'. A red warning message 'Modifications may cause changes to dependent settings' appears below the nominal delay. The 'Voice playout (jitter buffer) maximum delay' is set to '120'. Another red warning message 'Modifications may cause changes to dependent settings' appears below the maximum delay. At the bottom, there is a 'VAD' checkbox which is currently unchecked.

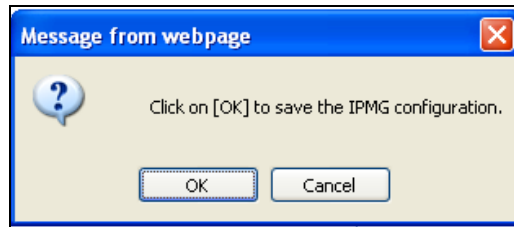
Step 5 – Scroll down and click on **Codec T.38 FAX**. Note that T.38 is enabled by default.



The screenshot shows the configuration for the T.38 FAX codec. At the top, there is a dropdown menu labeled '- Codec' with 'T38 FAX' selected, and a 'Select' button with a checkmark. Below this, the 'Codec name' is '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.

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

Media Gateways

	IPMG	IP Address	Zone	Type
	000 01	192.12.0.11	1	MGC

5.4 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.

AVAYA **CS1000 Element Manager**

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

Zones

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

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

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

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

Step 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 IPTF 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, **customera.com** was used in the reference configuration.
- **Local SIP port:** Enter **5060**
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter <Node id>. In the sample configuration, Node **1001** was used matching the node shown in **Section 5.2.1**.
- Check the **VTrk gateway application** checkbox.

The values defined for the sample configuration are shown below.

Node ID: 1001 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGW)

SIP domain name: customera.com

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: SS_1001

Gateway password: *

Application node ID: 1001 * (0-9999)

Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP: Add

Monitor addresses: Remove

* Required Value.

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

Save Cancel

Step 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 (e.g., **192.168.67.47**).
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**

Note - The Secondary TLAN IP address was not used.

AVAYA CS1000 Element Manager

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: 5060 (1 - 65535)
Transport protocol: TCP

Shared Bandwidth Management:
☐ Enable Shared Bandwidth Management

Proxy Or Redirect Server:
Proxy Server Route 1:
Primary TLAM IP address: 192.168.67.47
The IP address can have either IPv4 or IPv6 format based on the value of "TLAM address type"
Port: 5060 (1 - 65535)
Transport protocol: TCP
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** section, leave the fields blank. Use the defaults for all other values.

AVAYA CS1000 Element Manager

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: CUID display format:
Subscriber (SN): 0 <CC>-<Area code>-<SN>
National (NN): 0 <CC>-<NN>
International: 0 <International number>

SIP URI Map:
Public E.164 domain names:
National:
Subscriber:
Special number:
Unknown:
Private domain names:
UDP:
CDP:
Special number:
Vacant number:
Unknown:

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. Save Cancel

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, 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 interface also shows a 'Help' link in the top right corner.

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 SIPLine. 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 with the 'D-Channels' configuration page. The left navigation tree shows 'Routes and Trunks' expanded, with 'D-Channels' selected. The main area displays a list of D-Channels under the 'Maintenance' section, including 'D-Channel Diagnostics (LD 96)', 'Network and Peripheral Equipment (LD 32, Virtual D-Channels)', 'MSDL Diagnostics (LD 96)', 'TMDL Diagnostics (LD 96)', and 'D-Channel Expansion Diagnostics (LD 48)'. Below this is the 'Configuration' section, which includes a 'Choose a D-Channel Number' dropdown (set to 0) and a 'Type' dropdown (set to DCH). There are also buttons for 'to Add', 'Edit', and 'Delete'. A table lists the configured D-Channels: Channel 15 (Type: DCH, Card Type: DCIP, Description: VDCH) and Channel 20 (Type: DCH, Card Type: DCIP, Description: SIPLINE). Each row has an 'Edit' button.

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"/> <input type="button" value="more PRI"/>
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** 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:	<input type="button" value="Edit"/>

Step 4 – Scrolling down, in the **Advanced Options** 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** (not shown) 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.

Customer: 0	Total routes: 9	Total trunks: 80	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: SIP LINE	Edit Add trunk
+ Route: 26	Type: CID	Description: MRAN	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): 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): ☐

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

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE): Route uses ISDN Signaling Link (ISLD) ▼

- D channel number (DCH): 15 (0 - 254)

- Interface type for route (IFC): Meridian M1 (SL1) ▼

- Private network identifier (PNI): 00000 (0 - 32700)

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- Trunk route optimization (TRO): ☐

- Recognition of DT12 ABCD FALT signal for ISL (FALT): ☐

- Channel type (CHTY): B-channel (BCH) ▼

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

- Insert ESN access code (INAC): ☐

- Integrated service access route (ISAR): ☐

- Display of access prefix on CLID (DAPC): ☐

- Mobile extension route (MBXR): ☐

- Mobile extension outgoing type (MBXOT): National number (NPA) ▼

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

Calling number dialing plan (CNDP): Unknown (UKWN) ▼

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

5.5.5 SIP Trunk Configuration

Step 1 - Expand **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.

Route	Type	Description	Edit	Add trunk
Route: 15	TIE	Description: H323	Edit	Add trunk
Route: 16	TIE	Description: SIP	Edit	Add trunk
Trunk: 1 - 10				
Route: 17	TIE	Description: SIP VTRK TTY	Edit	Add trunk
Route: 18	TIE	Description: SIP LINE	Edit	Add trunk
Route: 26	DID	Description: MIRAN	Edit	Add trunk
Route: 27	MUS	Description: MUSIC	Edit	Add trunk
Route: 28	RAN	Description: RAN1	Edit	Add trunk
Route: 29	RAN	Description: RAN2	Edit	Add trunk
Route: 30	RAN	Description: RAN3	Edit	Add trunk

Step 2 – Click on **Trunk:1-10** to display each trunk channel. Then click on the **Edit** button for **Trunk: 1**, to display the trunk configuration.

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

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 CS1000 display phones if an incoming call on the trunk is anonymous or marked for privacy. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging.

AVAYA **CS1000 Element Manager**

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

Customer 0, Route 16 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE): 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).

AVAYA **CS1000 Element Manager** Help | Logout

Integrated services digital network option (ISDN): ☒
Mode of operation (MODE): Route uses ISDN Signaling Link (ISL)
- D channel number (DCH): 15 (0 - 254)
- Interface type for route (IFC): Meridian M1 (SLT)
- Private network identifier (PNI): 00000 (0 - 32700)
- Network calling name allowed (NCHA): ☒
- Network call redirection (NCRD): ☒
- Trunk route optimization (TRO): ☐
- Recognition of DT2 ABCD FALT signal for ISL (FALT): ☐
- Channel type (CHTY): B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP): Unknown Call type (UKWN)
- Insert ESN access code (INAC): ☐
- Integrated service access route (ISAR): ☐
- Display of access prefix on CUD (IDAPC): ☐
- Mobile extension route (MBXR): ☐
- Mobile extension outgoing type (MEOT): National number (NPA)
- Mobile extension timer (MBXT): 0 (0 - 8000 milliseconds)
Calling number dialing plan (CHDP): 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**. Click on **Submit** (not shown).

- Basic Route Options

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

Billing number required (BILN): ☐

Call detail recording (CDR): ☐

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

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

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

Display external dialed digits (DEXT): ☐

MFC feature options (MFC_FEAT): ☐

+ Network Options

+ General Options

+ Advanced Configurations

5.6 Routing of Inbound Numbers to CS1000

Calls from PSTN will dial IPTF DID numbers to reach stations on CS1000. The IPTF service will then deliver associated DNIS numbers, in SIP Invite messages, to the CPE. These DNIS numbers are converted to the associated extensions by the CS1000 Incoming Digit Translation (IDT) table.

Note – The DNIS digits are those included in the R-URI of the inbound Invite. These might not be the same as the IPTF dialed DID number.

Note – In the reference configuration, although AT&T assigned 10 digit DID numbers (e.g., 732555xxxx), the IPTF service delivered 10 digit DNIS numbers with the format 00000xxxxx.

Note – Due to the issue described in **Section 2.2, Item 6**, Session Manager must modify the DNIS digits that the CS1000 places in the PAI headers. See **Section 6.3.1**.

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**.

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

Incoming Digit Translation

Customer: 00 [Edit IDC]

+ Geographic Redundancy

+ Software

Customers

Routes and Trunks

- Routes and Trunks

- D-Channels

- Digital Trunk Interface

Dialing and Numbering Plans

- Electronic Switched Network

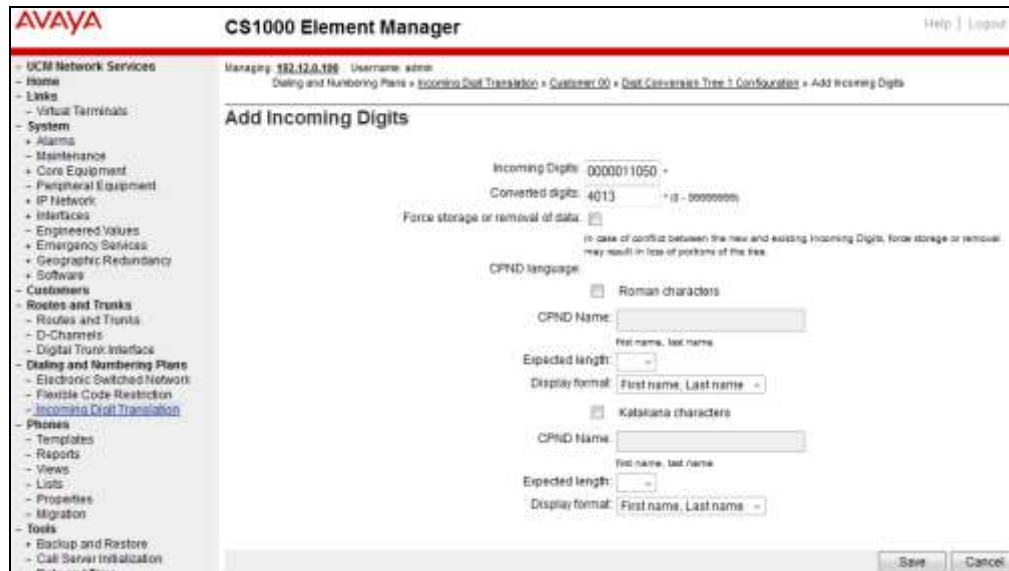
- Flexible Code Restriction

- Incoming Digit Translation

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 (**Section 5.5.5**).



Step 4 – The IDC Tree form will open. Click on the **Add** button. In the **Incoming Digits** field, enter an IPTF DNIS number (e.g., **0000011050**). In the **Converted Digits** field, enter the associated CS1000 extension (e.g., **4013**). Allow the other fields to default. Click on **Save**.



Step 5 – Repeat **Step 4** for all IPTF DNIS numbers and their associated destination extensions. For example, define an IPTF DNIS number for the Call Pilot main access number 2090, (see **Section 2.2, Item 9** and **Section 5.10**).

5.7 Enabling Plug-Ins for Call Transfer Scenarios

Plug-Ins allow specific CS1000 software feature behaviors to be changed. In the testing associated with these Application Notes, Plug-In 501 is required for successful completion of Unattended Transfer calls.

Step 1 - To view or enable a Plug-In, from the left navigation menu, expand **System** → **Software**, and select **Plug-Ins** (not shown). In the right side screen, a list of available Plug-Ins will be

displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-In **501** is displayed as shown in the screen below.

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

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

The screenshot shows the AVAYA CS1000 Element Manager interface. A message at the top states: "An internal error has occurred! Severity: Major". Below this is a table of Plug-Ins. The table has columns for a checkbox, Number, Description, MPLR Number, and Status. Plug-In 501 is highlighted with a red box, showing it is enabled.

<input type="checkbox"/>	Number	Description	MPLR Number	Status
<input type="checkbox"/>	223	PLRCLM REJECTS USRG CLBS REQUEST WITH NO CALLING NUMBER	MPLR12290	Disabled
<input type="checkbox"/>	224	PL No busy treatment on external transfer through application if OUT_T305 = 0	MPLR24676	Disabled
<input type="checkbox"/>	225	PL PKG 179, Taurus, electronic lock, Mail and CallPilot softkeys	MPLR22389	Disabled
<input type="checkbox"/>	226	PL CLID should display more than 10 digits	MPLR15783	Disabled
<input type="checkbox"/>	228	PL TTY 0 on CPU card (B184) causes cursor to go up on VDU	MPLR07613	Disabled
<input type="checkbox"/>	230	PL Unplugged telset disables after midnight routines	MPLR11700	Disabled
<input type="checkbox"/>	231	PL BRI 64K data not possible over DT12. With mix of spans (both DT1 and DT12) THIS is not supported.	MPLR10878	Disabled
<input type="checkbox"/>	232	PL QSIG CF: No diverting and originally called number in DL12	MPLR24273	Disabled
<input type="checkbox"/>	233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506	Disabled
<input type="checkbox"/>	235	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
<input type="checkbox"/>	500	NO DESCRIPTION	MPLR21979	Disabled
<input checked="" type="checkbox"/>	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Enabled

5.8 CS1000 Agent Access Provisioning

This section is not intended to be prescriptive, but simply illustrates a sampling of defining Agent access on the CS1000 in the sample configuration. Inbound IPTF numbers are mapped to the Agent extensions (or skill queues) as shown in **Section 5.6**.

The following Directory Numbers (DNs) are defined. In the reference configuration an Agent 4014 is 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 CS1000 and the Avaya Aura[®] Contact Center (see **Section 8**).
- **4014** – This is the Agents Single Call Ringing (SCR) number. This is the Agent's "local" extension independent of the Agent queue, and will also appear on the phone display. The Agent logs in with this number.

5.8.1 CS1000 IP Agent Phone

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

5.8.1.1 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.

AVAYA CS1000 Element Manager

Phone Details

System: EM on cota1
Phone Type: 1150
Sync Status: TREN

General Properties | Features | Keys | User Fields | Custom View: All

General Properties

Customer Number: 0
Terminal Number: 096 0 01 17
Designation: AGENT2 (1-6 characters)
Zone: 3
Key Expansion Modules: 0

5.8.1.2 Features

Scroll further down the **Phone Details** form and locate the **Features** section of the form. In this section various CS1000 telephone features are defined. The feature described below is found by scrolling through this section.

Step 1 – For the **SPV - ACD Supervisor/Agent** field select **ACD Agent**.

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

5.8.1.3 Keys

Scroll further down the **Phone Details** form and locate the **Keys** section of the form.

5.8.1.3.1 Key 0

Step 1 – For Key **0** select **ACD – Auto Call Distribution**

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

The screenshot shows a form for configuring Key 0. The 'Key No.' is 0. The 'Key Type' is 'ACD - Auto. Call Distribution'. The 'Key Value' section contains the following fields: 'ACD Directory Number' with value 4012, 'CLID' (empty), 'Numeric/D<space>ACD Position ID' with value 0 2003, and 'ANIE Entry' (empty).

5.8.1.3.2 Key 3 - Single Call Appearance

Step 1 – 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)

Step 2 – Click on **Save** (not shown).

The screenshot shows a form for configuring Key 3. The 'Key No.' is 3. The 'Key Type' is 'SCR - Single Call Ringing'. The 'Directory Number' is 4014. The 'Multiple Appearance Redirection Prime(MARP)' checkbox is checked. The 'First Name' is Agent2, 'Last Name' is empty, 'Display Format' is First, Last, and 'Language' is Roman.

5.8.2 Analog Fax Line

Following the same procedures shown in **Section 5.8.1**, an analog port is defined for use with a fax machine; Directory Number **2779** using TN **000 1 10 00**. No special Features or Keys are defined.

The screenshot shows the 'General Properties' form for an analog fax line. The 'Customer Number' is 0. The 'Terminal Number' is 000 1 10 00. The 'Designation' is ANALOG. The 'Directory Number' is 2779. The 'CLID entry' is empty.

5.9 Changing RFC2833 DTMF Telephone Event Type

The CS1000 uses RFC2833 DTMF Telephone Event type 101. The IPTF service recommends the value 100 (see **Section 2.2, Item 4**). Therefore the CS1000 value is changed to 100 as follows:

Step 1 – From a CS1000 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 CS1000 will now use RFC2833 DTMF telephone event type 100.

Note – If the CS1000 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 or other Call Pilot® features. In addition to defining an entry in the CS1000 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 IPTF service inserts in *To* headers, see **Section 2.2, Item 9**), must be defined to Call Pilot® as well. This is required because Call Pilot® uses the contents of the *To* header for admission control.

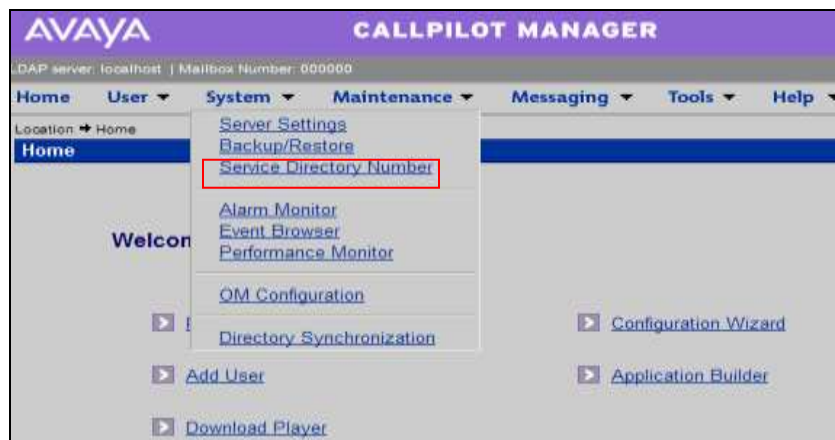
Note – The provisioning of Call Pilot® is beyond the scope of this document. Refer to [5] for more information.

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



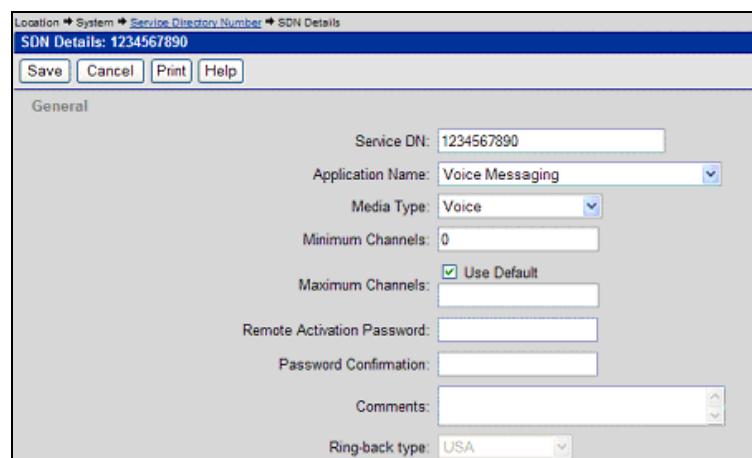
The image shows the CallPilot Manager login interface. At the top, there is a purple header with the text "> CALLPILOT MANAGER" and the AVAYA logo. Below the header, there is a section titled "Selecting a CallPilot Server:" with instructions: "Select a server and location from the list of preset servers, 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." To the right of the instructions, there are input fields for "Mailbox Number:" and "Password:", followed by a "Login" button. Below these, there is a "Server:" dropdown menu with the option "Preset server list; Enter data manually" selected. At the bottom, there are input fields for "Server:" and "Location:".

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



The image shows the CallPilot Manager main menu. At the top, there is a purple header with the AVAYA logo and the text "CALLPILOT MANAGER". Below the header, there is a navigation bar with tabs: "Home", "User", "System", "Maintenance", "Messaging", "Tools", and "Help". The "System" tab is selected, and its dropdown menu is open, showing options: "Server Settings", "Backup/Restore", "Service Directory Number" (highlighted with a red box), "Alarm Monitor", "Event Browser", "Performance Monitor", "QM Configuration", and "Directory Synchronization". The main content area shows a "Welcome" message and several links: "Configuration Wizard", "Application Builder", "Add User", and "Download Player".

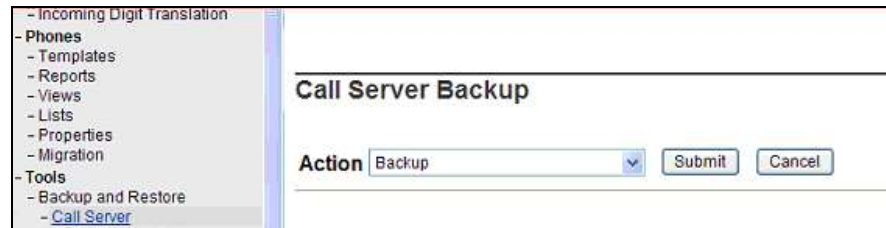
Step 3 – Click on **New** (not shown). Populate the form as shown below, where **1234567890** is the AT&T IP Toll Free customer Billing Number. Click on **Save**.



The image shows the "SDN Details" form in the CallPilot Manager. The form has a title bar with the text "Location: System > Service Directory Number > SDN Details" and "SDN Details: 1234567890". Below the title bar, there are buttons for "Save", "Cancel", "Print", and "Help". The form is divided into a "General" section. The "Service DN:" field is populated with "1234567890". The "Application Name:" dropdown menu is set to "Voice Messaging". The "Media Type:" dropdown menu is set to "Voice". The "Minimum Channels:" field is set to "0". The "Maximum Channels:" field has a checked box for "Use Default". The "Remote Activation Password:" and "Password Confirmation:" fields are empty. The "Comments:" field is a text area. The "Ring-back type:" dropdown menu is set to "USA".

5.11 CS1000 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 a web interface for the 'Call Server Backup' configuration. On the left is a navigation tree with the following items: '- Incoming Digit Translation', '- Phones', '- Templates', '- Reports', '- Views', '- Lists', '- Properties', '- Migration', '- Tools', '- Backup and Restore', and '- Call Server' (which is highlighted). The main content area is titled 'Call Server Backup'. Below the title, there is an 'Action' label followed by a dropdown menu currently set to 'Backup'. To the right of the dropdown are two buttons: 'Submit' and 'Cancel'.

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

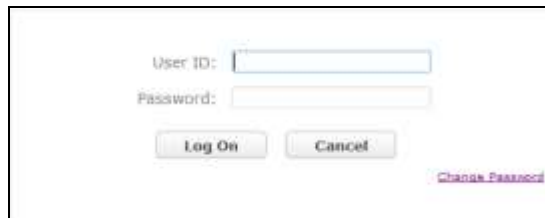
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

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 12**.

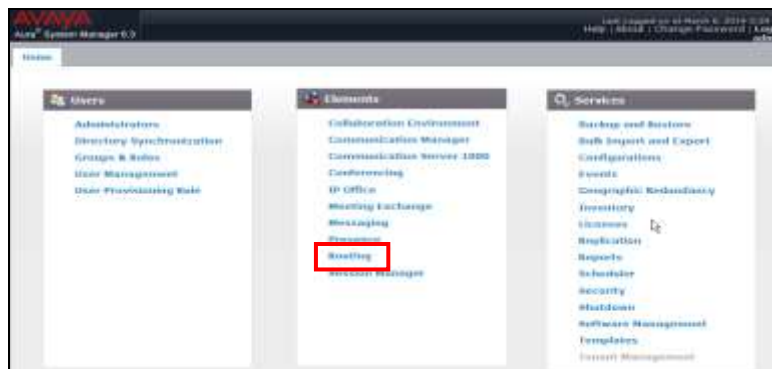
The following administration activities will be described:

- Define SIP Domain.
- Define Locations for CS1000 and for the Avaya SBCE.
- Configure the Adaptation Modules that will be associated with the SIP Entities for CS1000 and the Avaya SBCE.
- Define SIP Entities corresponding to CS1000 and Avaya SBCE.
- Define Entity Links describing the SIP trunk between CS1000 and Session Manager, and the SIP Trunk between Session Manager and Avaya SBCE.
- Define Routing Policies associated with CS1000 and Avaya SBCE.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Session Manager 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. From the welcome screen enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, **Home** screen is displayed.



From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



6.1 SIP Domain

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

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



6.2 Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g., 192.168.67.x for all devices on a particular subnet), individual devices (e.g., 192.168.67.10 for a devices' IP address), or an all inclusive Location may be defined where no IP address is specified. In the reference configuration an all inclusive Location called **Common** is used.

Note – As described above, Locations may be defined in several ways, depending on the CPE environment. The method used in the reference configuration should not be viewed as prescriptive.

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown).

Step 2 - In the **General** section, enter the following value:

- **Name:** Enter a descriptive name for the location (e.g., **Common**).

Use default values for remaining fields.

Step 3 – Verify that in the **Location Pattern** section, the **IP Address Pattern** field is blank (default). Let all other fields default.

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

6.3 Configure Adaptations

Session Manager can be configured to use Adaptation Modules designed to convert SIP headers into formats used by other Avaya products and endpoints, as well as formats required by Service Providers. In the reference configuration the following adaptations are used:

- **CS1000Adapter** – This adaptation is used to provide translation between various CS1000 generated headers, into formats used by other Avaya products and endpoints.
- **DigitConversionAdapter** – This adaptation modifies digit strings in the Request-URI. While this adaptation is not specified specifically in the reference configuration, its functionality is included as part of all other adaptations.

In addition, Module parameters **MIME=no** (to remove unnecessary CS1000 MIME headers), and **fromto=true** (to modify the From and To headers) are specified.

6.3.1 Adaptation to the CS1000

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

- **Adaptation Name:** Enter an identifier for the Adaptation Module.
- **Module Name:** Select **CS1000Adapter** from drop-down menu (or add an adapter with name **CS1000Adapter** if not previously defined).
- **Module Parameter Type:** Select **Name-Value Parameter**
- Click on **Add** and the Module option fields will open. Enter the following:
 - In the **Name** field enter **fromto**.
 - In the **Value** field enter **true**.
- Click on **Commit**.

Name	=	Value
fromto		true

Step 2 – In the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls to the CS1000.

- The CS1000 may insert local extensions in the PAI headers of responses or ReInvites. Session Manager will replace the local extension with its corresponding IPTF DID access number in the PAI header (see **Section 2.2, Item 6**). Enter the following:
 - **Matching Pattern** Enter a CS1000 extension (e.g., **4013**).
 - **Min** Enter minimum number of digits (e.g., **4**).
 - **Max** Enter maximum number of digits (e.g., **4**).
 - **Phone Context** Leave blank.
 - **Delete Digits** Enter **4**, to delete the extension.
 - **Insert Digits** Enter IPTF access number associated with the extension (e.g. **7325554301**).
 - **Address to modify** Enter **both**.
 - Repeat for all CS1000 extension/IPTF number associations.
- The CS1000 may insert IPTF DNIS digits in the PAI headers of responses or ReInvites. Session Manager will replace the IPTF DNIS digits with its corresponding IPTF DID access number in the PAI header (see **Section 2.2, Item 6**). Enter the following:
 - **Matching Pattern** Enter an IPTF DNIS number (e.g., **0000011051**).
 - **Min** Enter minimum number of digits (e.g., **10**).
 - **Max** Enter maximum number of digits (e.g., **10**).

- **Phone Context** Leave blank.
- **Delete Digits** Enter **10**, to delete the extension.
- **Insert Digits** Enter IPTF DID access number associated with the DNIS number (e.g., **7325554301**).
- **Address to modify** Enter **both**.
- Repeat for all CS1000 extension/IPTF number associations.

Step 3 - Click **Commit** (not shown) so save changes to the form.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*000011051	*10	*10		*10	7325554301	both		[PTF Invite PA]
*000011052	*10	*10		*10	7325554302	both		[PTF Invite PA]
*000011053	*10	*10		*10	7325554303	both		[PTF Invite PA]
*4013	*4	*4		*4	7325554302	both		[PTF 200OK PA]
*4014	*4	*4		*4	7325554301	both		[PTF 200OK PA]
*4015	*4	*4		*4	7325554303	both		[PTF 200OK PA]

Note - No **Digit Conversion for Outgoing Calls from SM** entries were required. Incoming IPTF calls have the inbound DNIS digits converted to their associated local extensions in the CS1000 Incoming Digit Translation table (see **Section 5.6**), so those digit conversions are not needed here.

6.3.2 Adaptation for calls from the CS1000 to AT&T

Some messages sent by the CS1000 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. The Module Parameter **MIME=no** is used to remove these headers.

Step 1 – Repeat the steps from **Section 6.3.1** with the following changes:

- **Adaptation Name:** Enter an identifier for the Adaptation Module.
- **Module Name:** Select **DigitConversionAdapter** from drop-down menu (or add an adapter with name **DigitConversionAdapter** if not previously defined)
- **Module Parameter:** Enter the following three parameters separated by spaces.
 - Enter **MIME** in the **Name** field, and **no** in the **value** field.

Step 2 – Click on **Commit** (not shown).

Name	Value
MIME	no

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

6.4 SIP Entities

SIP Entities are added for CS1000 and Avaya SBCE. A SIP Entity is created for Session Manager as part of the Session Manager installation. Its configuration is shown for completeness.

6.4.1 SIP Entity for the CS1000

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 CS1000 SIP GW.
- **Type:** Select **Other**.
- **Adaptation:** Select the Adaptation Module defined in **Section 6.3.1**.
- **Location:** Select the Location defined in **Section 6.2**.

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

- **SIP Link Monitoring:** Select **Use Session Manager Configuration**.

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

The screenshot displays the 'SIP Entity Details' configuration window. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main area is divided into several sections: 'General' (with fields for Name, FQDN or IP Address, Type, Adaptation, Location, Time Zone, SIP Timer B/F, Credential name, Call Detail Recording, and Connection Type Preference), 'Loop Detection' (with a Loop Detection Mode dropdown), 'SIP Link Monitoring' (with a dropdown set to 'Use Session Manager Configuration'), 'Entity Links' (with an 'Override Port & Transport with DNS SRV' checkbox), and a table for 'SIP Responses to an OPTIONS Request'.

Note - Once the Entity Links are provisioned for each Entity (see **Section 6.5**), the Entity Link information will also be displayed on the Entity forms.

6.4.2 SIP Entity for the Avaya SBCE

Repeat the steps in **Section 6.4.1** with the following changes:

- **Name:** A-SBCE.
- **FQDN or IP Address:** Enter the private side IP Address of the Avaya SBCE.
- **Type:** Select **Other**.
- **Adaptation:** Select the Adaptation Module defined in **Section 6.3.2**.
- **Location:** Select the Location defined in **Section 6.2**.

SIP Entity Details [Commit] [Cancel]

General

* Name: A-SBCE

* FQDN or IP Address: 192.168.70.120

Type: Other

Notes:

Adaptation: CSK to ATT

Location: Common

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:

Entity Links

Override Port & Transport with DNS SRV: ☐

[Add] [Remove]

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Delay New Service
Select: All, None							

SIP Responses to an OPTIONS Request

[Add] [Remove]

0 Items

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

6.4.3 SIP Entity for Session Manager

As mentioned above, the SIP Entity for Session Manager is created during the Session manager installation process, but is shown here for completeness.

The screenshot displays the 'SIP Entity Details' configuration window, which is divided into several sections:

- General:** Contains fields for Name (sm63), FQDN or IP Address (192.168.67.47), Type (Session Manager), Notes, Location (Common), Outbound Proxy, Time Zone (America/New_York), and Credential name.
- SIP Link Monitoring:** Includes a dropdown menu set to 'Use Session Manager Configuration'.
- Entity Links:** Features an 'Add' button and a table with columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The table is currently empty.
- Port:** Includes fields for TCP Failover port and TLS Failover port, with 'Add' and 'Remove' buttons. Below is a table with columns: Port, Protocol, Default Domain, and Notes. One entry is visible: Port 5060, Protocol TCP, Default Domain customersa.com.
- SIP Responses to an OPTIONS Request:** Includes an 'Add' button and a table with columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. The table is currently empty.

At the top right of the window are 'Commit' and 'Cancel' buttons.

6.5 Entity Links

The SIP trunk between Session Manager and CS1000 is defined by an Entity Link, as is the SIP trunk between Session Manager and Avaya SBCE.

Note – As mentioned previously, Entity Links created for the CS1000 and the Avaya SBCE will appear on their corresponding CS100E and Avaya SBCE SIP Entity forms. In addition, they will also appear on the Session Manager SIP Entity form.

6.5.1 Entity Link to CS1000 Entity

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

Step 2 - Click **New** (not shown), and enter the values shown below.

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

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
* sm63_CS1K	* sm63	TCP	* 5060	* CS1K	<input type="checkbox"/>	* 5060	trusted	<input type="checkbox"/>	

6.5.2 Entity Link to the Avaya SBCE

Repeat the steps in **Section 6.5.1** using the values shown below.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
* sm63_A-SBCE	* 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 CS1000, or the Avaya SBCE.

6.6.1 Routing Policy to the CS1000

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

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

Step 2 - In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the SIP Entity associated with CS1000 (see **Section 6.4.1**) and click **Select**. The selected SIP Entity displays on the Routing Policy Details page.

Step 3 - In the **Time of Day** section, add an appropriate time of day. In the sample configuration, time of day was not a relevant routing criteria, so the **24/7** range was chosen.

Step 5 - Use default values for remaining fields, and click **Commit**.

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 the Avaya SBCE

Repeat the steps in **Section 6.6.1** with the following changes:

- **Name:** Enter an identifier to define the routing policy (e.g. **A-SBCE**).
- Select the SIP Entity associated with Avaya SBCE (see **Section 6.4.2**).

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. As mentioned previously, in the reference configuration, the IPTF service sent 10 digit DNIS numbers with the format **00000xxxxx**.

Inbound calls to the CS1000

Step 1 - To define a dial pattern, select **Dial Patterns** from the navigation menu and click **New** (not shown).

Step 2 - In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to the CS1000 (e.g., **00000**).
- **Min:** Enter the minimum number of digits (e.g., **10**).
- **Max:** Enter the maximum number of digits (e.g., **10**).
- **SIP Domain:** Select **All**.
- **Notes:** Enter a brief description. [Optional].

Step 3 - In the **Originating Locations and Routing Policies** section, click **Add**.

Step 4 - The **Originating Locations and Routing Policy List** page opens.

- In the **Originating Location** list, select the location defined in **Section 6.2**.
- In the **Routing Policies** table, select the Routing Policy defined for CS1000 in **Section 6.6.1**.
- Click **Select** to save these changes and return to Dial Pattern Details page.

Step 5 – Click on **Commit**.

The screenshot shows the 'Dial Pattern Details' configuration page. The 'General' section contains the following fields:

- Pattern:** 00000
- Min:** 10
- Max:** 10
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** All
- Notes:** IPTF

The 'Originating Locations and Routing Policies' section includes an 'Add' button and a table with the following data:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Common		To_CS1K	1	<input type="checkbox"/>	CS1K	

The 'Denied Originating Locations' section includes an 'Add' button and a table with the following data:

Originating Location	Notes

7 Configure Avaya Session Border Controller for Enterprise

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

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [10 and 11] 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.

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (192.168.70.120), with access to the Main site. The connection to AT&T uses the Avaya SBCE public interface B1 (10.10.10.10).

The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

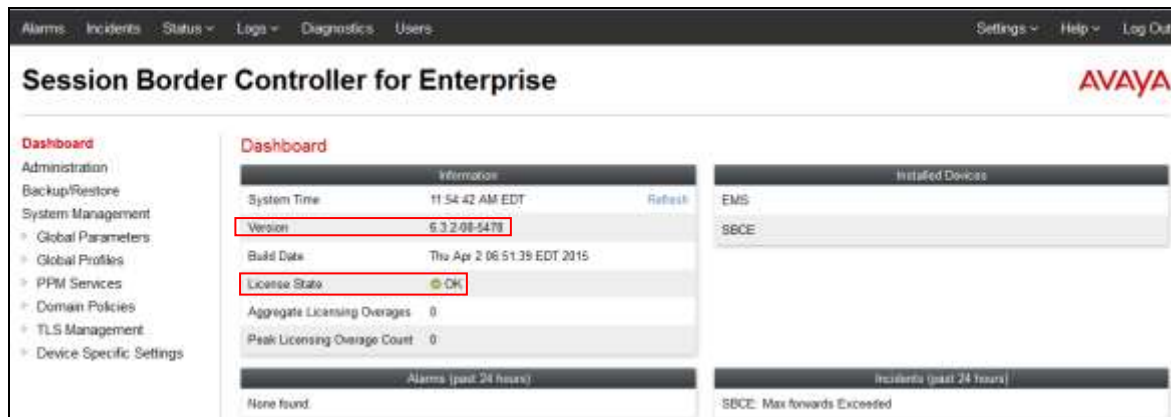
Step 1 - Access the web interface by typing “https://x.x.x.x” (where x.x.x.x is the management IP address of the Avaya SBCE).

Step 2 - Enter the Username and click on **Continue**.

Step 3 - Enter the password and click on **Log In**.

Step 4 - The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

Note – The provisioning described in the following sections use the menu options listed in the left hand column shown below.



7.1 System Management/Status

Step 1 - Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.

Note – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



Step 2 - Click on **View** (shown above) to display the **System Information** screen.

System Information: SBCE

General Configuration
 Appliance Name: SBCE
 Box Type: SIP
 Deployment Mode: Proxy

Device Configuration
 HA Mode: No
 Two Bypass Mode: No

License Allocation
 Standard Sessions: 0
 Advanced Sessions: 0
 Scopia Video Sessions: 0
 Encryption: [X]

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
192.168.70.120	192.168.70.120	255.255.255.0	192.168.70.1	A1
10.10.10.10	10.10.10.10	255.255.255.240	10.10.10.1	B1

DNS Configuration
 Primary DNS: 192.168.67.5
 Secondary DNS:
 DNS Location: DMZ
 DNS Client IP: 192.168.70.120

Management IP(s)
 IP: 192.168.63.64

7.2 Global Profiles

Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

7.2.1 Server Interworking – Avaya

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Session Manager.

Step 1 - Select **Global Profiles** → **Server Interworking** from the left-hand menu.

Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.

Interworking Profiles: avaya-ru

Clone

Interworking Profiles
 Add
 cs2100
 avaya-ru
 OCS-Edge-Server
 cisco-ccm
 cspg

General | Timers | URI Manipulation | Header Manipulation | Advanced

General
 Hold Support: NONE
 180 Handling: None
 181 Handling: None

Step 3 - Enter profile name: (e.g., **Avaya_Trunk_SI**), and click **Finish**.

Clone Profile

Profile Name: avaya-ru
 Clone Name: Avaya_Trunk_SI
 Finish

Step 4 - The new **Avaya_Trunk_SI** profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit** (not shown).



Step 5 - The **General** options screen will open.

- Check **T38 Support**. All other options can be left with default values, and click **Next**.



Step 6 - On the **Privacy/DTMF** window, select **Finish** to accept default values.

Editing Profile: IPO_S1

Privacy

Privacy Enabled ☒

User Name

P-Asserted-Identity ☐

P-Preferred-Identity ☐

Privacy Header

DTMF

DTMF Support ☒ None ☐ SIP NOTIFY ☐ SIP INFO

Step 7 - Returning to the **General** screen, select the **Advanced** tab shown in **Step 4**, and accept the default values. Click **Finish**.

Editing Profile: IPO_S1

Record Routes ☒ None ☐ Single Side ☐ Both Sides

Topology Hiding: Change Call-ID ☐

Call-Info NAT ☐

Change Max Forwards ☒

Include End Point IP for Context Lookup ☒

OCS Extensions ☐

AVAYA Extensions ☒

NORTEL Extensions ☐

Diversion Manipulation ☐

Diversion Header URI

Metaswitch Extensions ☐

Reset on Talk Spurt ☐

Reset SRTP Context on Session Refresh ☐

Has Remote SBC ☒

Route Response on Via Port ☐

Cisco Extensions ☐

7.2.2 Server Interworking – AT&T

Repeat the steps shown in **Section 7.2.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

- Click on **Add** and create a new profile for AT&T (e.g., **ATT_Trunk_SI**).
- On the **General** screen check **T38 Support**.
- All other options can be left as default.
- Accept default values for the **Privacy/DTMF**, **SIP Timers/Transport Timers**, and **Advanced** screens.

7.2.3 Signaling Manipulation

Note – The use of Signaling Manipulation scripts demands higher processing requirements for the Avaya SBCE. Therefore, the use of Signaling Rules (**Section 7.3.3**) is the preferred method for header/message manipulation. Signaling Manipulations should only be used in cases where the use of Signaling Rules does not meet the desired result. Refer to [10] for information on the Avaya SBCE scripting language.

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate/remove SIP headers/parameters. In the reference configuration Signaling manipulations are used to perform the following:

- Remove the Telephone Event 111 sent by the CS1000 (see **Section 2.2, item 4**).
- Modify AT&T Maxptime=30 to Ptime=30 (see **Section 2.2, item 1**).
- Remove Remote-Address headers added by the Avaya SBCE (see **Section 2.2, item 3**).

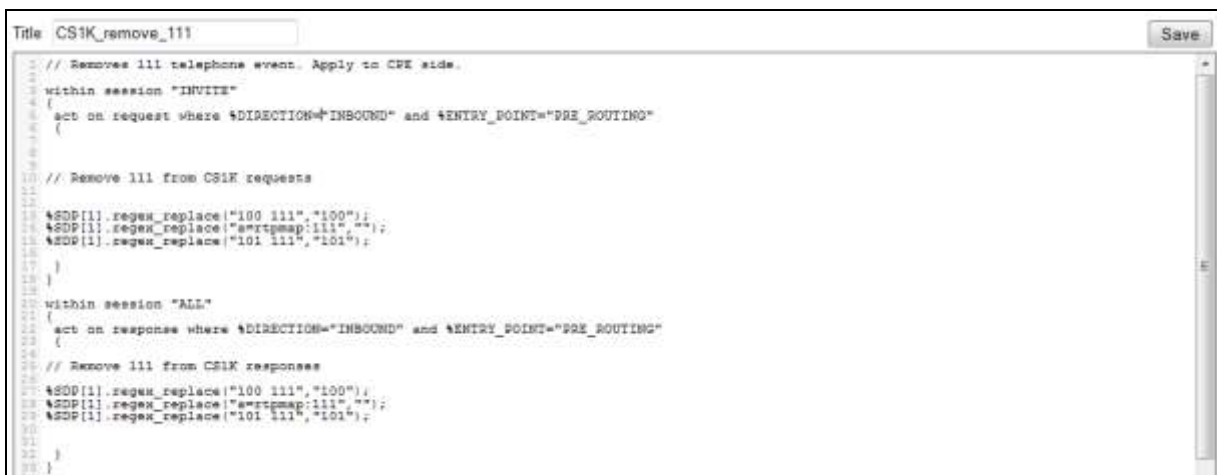
7.2.3.1 Remove Telephone Event 111

Step 1 - Select **Global Profiles** from the menu on the left-hand side.

Step 2 - Select **Signaling Manipulation**.

Step 3 - Click **Add Script** (not shown) and the script editor window will open.

Step 4 - Enter a name for the script in the **Title** box (e.g., **CS1K_remove_111**). The following script is defined:



```
Title: CS1K_remove_111
// Removes 111 telephone event. Apply to CPE side.
within session "INVITE"
{
  act on request where $DIRECTION="INBOUND" and $ENTRY_POINT="PRE_ROUTING"
  {
    // Remove 111 from CS1K requests
    $SDP[1].regex_replace("100 111","100");
    $SDP[1].regex_replace("a=rtspmap:111","");
    $SDP[1].regex_replace("101 111","101");
  }
}

within session "ALL"
{
  act on response where $DIRECTION="INBOUND" and $ENTRY_POINT="PRE_ROUTING"
  {
    // Remove 111 from CS1K responses
    $SDP[1].regex_replace("100 111","100");
    $SDP[1].regex_replace("a=rtspmap:111","");
    $SDP[1].regex_replace("101 111","101");
  }
}
```

Step 5 - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the Session Manager Server Configuration in **Section 7.2.4**.

7.2.3.2 Modify Maxptime and Remove Remote-Address

Repeating the steps in **Section 7.2.3.1**, create the following script to convert the AT&T Maxptime=30 to Ptime=30, and remove the Remote-Address header added by the Avaya SBCE.



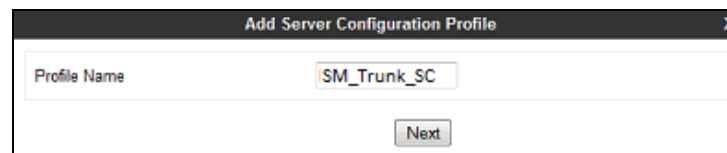
This script is applied to the AT&T Server Configuration in **Section 7.2.5**.

7.2.4 Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

Step 1 - Select **Global Profiles → Server Configuration** from the left-hand menu.

Step 2 - Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM_Trunk_SC**) and click **Next**.



Step 3 - The **Add Server Configuration Profile** window will open.

- Select **Server Type: Call Server**.
- **IP Address: 192.168.67.47** (Session Manager network IP Address).
- **Supported Transports: Check TCP**.
- **TCP Port: 5060**.
- Select **Next**.

Step 4 - The **Authentication** and **Heartbeat** windows will open (not shown).

- Select **Next** to accept default values.

Step 5 - The **Advanced** window will open.

- Select **Avaya_Trunk_SI** (created in **Section 7.2.1**), for **Interworking Profile**.
- In the **Signaling Manipulation Script** field select the script defined in **Section 7.2.3.1**.
- Select **Finish**.

Note – Since TCP transport is specified in **Step 3**, then the **Enable Grooming** option should be enabled.

7.2.5 Server Configuration – AT&T

Note – The IPTF service may provide a Primary and Secondary Border Element. This section describes the connection to a single (Primary) Border Element. See **Addendum 1** for information on configuring two IPTF Border Elements (Primary & Secondary).

Repeat the steps in **Section 7.2.4**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

Step 1 - Select **Add Profile** and enter a Profile Name (e.g., **ATT_SC**) and select **Next**.

Step 2 - On the **General** window (not shown), enter the following.

- Select Server Type: **Trunk Server**.
- **IP Address: 10.10.10.11** (AT&T Border Element IP address).
- **Supported Transports:** Check **UDP**.
- **UDP Port: 5060**.

- Select **Next**.

Step 3 - On the **Advanced** window, enter the following.

- Select **ATT_SI** (created in **Section 7.2.2**), for **Interworking Profile**
- In the **Signaling Manipulation Script** field select the script defined in **Section 7.2.3.2**.

7.2.6 Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

Step 1 - Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown).

Step 2 - Enter a **Profile Name**: (e.g., **SM_RP**) and click **Next**.

Step 3 - The Routing Profile window will open (not shown). Keeping all the default values, click on **Add** to define a next-hop address for Session manager. Enter the following values:

- **Priority/Weight** = **1**.
- **Server Configuration** = **SM_Trunk_SC** (from **Section 7.2.4**).
- **Next Hop Address** = Select the **192.168.67.47:5060 (TCP)** entry from the drop down menu (Session Manager IP address). Also note that the **Transport** field is grayed out.
- Click on **Finish**.

7.2.7 Routing – To AT&T

Repeat the steps in **Section 7.2.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

- Add a new profile (e.g., **ATT_RP**).
- On the Next-Hop Address window populate the following fields:
 - **Priority/Weight = 1.**
 - **Server Configuration = ATT_SC** (from **Section 7.2.5**).
 - **Next Hop Address:** Verify that the **10.10.10.11:5060** entry from the drop down menu is selected (AT&T Border Element IP address).
- Use default values for all other parameters.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT_SC	10.10.10.11:5060 (UDP)	None

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.10.10.11	UDP

7.2.8 Topology Hiding – Avaya Side

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

Step 1 - Select **Global Profiles** → **Topology Hiding** from the left-hand side menu.

Step 2 - Select the **Add** button (not shown), enter Profile Name: (e.g., **Avaya_TH**). Click **Next**.

Step 3 - The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until no new headers are added to the list, and the **Add Header** button is no longer displayed.

Topology Hiding Profile

Add Header

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete

Back Finish

Topology Hiding Profile

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

Back Finish

Step 4 - Populate the fields as shown below, and click **Finish** (not shown). Note that **customerera.com** is the domain used by the CPE (see **Sections 5.5.1** and **6.1**).

Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Refer-To	IP/Domain	Overwrite	customerera.com	Delete
SDP	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	customerera.com	Delete
Referred-By	IP/Domain	Overwrite	customerera.com	Delete
Request-Line	IP/Domain	Overwrite	customerera.com	Delete
From	IP/Domain	Overwrite	customerera.com	Delete

7.2.9 Topology Hiding – AT&T Side

Repeat the steps in **Section 7.2.8**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

- Enter a Profile Name: (e.g., **ATT_TH**).
- Use the default values for all fields and click **Finish** (not shown).

Edit Topology Hiding Profile

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

7.3 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.3.1 Application Rules

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

Step 2 - Select the **default-trunk** rule (not shown).

Step 3 - Select the **Clone** button (not shown), and the **Clone Rule** window will open (not shown).

- In the **Clone Name** field enter **SIP-Trunk_AR**.
- Click **Finish** (not shown). The completed **Application Rule** is shown below.

The screenshot shows the 'Application Rules: SIP_Trunk_AR' configuration window. On the left is a sidebar menu with 'Application Rules' selected. The main area has a 'Filter By Device' dropdown and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a table of application rules. The 'SIP_Trunk_AR' rule is highlighted. The table has columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The 'SIP_Trunk_AR' rule is of type 'Audio' with In and Out ports set to 80 and Maximum Concurrent Sessions set to 2000. Below the table is a 'Miscellaneous' section with fields for CDR Support (None) and RTCP Keep-Alive (No). An 'Edit' button is at the bottom right.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	80	80	2000	2000
Video				
IM				

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

7.3.2 Media Rules

Media Rules are used to define QOS parameters. The Media Rule described below will be applied to both directions, and therefore, only one rule is needed.

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

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

Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **Avaya-low-med_MR**.
- Click **Finish**. The newly created rule will be displayed.

Step 4 - Highlight the **Avaya-low-med_MR** rule just created (not shown):

- Select the **Media QOS** tab (not shown).
- Click the **Edit** button and the **Media QOS** window will open (not shown).
- Check the **Media QOS Marking** field is **Enabled**.
- Select the **DSCP** box.
- **Audio**: Select **EF** from the drop-down.
- **Video**: Select **EF** from the drop-down.

Step 5 - Click **Finish** (not shown). The completed **Media Rule** screen is shown below.



7.3.3 Signaling Rules

In the reference configuration, Signaling Rules are used to filter various SIP headers.

7.3.3.1 Avaya – Signaling Rules

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

Step 2 - The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.

Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

- In the **Rule Name** field enter **CS1K_SR**.
- Click **Finish**. The newly created rule will be displayed (not shown).

7.3.3.1.1 Avaya – Signaling Rule - Request Headers Tab

The following Signaling Rules remove SIP headers sent by CS1000 SIP requests that are either not supported or required by AT&T.

Step 1 - Highlight and the **CS1K_SR** rule created in **Section 7.3.3.1**, select the **Request Headers** tab, and enter the following:

- Select the **Add In Header Control** button (not shown). The **Add Header Control** window will open.
- Select the **Request Headers** tab (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **P-Location**.
- From the **Method Name** menu select **All**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

Step 2 - Click **Finish**

Step 5 - Repeat **Steps 1 & 2** to create a rule to remove the following headers:

- **Alert-Info**, (Proprietary = No).
- **History-Info**, (Proprietary = No).
- **Remote-Party-ID**, (Proprietary = No).
- **AV-Global-Session-ID**, (Proprietary = Yes).
- **P-AV-Message-ID**, (Proprietary = Yes).
- **P-AV-Message-ID**, (Proprietary = Yes).
- **X-nt-e164-clid**, (Proprietary = Yes).

The completed Request Headers form is shown below. Note that 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

7.3.3.1.2 Avaya – Signaling Rule Response Headers Tab

The following Signaling Rules remove headers sent by CS1000 SIP responses (e.g., 1xx and/or 200OK) that are either not supported or required by AT&T.

Step 1 - Highlight the **Avaya_SR** rule created in **Section 7.3.3.1**, and using the same procedures shown in **Section 7.3.3.1.1**, remove the following headers:

- **P-Location** 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.
- In the **Header Name** field, enter **P-Location**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**.
- **P-Location** header from **2xx** responses.
 - From the **Response Code** menu select **2xx**.
 - Click **Finish**.

Step 2 – Repeat **Step 1** to remove the following header for 1xx and 2xx responses:

- **P-AV-Message-ID**, (Proprietary = Yes).
- **AV-Global-Session-ID**, (Proprietary = Yes).
- **Remote-Party-ID**, (Proprietary = No).
- **History-Info**, (Proprietary = No).

The completed Response Headers form is shown below. Note that the Direction column says “IN”.

Signaling Rules: CS1K_SR

Click here to add a description

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

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

Step 2 - Highlight the **Avaya_SR** rule, select the **Signaling QOS** tab and enter the following:

- Click the **Edit** button and the **Signaling QOS** window will open (not shown).
- Verify that **Signaling QOS** is selected.
- Select **DCSP**.
- Select **Value = EF**.

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

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
Signaling QoS						<input checked="" type="checkbox"/>
QoS Type						DSCP
DSCP						EF

7.3.3.2 Signaling Rule Request Headers Tab

The Remote-Address header inserted by the Avaya SBCE is removed prior to sending it to AT&T (see **Section 2.2, Item 3**). Repeat the steps in **Section 7.3.3.1.1** to remove the Remote-Address header. The completed Request Headers form is shown below. Note that the Direction column says “OUT”.

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
Application Rules
Border Rules

Signaling Rules: ATT_SR

Add
Filter By Device...
Rename Clone Delete

Signaling Rules

default
No-Content-Type-Ch...
ATT_SR
CS1K_SR

Click here to add a description

General Requests Responses Request Headers Response Headers Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Remote-Address	ALL	Forbidden	Remove Header	Yes	OUT

Note - No Response Header manipulation is required.

Step 1 - Highlight the **ATT_SR** rule, select the **Signaling QOS** tab and repeat **Steps 2 & 3** from **Section 7.3.3.1**.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
Signaling QoS						<input checked="" type="checkbox"/>
QoS Type						DSCP
DSCP						EF
Edit						

7.3.4 Endpoint Policy Groups – Avaya Connection

Step 1 - Select **Domain Policies** from the menu on the left-hand side.

Step 2 - Select **End Point Policy Groups**.

Step 3 - Select **Add**.

- **Name:** Avaya_default-low_PG.
- **Application Rule:** SIP_Trunk_AR (created in **Section 7.3.1**).
- **Border Rule:** default.
- **Media Rule:** Trunk_low_med_MR (created in **Section 7.3.2**).
- **Security Rule:** default-low.
- **Signaling Rule:** CS1K_SR (created in **Section 7.3.3**).

Step 4 - Select **Finish** (not shown). The completed **Policy Groups** screen is shown below.



7.3.5 Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps 1 through 4 from Section 7.3.4 with the following changes:

- **Group Name:** ATT_default-low_PG.
- **Signaling Rule:** ATT_SR (created in Section 7.3.3).



7.4 Device Specific Settings

7.4.1 Network Management

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

Step 2 - The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.



Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

Interfaces		Networks				
					Add	
Name	Gateway	Subnet Mask	Interface	IP Address		
Network_A1	192.168.70.1	255.255.255.0	A1	192.168.70.120	Edit	Delete
Network_B1	10.10.10.1	255.255.255.240	B1	10.10.10.10	Edit	Delete

7.4.2 Advanced Options

In **Section 7.4.3**, the media UDP port ranges required by AT&T are configured (16384 – 32767). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be defined in **Section 7.4.3**.

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

Step 2 - Select the **Port Ranges** tab.

Step 3 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 4 - Scroll to the bottom of the window and select **Save** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

PPM Services

Domain Policies

TLS Management

Device Specific Settings

Network Management

Media Interface

Signaling Interface

End Point Flows

Session Flows

DMZ Services

TURN/STUN Service

SNMP

Syslog Management

Advanced Options

Troubleshooting

Advanced Options: SBCE

Devices

SBCE

CDR Listing

Feature Control

SSP Options

Network Options

Port Ranges

RTCP Monitoring

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

Port Range Configuration	
Signaling Port Range	12000 - 16000
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	9000 - 9999
HTTP Port Range	30000 - 31000
OCS FTP Listen Port Range	6881 - 6901
OCS Alternate FTP Listen Port Range	11175 - 11185

Save

7.4.3 Media Interfaces

As mentioned in **Section 7.4.2**, the IPTF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the IPTF service.

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).

Step 2 - Select **Media Interface**.

Step 3 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** **Inside_Trunk_MI**.
- **IP Address:** **192.168.70.120** (Avaya SBCE A1 address).
- **Port Range:** **16384 – 32767**.

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

Step 5 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** **Outside_Trunk_MI**.
- **IP Address:** **10.10.10.10** (Avaya SBCE B1 address).
- **Port Range:** **16384 – 32767**.

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**). The completed **Media Interface** screen is shown below.



7.4.4 Signaling Interface

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).

Step 2 - Select **Signaling Interface**.

Step 3 - Select **Add** (not shown) and enter the following:

- **Name:** **Inside_Trunk_SI**.
- **IP Address:** **192.168.70.120** (Avaya SBCE A1 address).
- **TCP Port:** **5060**.

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

Step 5 - Select **Add** again, and enter the following:

- **Name:** **Outside_Trunk_SI**.
- **IP Address:** **10.10.10.10** (Avaya SBCE B1 address).
- **UDP Port:** **5060**.

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).



7.4.5 Endpoint Flows

Endpoint flows combine the previously defined Device Specific Settings for both the CS1000 and AT&T.

7.4.5.1 Endpoint Flows – For Session Manager

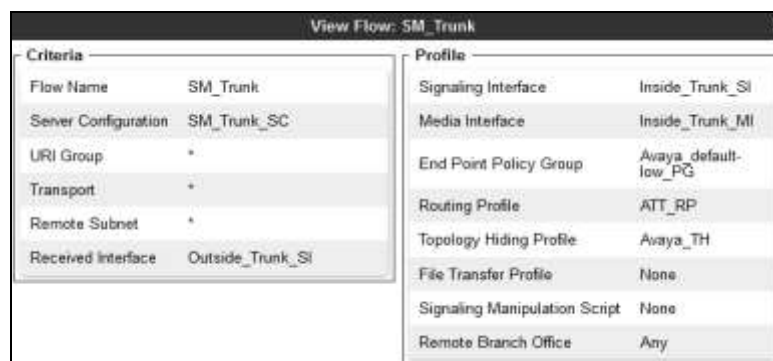
Step 1 - Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side.

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

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

- **Name:** SM_Trunk.
- **Server Configuration:** SM_Trunk_SC (Section 7.2.4).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Outside_Trunk_SI (Section 7.4.4).
- **Signaling Interface:** Inside_Trunk_SI (Section 7.4.4).
- **Media Interface:** Inside_Trunk_MI (Section 7.4.3).
- **End Point Policy Group:** Avaya_default-low_PG (Section 7.3.4).
- **Routing Profile:** ATT_RP (Section 7.2.7).
- **Topology Hiding Profile:** Avaya_TH (Section 7.2.8).
- Let other values default.

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



7.4.5.2 Endpoint Flows – For AT&T

Step 1 - Repeat steps 3 and 4 from Section 7.4.4.1, with the following changes:

- **Name:** ATT.
- **Server Configuration:** ATT_SC (Section 7.2.5).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Inside_Trunk_SI (Section 7.4.4).
- **Signaling Interface:** Outside_Trunk_SI (Section 7.4.4).
- **Media Interface:** Outside_Trunk_MI (Section 7.4.3).
- **End Point Policy Group:** ATT_default-low_PG (Section 7.3.5).
- **Routing Profile:** SM_RP (Section 7.2.6).
- **Topology Hiding Profile:** ATT_TH (Section 7.2.9).

Criteria		Profile	
Flow Name	ATT	Signaling Interface	Outside_Trunk_SI
Server Configuration	ATT_SC	Media Interface	Outside_Trunk_MI
URI Group	*	End Point Policy Group	ATT_default-low_PG
Transport	*	Routing Profile	SM_RP
Remote Subnet	*	Topology Hiding Profile	ATT_TH
Received Interface	Inside_Trunk_SI	File Transfer Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any

The completed **End Point Flows** screen is shown below.

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP

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
2	Anyto_Traffic	*	Outside_Trunk_SI	Inside_Trunk_SI	Anyto_default-low_PG	Te_ATT_VTE

8 Configure Avaya Aura® Contact Center

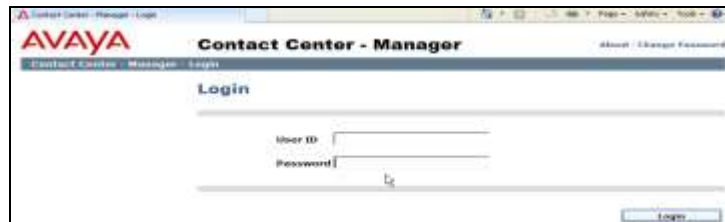
In the reference configuration, Avaya Aura® Contact Center is used to manage Agent functionalities and integrate these functions to the CS1000.

Note - In the reference configuration, Application Module Link (AML) protocol is used between the CS1000 and Avaya Aura® Contact Center. The provisioning and establishment of the AML connection between Avaya Aura® Contact Center and the CS1000 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 [12-14] for more information). Only the Agent provisioning supporting the AT&T IP Toll Free solution testing is shown below.

8.1 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 5.8**), 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**
 Last Name: **agent2**
 Title:
 Department:
 Language: **English**
 Comment:

User Type: **Agent**
 Login ID: **4014**
 Personal DN:
 ACD Queue:
 ACD Queue Error:

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

Associate User Account

Agent Information

Primary Supervisor: **Default Supervisor**
 Agent Key:
 Login Status: **Logged Out**

Call Presentation: **Call_Centre_Administrator**
 Threshold: **Agent_Template**
 Tn Name:

Contact Types

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

Skillsets

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

Assign Skillsets

Partitions

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

8.2 Verify Control DN (CDN) and Agent Connection Status

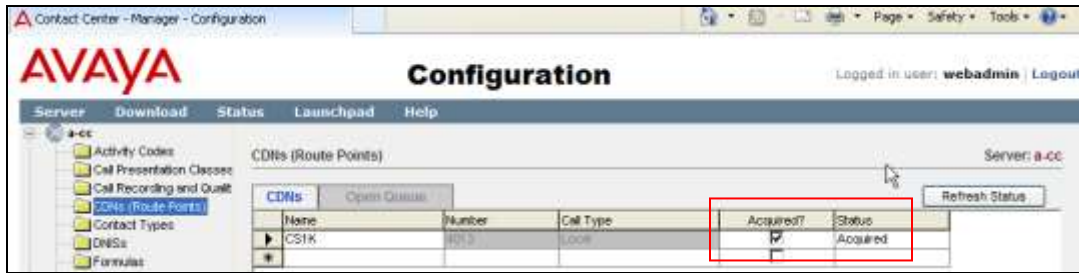
8.2.1 CDN Connection status

The Avaya Aura[®] Contact Center/CS1000 CDN connection status can be verified as follows.

Step 1 – Connect to **Launchpad** as described in **Section 8.1**.

Step 2 – Select **Configuration**.

Step 3 – From the left hand menu select **CDNs (Route Points)**. The connection provisioned on Avaya Aura[®] Contact Center to the CS1000 will be displayed. Verify the status is **Acquired**.

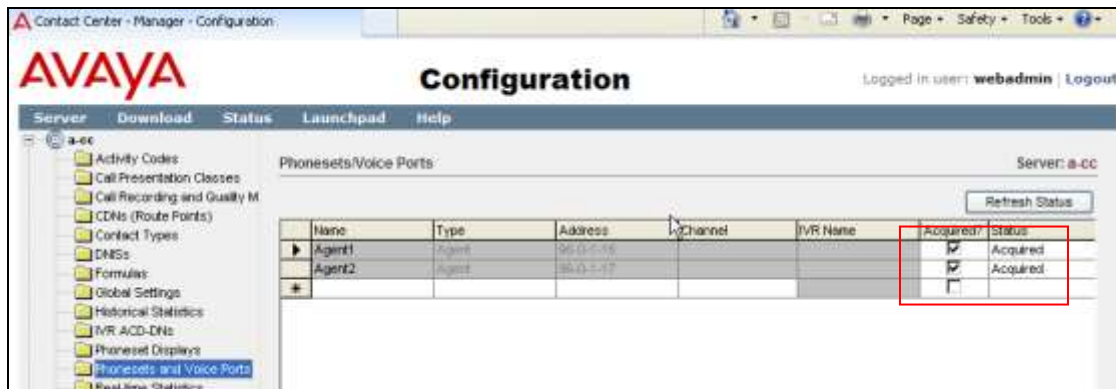


8.2.2 Agent Connection status

Step 1 – Connect to **Launchpad** as described in **Section 8.1**.

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**.



9 AT&T IP Toll Free Service

The IPTF service provided DID/DNIS numbers for the reference configuration. The DNIS numbers terminated to the CS1000 location via the IPTF service. Any DID and DNIS numbers shown in these application notes are examples. Customers will be assigned DIDs by AT&T. It should be noted that the DID numbers dialed, and the DNIS numbers inserted into SIP headers may not be the same digit strings.

The IPTF service also provides a network border element IP address for the reference configuration. Customers will be assigned a border element IP address by AT&T.

10 Verification Steps

The following steps may be used to verify the reference configuration.

10.1 General

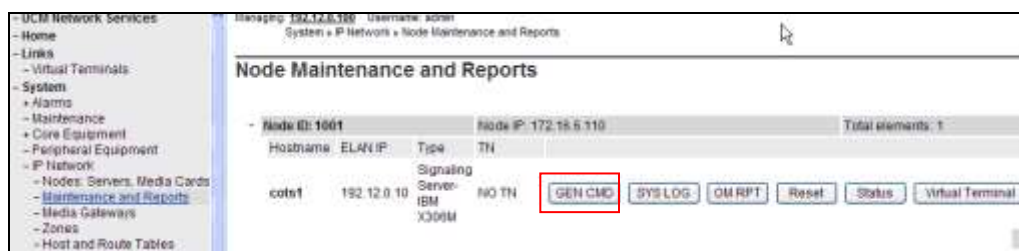
- Place an inbound call an agent or telephone, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly.
- Place an inbound call to an agent queue with no available agent. Verify that the call covers to Music On Hold, and that the call is connected when an agent is available.

10.2 CS1000 Verifications

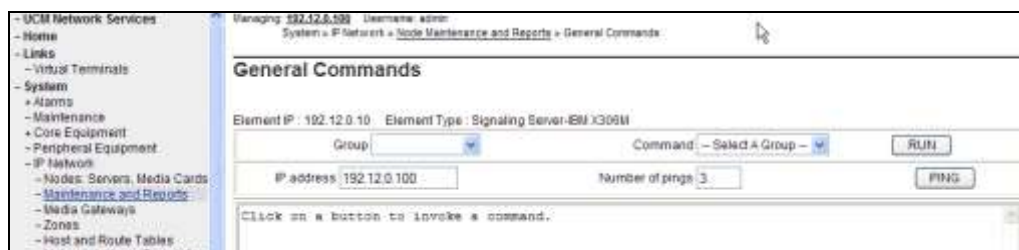
This section illustrates verifications that may be performed using the CS1000 Element Manager GUI.

10.2.1 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** as **Active**.

General Commands

Element IP: 192.12.0.10 Element Type: Signaling Server-IBM X309M

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

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

SIPGw 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

10.2.2 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

D-Channel Diagnostics

- MSDL Diagnostics
- TMDI Diagnostics

When **D-Channel Diagnostics** is selected on the right menu above, 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

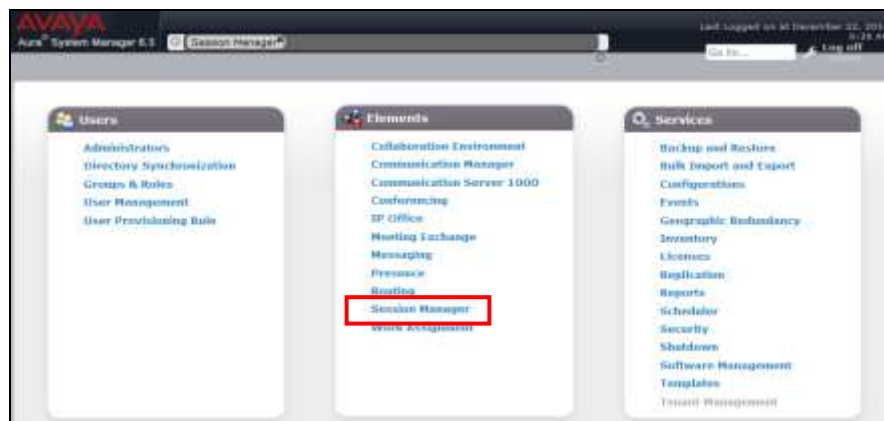
Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	<input type="button" 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	RECV	PDCH	BDCH
<input type="radio"/> 015	VDCH	OPER	EST	ACTV	AUTO				
<input type="radio"/> 020	SIPLINE	OPER	EST	ACTV	AUTO				

10.3 Avaya Aura® Session Manager

Session Manager configuration may be verified via System Manager.

Step 1 – Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



Step 2 – The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns all show good status.

In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **2** Entities defined.

Session Manager Dashboard 5.3.15.8.031364

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

Session Manager Instances

Service State: [Shutdown System] As of 10:35 AM

Show: All

	Service Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Big Brother Status	Data Replication	User Data Storage Status	Version
<input type="checkbox"/>	sm63	Core	✓	0/0/0	Up	Accept New Service	0/2	0	1/1	✓	✓	5.3.15.8.031364

Select: All, None

Step 3 - Clicking on the **0/2** entry (shown above) in the **Entity Monitoring** column, results in the following display:

All Entity Links for Session Manager: sm63

Summary View

Status Details for the selected Session Manager:

Filter: Enable

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
A-SBCE	192.168.70.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP
CSIX	172.16.6.110	5060	TCP	FALSE	UP	200 OK	UP

Note the **A-SBCE** Entity from the list of monitored entities above. The **Reason Code** column indicates that Session Manager has received a **SIP 405 Method Not Allowed** response to the SIP OPTIONS it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Also note that the Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T IPTF Border Element, and it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends it back to Session Manager.

Another useful tool is to select **System Tools** → **Call Routing Test** (not shown) from the left hand menu. This tool allows specific call criteria to be entered, and the simulated routing of this call through Session Manager is then verified.

10.4 Avaya Session Border Controller for Enterprise

10.4.1 System Status

Step 1 – Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the Dashboard screen.

Alarms Incidents Status Logs Diagnostics Users

Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
TLS Management
Device Specific Settings

Dashboard

Information

System Time	09:36:24 AM EST	Refresh
Version	6.3.1-22-4853	
Build Date	Fri Nov 21 17:35:09 EST 2014	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices

EMS
SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

SBCE: Max Inroads Exceeded

Notes

No notes found.

Add

10.4.2 Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to Device Specific Settings → Advanced Options → Troubleshooting → Trace

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

- Select the desired **Interface** from the drop down menu (e.g., **All**).
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
- Click **Start Capture** to begin the trace.

Note – Specifying **All** in the **Interface** field will result in the Avaya SBCE capturing traffic from both the A1 and B1 interfaces defined in the reference configuration. Also, when specifying the **Maximum Number of Packets to Capture**, be sure to estimate a number large enough to include all packets for the duration of the test.

The screenshot shows the 'Trace: SBCE' interface with the 'Packet Capture' tab selected. The 'Packet Capture Configuration' window is open, displaying the following fields: Status (Ready), Interface (Any), Local Address (IP:Port) (All), Remote Address (IP:Port) (*), Protocol (All), Maximum Number of Packets to Capture (5000), and Capture Filename (TEST.pcap). The 'Start Capture' and 'Clear' buttons are at the bottom right.

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

The screenshot shows the 'Trace: SBCE' interface with the 'Packet Capture' tab selected. The 'Packet Capture Configuration' window is open, displaying the following fields: Status (In Progress), Interface (Any), Local Address (IP:Port) (All), Remote Address (IP:Port) (*), Protocol (All), Maximum Number of Packets to Capture (5000), and Capture Filename (TEST.pcap). The 'Stop Capture' button is highlighted at the bottom right. A blue banner at the top of the configuration window states: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.'

Step 3 – Run the test.

Step 4 – When the test is completed, select **Stop Capture** button shown above.

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

Step 6 - Click on the **File Name** link to download the file or use Wireshark to open the trace.

Trace: SBCE

Devices	Packet Capture	Captures
SBCE	Last Modified ▾	Descending ▾
	Sort	Reset
		Refresh
	File Name	File Size (bytes)
	TEST_20150106085556.pcap	94,208
		Last Modified
		January 6, 2015 9:56:11 AM EST
		Delete

11 Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000 7.6, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.3 can be configured to interoperate successfully with AT&T IP Toll Free service via either AVPN or MIS-PNT transport, within the constraints specified in **Section 2.2**.

Testing was performed on a simulated AT&T IP Toll Free service circuit. The reference configuration shown in these Application Notes is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

12 References

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

Avaya Communication Server 1000

- [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] *Deploying Avaya Aura® Session Manager*, Release 6.3, Issue 6, November 2014
- [7] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014
- [8] *Deploying Avaya Aura® System Manager on System Platform*, Release 6.3, Issue 4, June 2014
- [9] *Administering Avaya Aura® System Manager for Release 6.3.10*, Release 6.3, November 2014

Avaya Session Border Controller for Enterprise

- [10] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014
- [11] *Deploying Avaya Session Border Controller for Enterprise*, Release 6.3, October 2014

Avaya Aura® Contact Center

- [12] *Avaya Aura® Contact Center Server Administration*, Release 6.4, 44400-610, Issue 05.03, December 2014
- [13] *Avaya Aura® Contact Center Administration—Client Administration*, Release 6.4, 44400-611, Issue 05.04, May 2015
- [14] *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*, Release 6.4, 44400-512, Issue 05.03, December

AT&T IP Toll Free Service:

- [15] AT&T IP Toll Free Service description - <http://www.business.att.com/enterprise/Service/voice-services/contact-center-solutions/ip-toll-free/>

13 Addendum 1 – Redundancy to Multiple AT&T Border Elements

The IPTF service may provide multiple network border elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T border elements **10.10.10.11** and **10.10.10.12**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to 10.10.10.12.

13.1 Configure the Secondary Border Element Server Configuration

Step 1 - Repeat the steps in **Section 7.2.5**, using the parameters shown below, to create a Server Configuration for the connection to the AT&T secondary Border Element.

Step 2 - On the **General** tab:

- Enter the IP address of the AT&T Secondary Border Element (e.g., **10.10.10.12**).

Server Type	Trunk Server	
IP Address / FQDN	Port	Transport
10.10.10.12	5960	UDP

Step 3 - On the **Heartbeat** tab:

- Check **Enable Heartbeat**.
- **Method**: **OPTIONS**.
- **Frequency**: As desired (e.g., **60** seconds).
- **From URI**: **secondary@customer.com**
- **To URI**: **secondary@customer.com**

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	secondary@customer.com
To URI	secondary@customer.com

Step 4 – Configure the **Advanced** tab as shown in **Section 7.2.5**, and click on **Finish** (not shown).

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	CS1K_maxtime_Remote_Address
Connection Type	SUBID

Step 5 – Select the Sever Configuration for the primary AT&T Border Element (**ATT_SC**) created in **Section 7.2.5**, and populate the **Heartbeat** tab as follows:

- Check **Enable Heartbeat**.
- **Method: OPTIONS**
- **Frequency:** As desired (e.g., **60** seconds).
- **From URI: primary@customera.com**
- **To URI: primary@customera.com**

Step 6 – Click on **Finish** (not shown).

13.2 Add Secondary Border Element IP Address to Routing

Repeat the steps in **Section 7.2.7**, using the parameters shown below, to add a Routing Profile for the AT&T secondary Border Element.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT_SC	10.10.10.11:5060 (UDP)	None
2	ATT_Secondary_SC	10.10.10.12:5060 (UDP)	None

13.3 Configure Secondary AT&T Border Element End Point Flow

Repeat the steps in **Section 7.4.5**, using the parameters shown below, to add an Endpoint Flow for the AT&T secondary Border Element.

Subscriber Flows
Server Flows

Server Configuration: ATT_Primary_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP	View Clone Edit Delete

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	SM_RP	View Clone Edit Delete

Server Configuration: SM_Trunk_SC

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default-low_PG	ATT_RP	View Clone Edit

©2015 Avaya Inc. All Rights Reserved.

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

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