



## Avaya Solution & Interoperability Test Lab

---

# **Application Notes for Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2 with AT&T IP Flexible Reach - Enhanced Features – Issue 1.0**

## **Abstract**

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and the Avaya Session Border Controller for Enterprise 6.2, with the AT&T IP Flexible Reach - Enhanced Features 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 1000E 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 6.2 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service, and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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

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

## Table of Contents

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing .....	5
2.2.	Test Results.....	6
2.2.1	Known Limitations .....	6
2.3.	Support.....	8
3.	Reference Configuration.....	8
3.1.	Illustrative Configuration Information.....	11
3.2.	Call Flows .....	12
3.2.1	Inbound .....	12
3.2.2	Outbound.....	13
3.2.3	Call Forward Re-direction .....	14
3.2.4	Coverage to Voicemail .....	15
4.	Equipment and Software Validated .....	16
5.	Configure Avaya CS1000E.....	17
5.1.	Logging In and Selecting the System Element.....	17
5.2.	Administer Telephony Node.....	18
5.2.1	Node Information and IP Addresses .....	18
5.2.2	Enable Terminal Proxy Server.....	20
5.2.3	Synchronize Configuration .....	21
5.3.	Voice Codecs .....	22
5.3.1	IP Telephony Node Codec Configuration.....	22
5.3.2	Media Gateway Codec Configuration .....	24
5.4.	Zones and Bandwidth Management.....	26
5.4.1	Zone 5 – SIP Trunk.....	26
5.4.2	Zone 3 – IP Telephones .....	27
5.5.	SIP Trunk Gateway.....	28
5.5.1	Provision SIP Gateway .....	28
5.5.2	Integrated Services Digital Network (ISDN).....	30
5.5.3	Virtual D-Channel Configuration .....	31
5.5.4	SIP Routes Configuration .....	32
5.5.5	SIP Trunk Configuration.....	34
5.5.6	Administer Virtual Super-Loop .....	37
5.6.	Routing of Outbound Dialed Numbers to Session Manager .....	37
5.6.1	Route List Block .....	38
5.6.2	Digit Manipulation Block .....	40
5.6.3	NARS Access Code .....	41
5.6.4	Numbering Plan Area Codes .....	42
5.6.5	Other Special Numbers to Route to Session Manager.....	43
5.7.	Routing of Inbound Numbers to Avaya CS1000E .....	44
5.8.	Enabling Plug-Ins for Call Transfer Scenarios .....	45
5.9.	Customer Information.....	46
5.9.1	Calling Number Provisioning for calls to the AT&T IP Flexible Reach Service.....	46
5.10.	Avaya CS1000E Stations.....	49

5.10.1	Example IP UNISlim Phone DN 4094, .....	49
5.10.2	Analog Fax Line .....	52
5.11.	Changing RFC2833 DTMF Telephone Event Type .....	53
5.12.	Ad Hoc Privacy Dialing.....	53
5.13.	Configuration Backup.....	54
6.	Configure Avaya Aura® Session Manager Release 6.3 .....	55
6.1.	SIP Domain.....	56
6.2.	Locations.....	56
6.2.1	Location for Avaya CS1000E.....	56
6.2.2	Location for the Avaya Session Border Controller for Enterprise .....	58
6.3.	Configure Adaptations.....	58
6.3.1	Adaptation for the Avaya CS1000E .....	58
6.3.2	Adaptation for from the Avaya CS1000E to the Avaya SBCE Entity .....	60
6.4.	SIP Entities.....	61
6.4.1	SIP Entity for Avaya CS1000E.....	61
6.4.2	SIP Entity for the Avaya SBCE.....	62
6.5.	Entity Links.....	63
6.5.1	Entity Link to Avaya CS1000E Entity.....	63
6.5.2	Entity Link to the Avaya SBCE.....	63
6.6.	Routing Policies .....	64
6.6.1	Routing Policy to the Avaya CS1000E.....	64
6.6.2	Routing Policy to the Avaya SBCE.....	65
6.7.	Dial Patterns.....	66
6.7.1	Inbound AT&T calls to Avaya CS1000E Users .....	66
6.7.2	Outbound Calls to AT&T .....	67
7.	Configure Avaya Session Border Controller for Enterprise .....	69
7.1.	Initial Installation/Provisioning .....	69
7.2.	Log into the Avaya SBCE.....	69
7.3.	Global Profiles .....	70
7.3.1	Server Interworking – Avaya Side.....	70
7.3.2	Server Interworking – AT&T Side .....	71
7.3.3	Routing – Avaya Side .....	71
7.3.4	Routing – AT&T Side.....	71
7.3.5	Server Configuration – To Session Manager.....	72
7.3.6	Server Configuration – To AT&T Primary Border Element .....	73
7.3.7	Topology Hiding – Avaya Side .....	74
7.3.8	Topology Hiding – AT&T Side.....	75
7.3.9	Signaling Manipulation.....	75
7.4.	Domain Policies .....	77
7.4.1	Application Rules.....	77
7.4.2	Media Rules .....	78
7.4.3	Signaling Rules .....	78
7.4.4	Endpoint Policy Groups – Avaya .....	81
7.4.5	Endpoint Policy Groups – AT&T .....	82
7.5.	Device Specific Settings .....	82
7.5.1	Network Management.....	82
7.5.2	Media Interface .....	83
7.5.3	Signaling Interface.....	83

7.5.4	Endpoint Flows – To Avaya (Session Manager) .....	84
7.5.5	Endpoint Flows – To AT&T Primary .....	84
8.	AT&T IP Flexible Reach Service .....	85
8.1.	AT&T Provisioning .....	85
9.	Verification Steps.....	86
9.1.	Avaya CS1000E Verifications.....	86
9.1.1	IP Network Maintenance and Reports Commands.....	86
9.1.2	System Maintenance Commands.....	87
9.2.	SIP Protocol Traces.....	89
9.3.	System Manager / Session Manager Verification.....	91
9.3.1	Verify Service State and Entity Link Status .....	91
9.3.2	Call Routing Test.....	92
9.4.	Avaya Aura® Session Border Controller Verification .....	93
9.4.1	Verify Sipera SBCE Connectivity to AT&T IP Flexible Reach.....	93
9.4.2	Internal Tracing.....	93
10.	Conclusion .....	95
11.	References.....	95
11.1.	Avaya .....	95
11.2.	AT&T IP Flexible Reach service.....	95
12.	Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements .....	96
12.1.1	Configure the Secondary Border Element Server Configuration .....	96
12.1.2	Add Secondary Border Element IP Address to Routing.....	97
12.1.3	Configure Secondary AT&T Border Element End Point Flow .....	98

# 1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.6 (Avaya CS1000E), Avaya Aura® Session Manager Release 6.3 (Session Manager), and the Avaya Session Border Controller for Enterprise 6.2 (Avaya SBCE), with the AT&T IP Flexible Reach - Enhanced Features SIP trunk service for PSTN access (IPFR-EF).

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 1000E 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 6.2 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service, and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T Flexible Reach is one of the many SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features which are not part of IP Flexible Reach service. The AT&T IP Flexible Reach - Enhanced Features service utilizes AVPN<sup>1</sup> or MIS/PNT<sup>2</sup> transport services.

**Note** – The AT&T IP Flexible Reach - Enhanced Features service will be referred to as IPFR-EF in the remainder of this document.

## 2. General Test Approach and Test Results

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 3.2** for examples) between the Avaya CS1000E, Avaya SBCE, and the IPFR-EF service. The Avaya CS1000E users make calls to and from the PSTN via the IPFR-EF service.

### 2.1. Interoperability Compliance Testing

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

- SIP trunking of inbound and outbound calls.
  - Incoming calls from the PSTN were routed to the DID numbers assigned by the AT&T IP Flexible Reach service to the Avaya CS1000E location. These incoming PSTN calls arrived via the SIP trunk and were answered by Avaya IP UNiStim telephones (desk phones and soft phones) and fax machine emulation software (Ventafax). Proper call disconnect was verified.
  - Outgoing calls from the Avaya CS1000E location to the PSTN were routed via the SIP trunk to the IPFR-EF service. These outgoing PSTN calls were originated from Avaya IP 1140E UniStim and SIP telephones, as well as fax machine emulation software (Ventafax). Proper call disconnect was verified.

---

<sup>1</sup> AVPN supports compressed RTP (cRTP).

<sup>2</sup> MIS/PNT does not support cRTP.

- Use of G.729A and G.711mu-law codecs were verified.
- Inbound and outbound T.38 and G.711 Fax were verified. The sender and receiver of a fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3. Fax speeds up to 14400 bps are supported in the configuration tested. In addition, Fax Error Correction Mode (ECM) is supported in the reference configuration.
- Avaya CS1000E stations call coverage to Avaya Call Pilot® for message generation and retrieval (including Message Wait Indicator).
- Passing of DTMF events (RFC2833) and DTMF recognition by navigating automated menus (e.g., Avaya Call Pilot® message selection and retrieval).
- PBX features such as hold, resume, conference and transfer.
- Requests for privacy (i.e., caller anonymity) for Avaya CS1000E outbound calls to the PSTN, and for inbound calls from the PSTN to Avaya CS1000E, were verified.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both the AT&T IP Flexible Reach service and Avaya SBCE were able to monitor health using SIP OPTIONS.
- Inbound calls to Avaya CS1000E station that were call forwarded back to PSTN destinations, through use of Diversion Header, were verified.
- Proper UDP port ranges for RTP media (16384-32767) were verified.

## 2.2. Test Results

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

### 2.2.1 Known Limitations

1. **CS1000E Unattended Call Transfers** - To allow the Avaya CS1000E user to transfer a call from PSTN user A to PSTN user B, before user B has answered the call (unattended transfer), Avaya CS1000E plug-in 501 must be enabled as shown in **Section 5.8**. However, while plug-in 501 will allow the Avaya CS1000E user to complete the transfer operation, user A will not hear ring back tone while user B is ringing. PSTN users A and B will have two-way talk path once user B answers. This is known CS1000E behavior.
2. **History Info and Diversion Headers** - The AT&T IP Flexible Reach service does not support SIP History-Info headers. However, the AT&T IP Flexible Reach service requires that SIP Diversion Header be sent for certain redirected calls (e.g., Call Forward). Session Manager will convert the History Info header into the Diversion Header by the use of the adaptation “*DiversionTypeAdapter*” for these types of calls (see **Section 6.3.2**). For all other calls, the Avaya SBCE will strip off History-Info headers (see **Section 7.4.3**).
3. **Maxptime:30 and Ptime:10** – For inbound calls, the AT&T IPFR-EF service sends Invites with the SIP parameter *maxptime:30*. In response, the Avaya CS1000E will send *ptime:10* for any UNISTim or digital stations. This is known CS1000E 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 AT&T IPFR-EF *maxptime:30* parameter, to *ptime:30*, thereby making Avaya CS1000E respond with *ptime:30* as required (see **Section 7.3.9**).

4. **Removal of SIP Headers** – Depending on the call flow and the endpoints involved, the Avaya CS1000E and Session Manager may send multiple SIP headers that are not used by AT&T. In addition, it has been found that large packets (e.g., > 1800 bytes) may cause the IPFR-EF network to return a 408 Request Timeout. Therefore in the interest of reducing packet overhead, and avoid possible related issues, the following headers are removed:
  - a. MIME type headers are removed by Session Manager Adaptations (see **Section 6.3.2**).
  - b. The Avaya SBCE removes the following SIP headers (see **Section 7.4.3**):
    - i. Alert-Info, x-nt-e164-clid, History-Info, Remote-Party-ID, Resource-Priority, AV-Global-Session-ID, P-AV-Message-ID, and P-Location.
5. **Telephone Events 101 and 111** - The Avaya CS1000E uses Telephone Event type 101 by default. This value is changed to the AT&T recommended value of 100 in the Avaya CS1000E (see **Section 5.11**). In addition, Telephone event type 111 is also sent by the Avaya CS1000E. This value is removed by the Avaya SBCE (see **Section 7.3.9**). Note that the 1140E SIP telephones use a value of 101 for their RFC2833 Telephone Event Type, however no issues were found when 101 was used.
6. **AT&T IP Flexible Reach Enhanced Features are currently not supported in the current Avaya CS1000E configuration** – During testing, two issues were found related to support of the AT&T IP Flexible Reach Enhanced Features.
  - a. **Network based “Blind Transfer” (Call Redirection using PBX generated REFER)** – The Avaya CS1000E does not support Refer.
  - b. **Simultaneous Ring and Sequential Ring** – If the “secondary” number is answered, a ReInvite/491 sequence results, and the network does not resend its ReInvite. Subsequently, the network sends a BYE terminating the “secondary” call.
    - i. This issue is under investigation by AT&T.
    - ii. **Note** - A workaround is to disable the “Answer Confirmation” option for Simultaneous Ring and Sequential Ring features via the A&T IP Flexible Reach Premium Online Web Portal.
  - c. **Network based Call Forward scenarios cannot be signaled by the Avaya CS1000E stations to enable/disable Call Forward options** – The Call Forward features, (Network based Call Forwarding Ring No Answer (CF-RNA), Network based Call Forwarding Busy (CF-Busy), Network based Call Forwarding Not Reachable (CF-NR), are enabled/disabled by sending a dialed string beginning with \* (asterisk), in the R-URI of the Invite sent to AT&T. The Avaya CS1000E does not have the capability to send \* as part of the dialed string.
    - i. **Note** – Customers may manually enable/disable these Enhanced features by logging into the A&T IP Flexible Reach Premium Online Web Portal, and modifying the appropriate feature.
7. **The Avaya CS1000E does not populate the PAI header correctly for inbound calls.** In the reference configuration , the IPFR-EF service sends a seven digit DNIS number in the R-URI. If this seven digit number is entered in the Avaya CS1000E Incoming Digit Translation (IDT) table (see **Section 5.7**), the Avaya CS1000E will populate subsequent PAI headers with the associated destination extension, instead of the desired DNIS digits.

- a. The workaround is to have Session Manager modify the R-URI to a ten digit number prior to sending the call to the Avaya CS1000E (see **Section 6.3.1**). As a result, the PAI is populated with the associated IPFR-EF DNIS number.
  - b. An Avaya CS1000E MR has been opened.
8. **Fax support** - G.711 and T.38 fax is supported, and the sender and receiver of a fax call may use either Group 3 or Super Group 3 fax machines. However the T.38 fax protocol carries all fax transmissions as Group 3. Fax speeds of 14400, with Error Correction Mode, were observed in the reference configuration.
9. **Emergency 911/E911 Services Limitations and Restrictions** - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor. While AT&T IP Flexible Reach services support 911/E911 calling capabilities under certain Calling Plans, there are circumstances when that 911/E911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at <http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

## 2.3. Support

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

<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

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



- IBM 306M Consumer **Off the Shelf** (COTS) servers, COTS1 and COTS2.
  - Signaling Server and SIP Gateway (COTS1).
  - SIPLINE and UCM (COTS2).

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

- Avaya “desk” phones are represented with Avaya 1140E UNISTim IP, 1140E SIP, and Digital M3904 telephones.
- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP to communicate with the Avaya CS1000E.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Avaya SBCE provides address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network. TCP transport protocol is used between Avaya SBCE and Session Manager. UDP transport protocol is used between Avaya SBCE and the AT&T IP Flexible Reach service.
- An existing Avaya Call Pilot® system provides the corporate voice messaging capabilities in the reference configuration. **Note** - The provisioning of Avaya Call Pilot® is beyond the scope of this document (see [5] for more information).

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

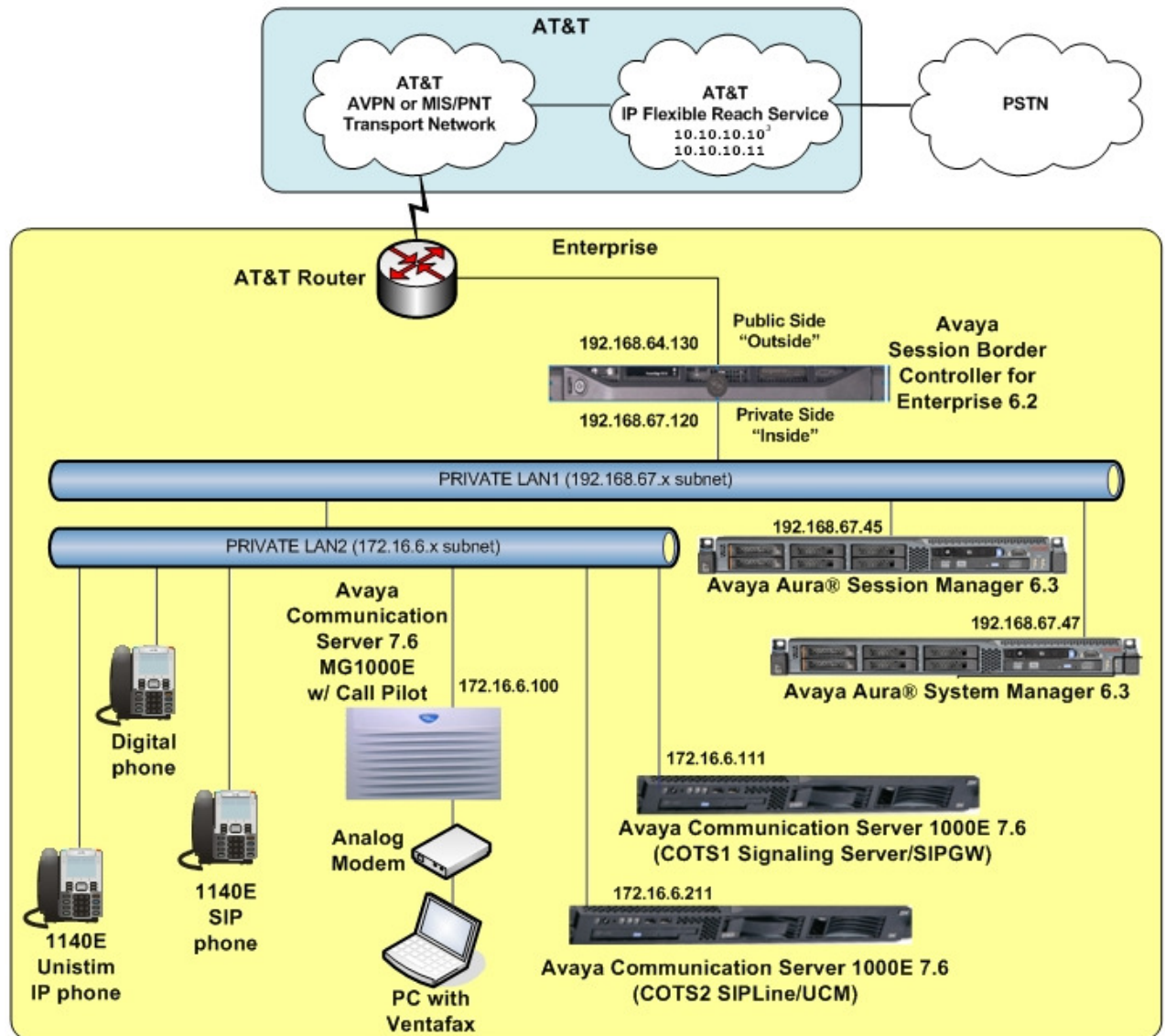


Figure 1: Avaya Interoperability Reference Configuration

<sup>3</sup> See the note in **Section 3.1** regarding these IP addresses.

### 3.1. Illustrative Configuration Information

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

**Note** – The IPFR-EF 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 IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
<b>Avaya CS1000E</b>	
COTS1 SIP Signaling Server IP Address (TLAN)	172.16.6.110
COTS2 SIP Line IP Address (TLAN)	172.16.6.210
MGC Media (DSP) IP Address (TLAN)	172.16.6.115
Avaya CS1000E extensions	40xx
<b>Avaya Call Pilot®</b>	
Call Pilot Application	172.16.6.12
Call Pilot Mailboxes	4xxx
<b>Avaya SBCE</b>	
IP Address of “Outside” (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service)	192.168.64.130
IP Address of “Inside” (Private) Interface (connected to Session Manager)	192.168.67.120
<b>AT&amp;T IP Flexible Reach Service</b>	
Border Element IP Addresses (Primary & Secondary)	10.10.10.10, 10.10.10.11*

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

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

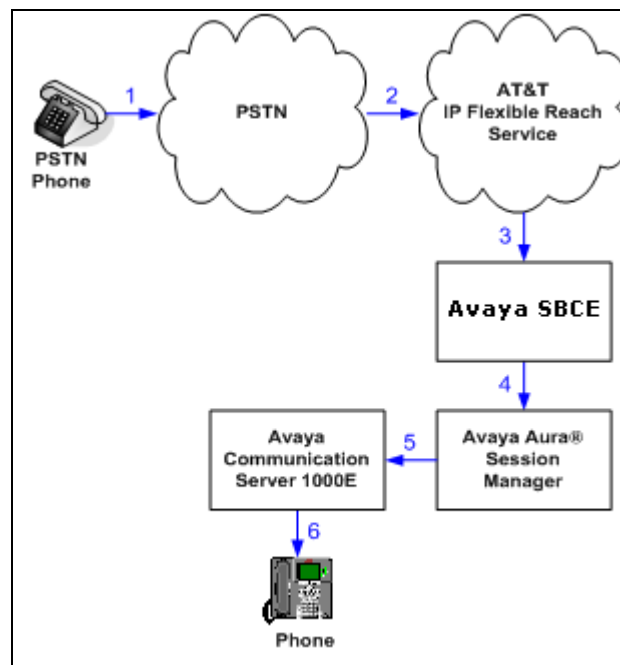
## 3.2. Call Flows

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

### 3.2.1 Inbound

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

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

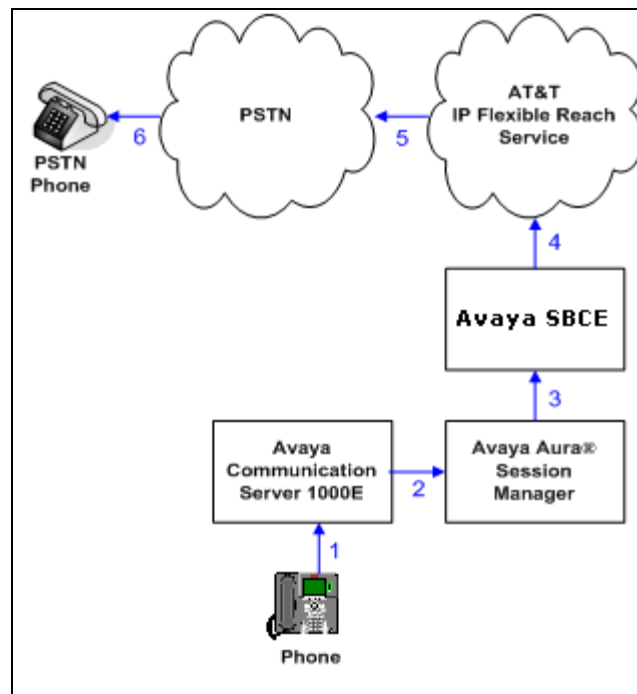


**Figure 2: Inbound AT&T IP Flexible Reach Call**

### 3.2.2 Outbound

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

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



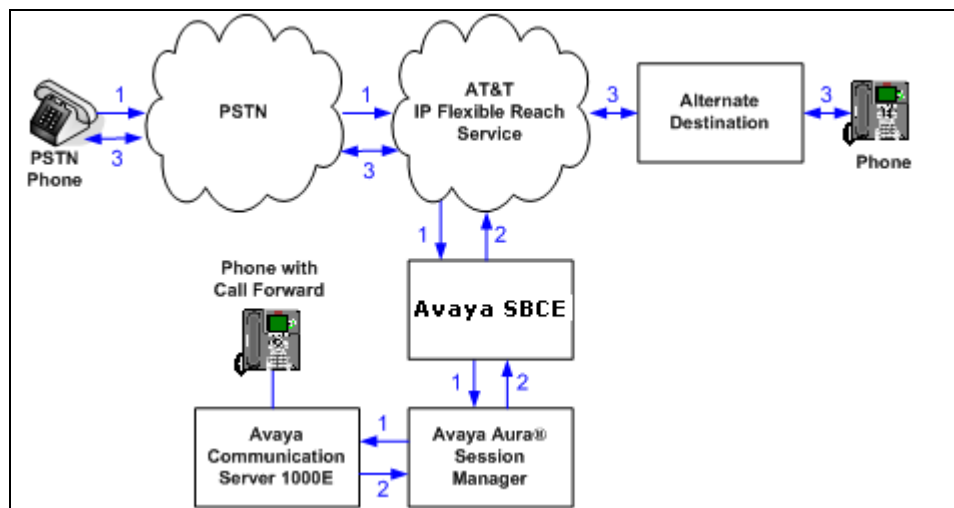
**Figure 3: Outbound AT&T IP Flexible Reach Call**

### 3.2.3 Call Forward Re-direction

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

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

1. Same as the first call scenario in **Section 3.2.1**.
2. Because the Avaya CS1000E phone has set Call Forward to another AT&T IP Flexible Reach service number, the Avaya CS1000E initiates a new call back out to Session Manager, Avaya SBCE, and to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service places a call to the alternate destination and upon answering; Avaya CS1000E connects the calling party to the target party.

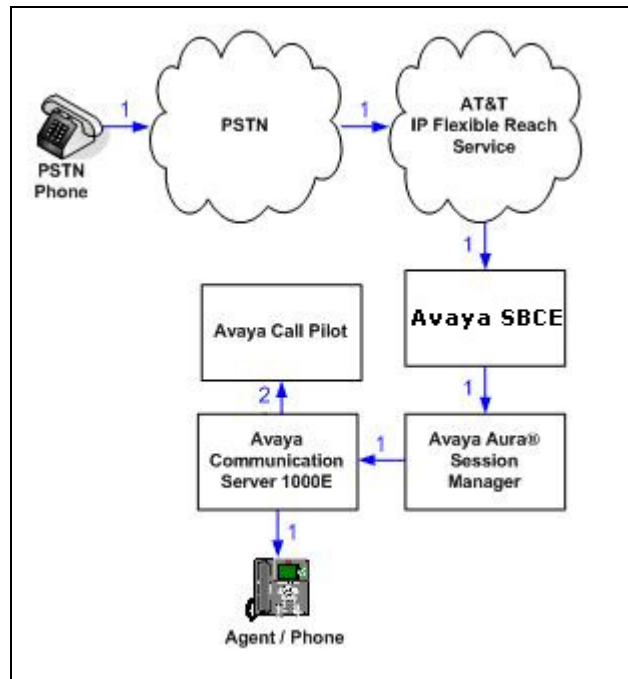


**Figure 4: Re-directed (e.g., Call Forward) AT&T IP Flexible Reach Call**

### 3.2.4 Coverage to Voicemail

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

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



**Figure 5: Coverage to Voicemail**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
HP Proliant DL360 G7 server <ul style="list-style-type: none"><li>System Platform</li><li>Avaya Aura® System Manager</li></ul>	<ul style="list-style-type: none"><li>6.3.0.0.18002</li><li>6.3.3.5 with SP3 (1719)</li></ul>
IBM 8800 server <ul style="list-style-type: none"><li>Avaya Aura® Session Manager</li></ul>	<ul style="list-style-type: none"><li>6.3 SP3 (6.3.3.3.0.633004)</li></ul>
Avaya CS1000E Platform <ul style="list-style-type: none"><li>MG1000E Media Gateway</li><li>IBM xSeries 306M (COTS) SIP Signaling server</li><li>Call Pilot</li></ul>	Version 4021, Release 765P+ <ul style="list-style-type: none"><li>Service_Pack CPM_7.6.2</li><li>Deplists_CPM_X21_07_65P.zip</li><li>Patch p30224_1.ntl</li><li>CP 5.00.41</li></ul>
Dell R310 <ul style="list-style-type: none"><li>Avaya Session Border Controller for Enterprise</li></ul>	<ul style="list-style-type: none"><li>6.2 Q48</li></ul>
Avaya 1140E Series IP Deskphones (UNISTim)	<ul style="list-style-type: none"><li>0625C8Q</li></ul>
Avaya 1140E Series IP Deskphones (SIP)	<ul style="list-style-type: none"><li>SIP1140e04.03.12.00.bin</li></ul>
Avaya M3904 Series Digital Deskphones	-
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none"><li>6.1.59.144</li></ul>

**Table 2: Equipment and Software Versions**



## 5. Configure Avaya CS1000E

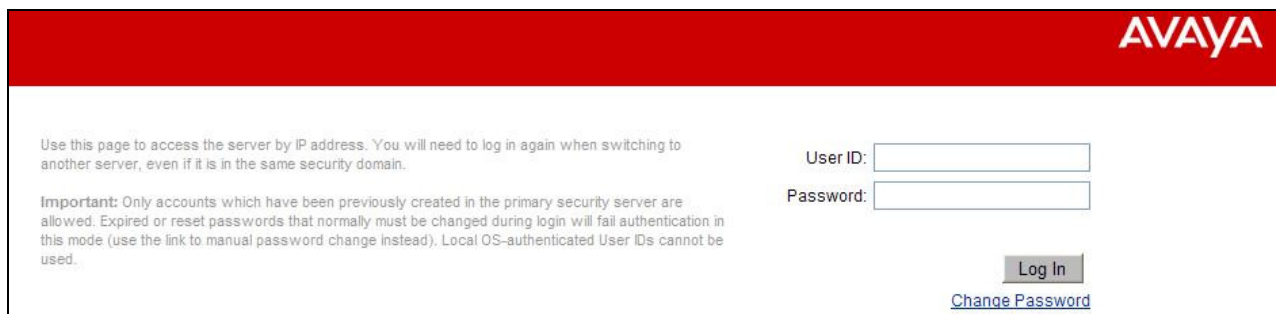
This section describes the Avaya CS1000E configuration, focusing on the routing of calls to Session Manager over a SIP trunk. In the sample configuration, Avaya CS1000E Release 7.6 was deployed with Call Server applications running on a CPPM server platform with MGC, and utilizing servers running separate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

Session Manager Release 6.3 provides all the SIP Proxy Service (SPS) and Network Connect Services (NCS) functions previously provided by the Network Routing Service (NRS). As a result, the NRS application is not required to configure a SIP trunk between Avaya CS1000E and Session Manager Release 6.3. Therefore NRS was not included in the reference configuration.

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

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

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

The screenshot shows the Avaya login interface. At the top is a red header with the 'AVAYA' logo in white. Below the header, on the left, is a block of text: 'Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.' followed by an 'Important' note about account creation and password changes. On the right side, there are two input fields labeled 'User ID:' and 'Password:'. Below these fields 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 Avaya CS1000E is registered as a member of the System Manager Security framework. The Element Manager then may be accessed via the System Manager **UCM Services** link.

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

The screenshot shows the Avaya Unified Communications Management interface. The left sidebar contains a navigation tree with categories like Network, CS 1000 Services, User Services, Security, and Tools. The main content area is titled 'Elements' and displays a table of registered elements. The table has columns for Element Name, Element Type, Release, Address, and Description. The first row, 'EM on cots1', is highlighted with a red box.

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

## 5.2. Administer Telephony Node

### 5.2.1 Node Information and IP Addresses

Expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**. The **IP Telephony Nodes** page is displayed as shown below. Click <Node id> in the **Node ID** column to view details of the node.

In the sample configuration, node **1001** is selected.

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

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

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 Avaya CS1000E in **Section 6.4.1**.

**AVAYA CS1000 Element Manager** Help | Logout

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

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

Node ID:  \* (0-9999)

Call server IP address:  \* TLAN address type: ☒ IPv4 only  
☐ IPv4 and IPv6

**Embedded LAN (ELAN)** **Telephony LAN (TLAN)**

Gateway IP address:  \* Node IPv4 address:  \*

Subnet mask:  \* Subnet mask:  \*

Node IPv6 address:

\* Required Value.

**Associated Signaling Servers & Cards**

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

**AVAYA CS1000 Element Manager** Help | Logout

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

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

Subnet mask:  \* 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](#)

\* Required Value.

**Associated Signaling Servers & Cards**

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and Customers. The main content area is titled 'CS1000 Element Manager' and includes a 'Help | Logo' link. Below the title bar, there are two 'Subnet mask' fields set to '255.255.255.0' and a 'Node IPv6 address' field. The 'IP Telephony Node Properties' section lists various services like Voice Gateway (VGW) and Codecs, Quality of Service (QoS), LAN, SNTP, Numbering Zones, and MCDN Alternative Routing Treatment (MALT) Causes. The 'Applications (click to edit configuration)' section lists SIP Line, Terminal Proxy Server (TPS), Gateway (SIPGW), Personal Directories (PD), Presence Publisher, and IP Media Services. The 'Associated Signaling Servers & Cards' section includes a table with columns for Hostname, Type, Deployed Applications, ELAN IP, TLAN IPv4, and Role. The table shows a single entry for 'cots1' with Type 'Signaling\_Server' and Role 'Leader'. Below the table, there is a 'Show: IPv6 address' checkbox and a note: '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 **UNISim Line Terminal Proxy Server** checkbox to enable proxy service on this node.

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

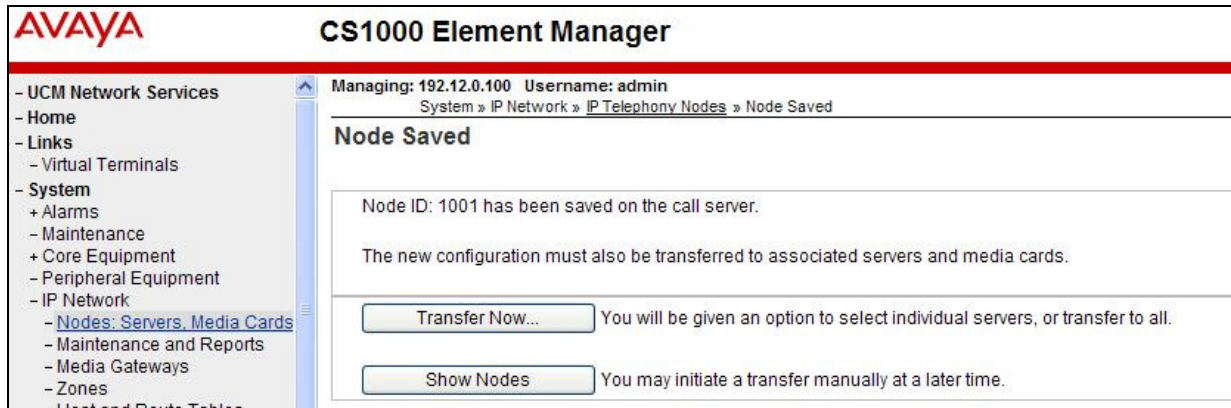
The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and Customers. The main content area is titled 'CS1000 Element Manager' and includes a 'Help | Logo' link. Below the title bar, there is a 'Managing: 192.12.0.100 Username: admin' section. The 'System > IP Network > IP Telephony Nodes > Node Details > UNISim Line Terminal Proxy Server (LTPS) Configuration' breadcrumb is shown. The 'Node ID: 1001 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details' section is active. The 'Firmware | DTLS | Network Connect Server' tabs are visible. The 'UNISim Line Terminal Proxy Server' checkbox is checked, and the 'Enable proxy service on this node' checkbox is also checked. The 'Firmware' section includes fields for IP address (0.0.0.0), Full file path (download/firmwa), Server Account/User ID, and Password. The 'DTLS' section includes a 'DTLS Session' dropdown set to 'Off'.

### 5.2.3 Synchronize Configuration

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

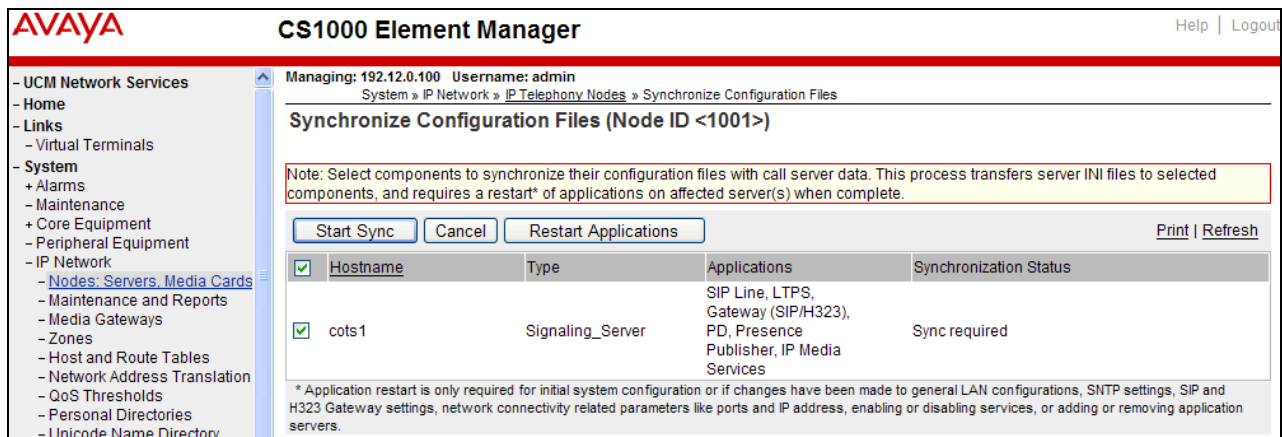
**Step 2** - Click **Save** on the **Node Details** screen (not shown).

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



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

**Step 4** - Select the appropriate Hostname (e.g., **cots1**) and click **Start Sync**.



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



AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin

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

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

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

Start Sync Cancel Restart Applications Print Refresh

Hostname	Type	Applications	Synchronization Status
<input type="checkbox"/> cots1	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	Synchronized

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

**Step 5** - After synchronization completes, click on the **Refresh** button in the right hand corner, Select the appropriate Hostname (e.g., cots1), and click **Restart Applications**.  
**NOTE** - When the applications restart, the phones will also reset.

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin

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

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

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

Start Sync Cancel Restart Applications Print Refresh

Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/> cots1	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	Synchronized

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

## 5.3. Voice Codecs

The following section describes how to set codec preferences as well as setting Packet Interval (PTIME) values. Note that the Avaya CS1000E always specifies G.711mu-law 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** (not shown).

The following screen shows the **General** parameters used in the sample configuration.

System  
+ Alarms  
- Maintenance  
+ Core Equipment  
- Peripheral Equipment  
- IP Network  
- Nodes, Servers, Media Cards  
- Maintenance and Reports  
- Media Gateways  
- Zones  
- Host and Route Tables  
- Network Address Translation  
- QoS Thresholds  
- Personal Directories  
- Unicode Name Directory  
+ Interfaces  
- Engineered Values  
+ Emergency Services  
+ Software

General | Voice Codecs | Fax

General

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

☒ Dynamic attenuation

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

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

Signaling options: ☒ DTMF tone detection  
☐ Low latency mode  
☒ Remove DTMF delay (squell DTMF from TDM to IP)  
☒ Modem/Fax pass-through  
☒ V.21 Fax tone detection  
☐ R factor calculation

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

Voice Codecs

Codec G.711: ☒ Enabled (required)

Voice payload size: 30 (milliseconds per frame)

Voice payout (jitter buffer) delay: 60 120 (milliseconds)  
 Nominal Maximum  
 Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

**Step 4** – Scroll down to the G.729 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 G.729: ☒ Enabled

Voice payload size: 30 (milliseconds per frame)

Voice payout (jitter buffer) delay: 60 120 (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**

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).

**AVAYA CS1000 Element Manager** Help | Log

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

**Media Gateways**

Buttons: Add... Digital Trunking... Reboot Delete Virtual Terminal More Actions

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

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

**Step 2** - Scroll down and click on **VGW and IP phone codec profile**.

Hostname DB1 \*

**- DSP Daughterboard 2**

Type of the DSP daughterboard NODB

Telephony LAN (TLAN) IP address 0.0.0.0

Telephony LAN (TLAN) gateway IP address 172.16.6.1

Telephony LAN (TLAN) IPv6 address

Telephony LAN (TLAN) subnet mask 255.255.255.0

Hostname DB2 \*

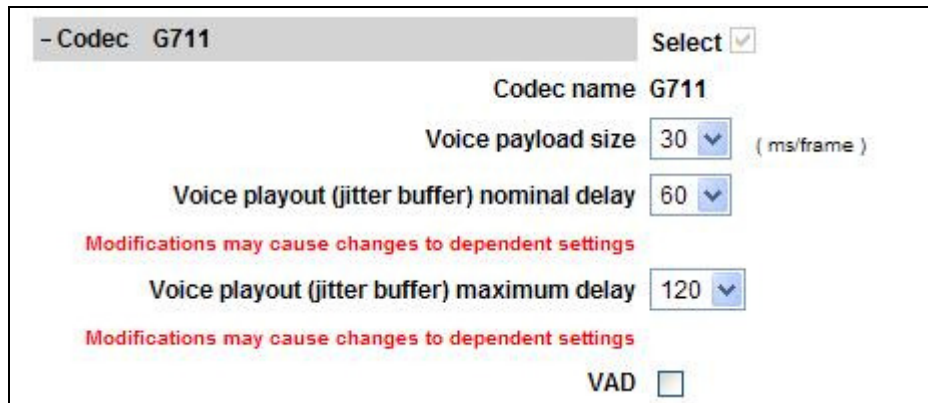
**+ VGW and IP phone codec profile**

+ QoS

+ Media Based CLID



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



- Codec G711 Select ☒

Codec name G711

Voice payload size 30 (ms/frame)

Voice playout (jitter buffer) nominal delay 60

Modifications may cause changes to dependent settings

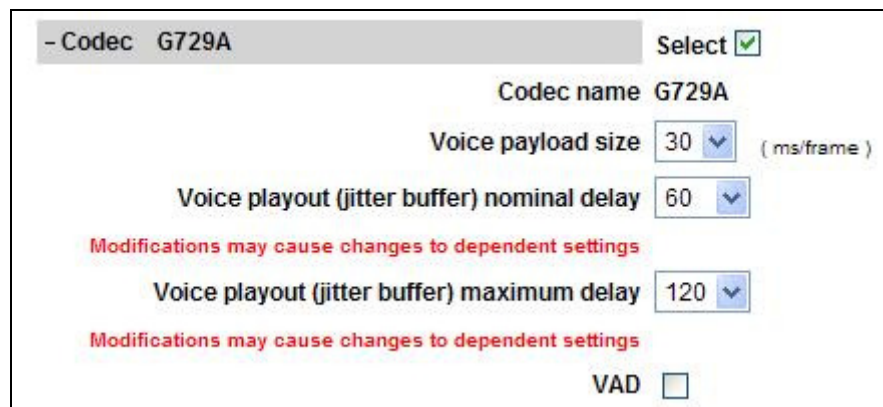
Voice playout (jitter buffer) maximum delay 120

Modifications may cause changes to dependent settings

VAD ☐

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

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



- Codec G729A Select ☒

Codec name G729A

Voice payload size 30 (ms/frame)

Voice playout (jitter buffer) nominal delay 60

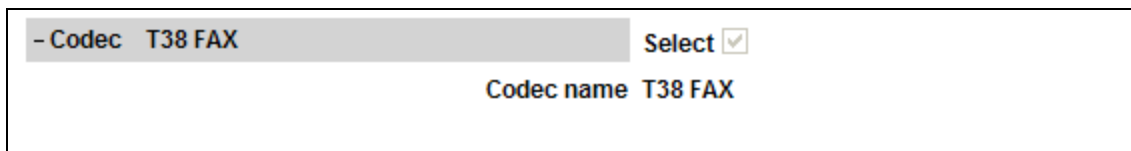
Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 120

Modifications may cause changes to dependent settings

VAD ☐

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

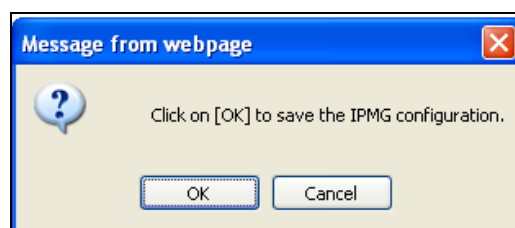


- Codec T38 FAX Select ☒

Codec name T38 FAX

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

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



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

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

### Media Gateways

Buttons: Add... Digital Trunking... **Reboot** Delete Virtual Terminal More Actions Refresh

	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

Buttons: Add... Edit... Import... Export Maintenance... Delete Refresh

	Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	3	10000	BQ	10000	BB	SHARED	MO	PHONES
2	5	100000	BQ	100000	BB	SHARED	VTRK	VTRK

**Step 2** – Select **Zone Basic Property and Bandwidth Management** for Zone 5.

## Edit Bandwidth Zone

Zone Basic Property and Bandwidth Management

Adaptive Network Bandwidth Management and CAC

Alternate Routing for Calls between IP Stations

Branch Office Dialing Plan and Access Codes

Branch Office Time Difference and Daylight Saving Time Property

Media Services Zone Properties

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

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
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="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.

The screenshot shows a web interface for managing SIP Gateway configurations. At the top, it displays the management IP (192.12.0.100) and username (admin). The breadcrumb trail is System » IP Network » IP Telephony Nodes » Node Details. The main title is 'Node Details (ID: 1001 - LTPS, Gateway ( SIPGw ))'. Below this, there are input fields for 'Gateway IP address' (192.12.0.1), 'Node IPv4 address' (172.16.0.110), 'Subnet mask' (255.255.255.0), and 'Node IPv6 address'. A section titled 'IP Telephony Node Properties' lists several links: Voice Gateway (VGW) and Codecs, Quality of Service (QoS), LAN, SNTP, Numbering Zones, and MCDN Alternative Routing Treatment (MALT) Causes. Another section titled 'Applications (click to edit configuration)' lists links: SIP Line, Terminal Proxy Server (TPS), Gateway (SIPGw) (which is highlighted with a red box), Personal Directories (PD), Presence Publisher, and IP Media Services. At the bottom, there is a legend for '\* Required Value.' and 'Save' and 'Cancel' buttons.

**Step 2** - On the **Node ID: 1001 - Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields.

- **SIP domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, “cots1.ntlab.com” was used in the reference configuration.
- **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: cots1.ntlab.com \*

Local SIP port: 5060 \* (1 - 65535)

Gateway endpoint name: SS\_1001 \*

Gateway password: \*

Application node ID: 1001 \* (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ☒ IPv4  
☐ IPv6

#### Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:  Add

Monitor addresses:

Remove

\* Required Value.

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

Save Cancel

### Step 3 - Scroll down to the section: **SIP Gateway Settings → Proxy or Redirect Server.**

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

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration, “192.168.67.47” was used.
- **Port:** Enter “5060”
- **Transport protocol:** Select “TCP”

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

### AVAYA CS1000 Element Manager

Help | Log

Managing: 192.12.0.100 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

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

General | SIP Gateway Settings | SIP Gateway Services

Port: 5060 (1 - 65535)

Transport protocol: TCP ▼

Shared Bandwidth Management:

☐ Enable Shared Bandwidth Management

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 192.168.67.47

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

Port: 5060 (1 - 65535)

Transport protocol: TCP ▼

Options: ☐ Support registration  
☐ Primary CDS proxy



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

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

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1001 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Number translation: Strip: Prefix: CLID display format:

Subscriber (SN): 0 <CCC><Area code><SN>

National (NN): 0 <CCC><NN>

International: 0 <International number>

SIP URI Map:

Public E.164 domain names

National: UDP:

Subscriber: CDP:

Special number: Special number:

Unknown: Vacant number:

Unknown:

SIP Gateway Services

SIP Converged Desktop: ☐ Enable CD service

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).

AVAYA CS1000 Element Manager

+ Core Equipment

+ Digital Private Network Signaling System 1 Package: 123

+ Flexible Tones and Cadences Package: 125

+ Multifrequency Compelled Signaling Package: 128

+ International Supplementary Features Package: 131

+ Enhanced Night Service Package: 133

- Integrated Services Digital Network Package: 145

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier: 0 (1 - 16383)

- Private network identifier: 1 (1 - 16383)

### 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. The left navigation pane is expanded to 'Routes and Trunks' > 'D-Channels'. The main content area is titled 'D-Channels' and includes a 'Maintenance' section with links to 'D-Channel Diagnostics (LD 96)', 'Network and Peripheral Equipment (LD 32, Virtual D-Channels)', 'MSDL Diagnostics (LD 96)', 'TMDI Diagnostics (LD 96)', and 'D-Channel Expansion Diagnostics (LD 48)'. Below this is a 'Configuration' section with a 'Choose a D-Channel Number' dropdown set to '0' and a 'Type' dropdown set to 'DCH', followed by a 'to Add' button. A table lists two channels:

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

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

The screenshot shows the 'Basic Configuration' section of the D-Channels 100 Property Configuration screen. It contains the following settings:

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:  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:

**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: ☒

**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.

**AVAYA CS1000 Element Manager**

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

**Routes and Trunks**

Customer: 0	Total routes: 9	Total trunks: 60	<input type="button" value="Add route"/>	
+ Route: 15	Type: TIE	Description: H323	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 16	Type: TIE	Description: SIP	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 17	Type: TIE	Description: SIP VTRK TTY	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 18	Type: TIE	Description: SIPLINE	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 26	Type: DID	Description: MIRAN	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 27	Type: MUS	Description: MUSIC	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 28	Type: RAN	Description: RAN1	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>



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

**- Basic Configuration**

Route data block (RDB) (TYPE):

Customer number (CUST):

Route number (ROUT):

Designator field for trunk (DES):

Trunk type (TKTP):

Incoming and outgoing trunk (ICOG):

Access code for the trunk route (ACOD):

Trunk type M911P (M911P): ☐

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

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

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

- Protocol ID for the route (PCID):

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

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

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE):

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

- Interface type for route (IFC):

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

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- Trunk route optimization (TRO): ☐

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

- Channel type (CHTY):

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

- Insert ESN access code (INAC): ☐

- Integrated service access route (ISAR): ☐

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

- Mobile extension route (MBXR): ☐

- Mobile extension outgoing type (MBXOT):

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

Calling number dialing plan (CNDP):

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

**- Basic Route Options**

Attendant announcement (ATAN):

Billing number required (BILN): ☐

Call detail recording (CDR): ☐

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

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

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

- Display external dialed digits (DEXT): ☐

Multifrequency compelled or MFC signaling (MFC):

Process notification networked calls (PNNC): ☐

## 5.5.5 SIP Trunk Configuration

**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.

AVAYA CS1000 Element Manager

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

**Routes and Trunks**

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

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

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

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

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

**- Basic Configuration**

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:  \*

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

**Step 4** – Going back to the screen shown in **Step 1**, select the **Edit** button next to **Route 16** to verify the configuration, as shown below. Verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.2**. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging.

**AVAYA** **CS1000 Element Manager**

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

### Customer 0, Route 16 Property Configuration

**- Basic Configuration**

Route data block (RDB) (TYPE): 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 (ISLD) ▼

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

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

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

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- Trunk route optimization (TRO): ☐

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

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

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

- Insert ESN access code (INAC): ☐

- Integrated service access route (ISAR): ☐

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

- Mobile extension route (MBXR): ☐

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

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

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

**Step 6** - Scrolling down, open **Basic Route Options** and verify that the DCNO number specified (e.g., 1), matches the **Digit Conversion Tree Number** specified in **Section 5.7, Step 3**.

**- Basic Route Options**

Attendant announcement (ATAN) :

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

North American toll scheme (NATL) : ☒

Controls or timers (CNTL) : ☐

Conventional (Tie trunk only) (CNVT) : ☐

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

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

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

- Display external dialed digits (DEXT) : ☐

MFC feature options (MFC\_FEAT) : ☐

**+ Network Options**

**+ General Options**

**+ Advanced Configurations**

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

### 5.5.6 Administer Virtual Super-Loop

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

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 192.12.0.100 Username: admin  
System » Core Equipment » Superloops

**Superloops**

Refresh

Superloop Number	Superloop Type
1 <input type="radio"/> 0	IPMG
2 <input type="radio"/> 96	Virtual

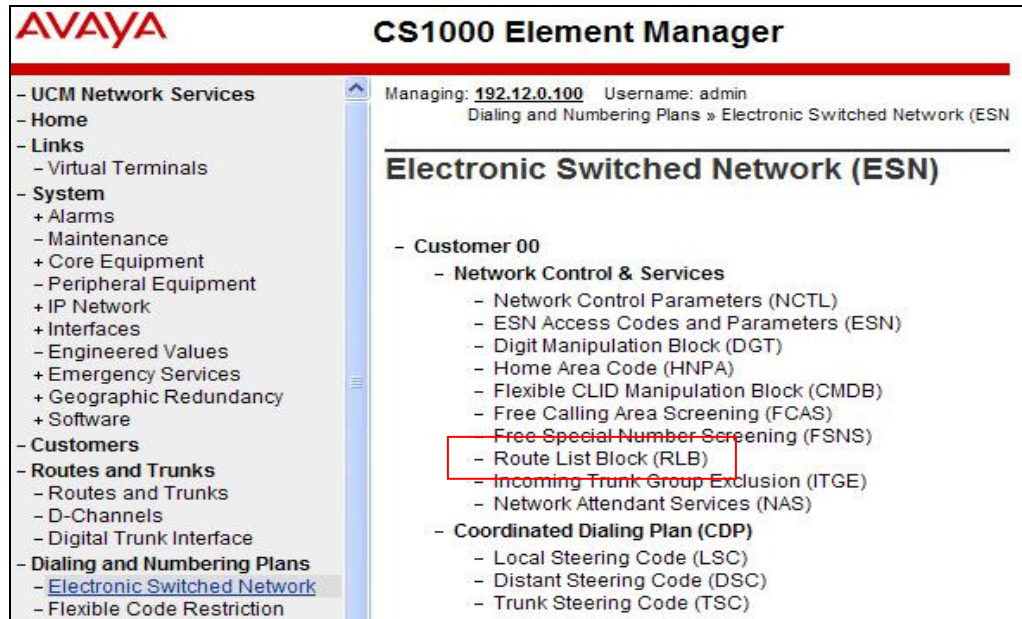
## 5.6. Routing of Outbound Dialed Numbers to Session Manager

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

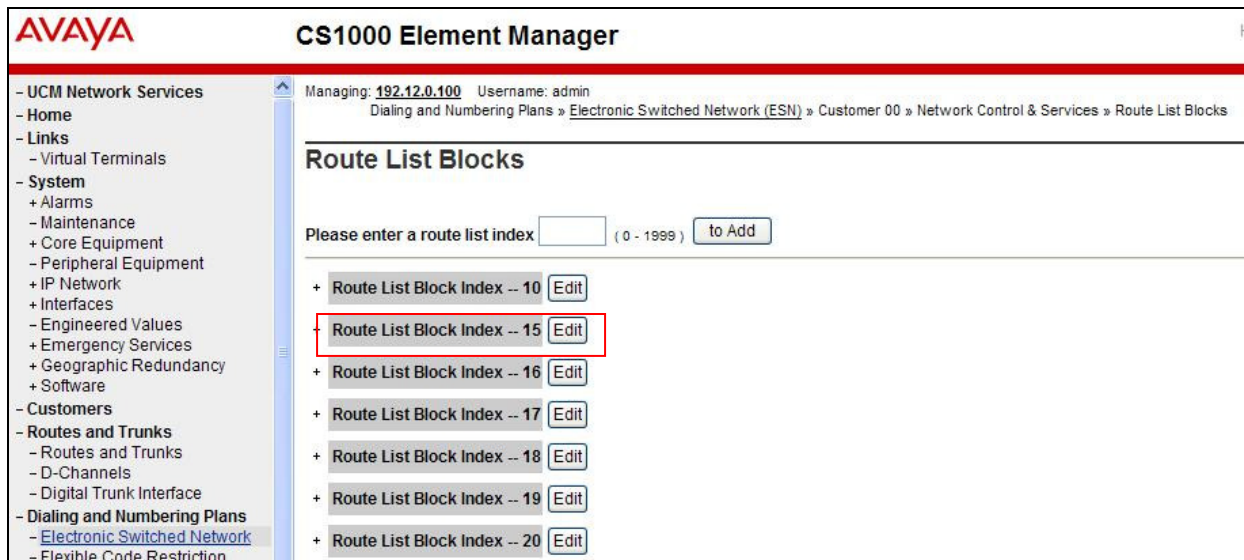


## 5.6.1 Route List Block

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



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



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

**AVAYA** CS1000 Element Manager

Managing: 192.12.0.100 Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Configuration Block

**Route List Block**

**General Properties**

Number of Alternate Routing Attempts: 5 (1 - 10)  
Initial Set: 1 (0 - 64)  
Set Minimum Facility Restriction Level: 1  
Overlap Length: 0 (0 - 24)  
Extended Local Calls: ☐  
Route List Index: 15

Please choose the Data Entry Index 2 to Add

+ Data Entry Index -- 0 Edit  
+ Data Entry Index -- 1 Edit

**Step 4** – Verify that the **Digit Manipulation Index** is set to **15** (see Section 5.6.2).

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

**General Properties**

Entry Number for the Route List: 0

**Indexes**

Time of Day Schedule: 0  
Facility Restriction Level: 0 (0 - 7)  
Digit Manipulation Index: 15  
ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)  
Free Calling Area Screening Index: 0  
Free Special Number Screening Index: 0  
Business Network Extension Route: ☐  
Incoming CLID Table: 0 (0 - 0)

**Options**

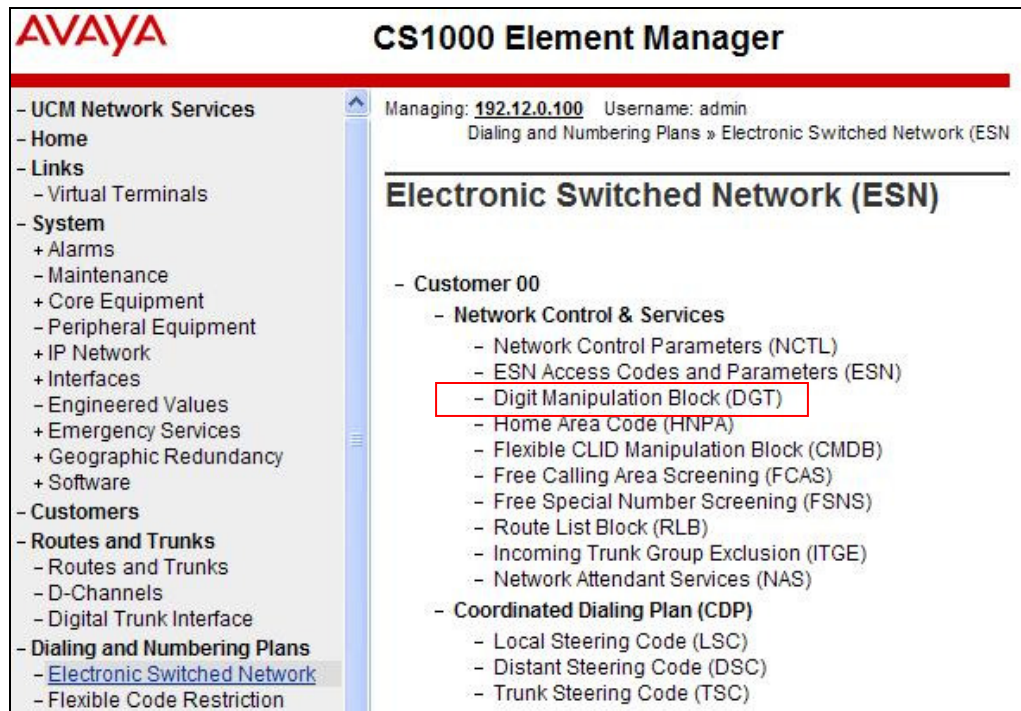
Local Termination entry: ☐  
Route Number: 16  
Skip Conventional Signaling: ☐  
Use Tone Detector: ☐  
Conversion to LDN: ☐

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

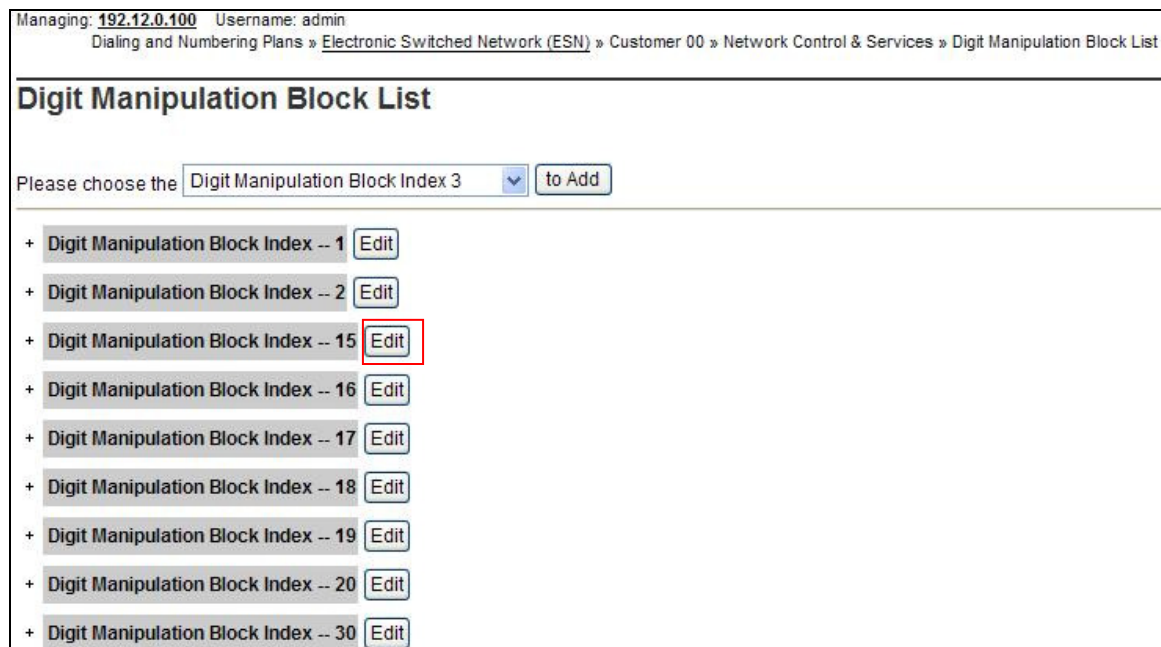
## 5.6.2 Digit Manipulation Block

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

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



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





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

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

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

**Step 4** – Click on **Submit**.

### 5.6.3 NARS Access Code

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

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

**Step 2** - Select **ESN Access Codes and Parameters (ESN)**. Although not shown below, this option can be seen on the screenshot shown in **Section 5.6.2, Step 1**.

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

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

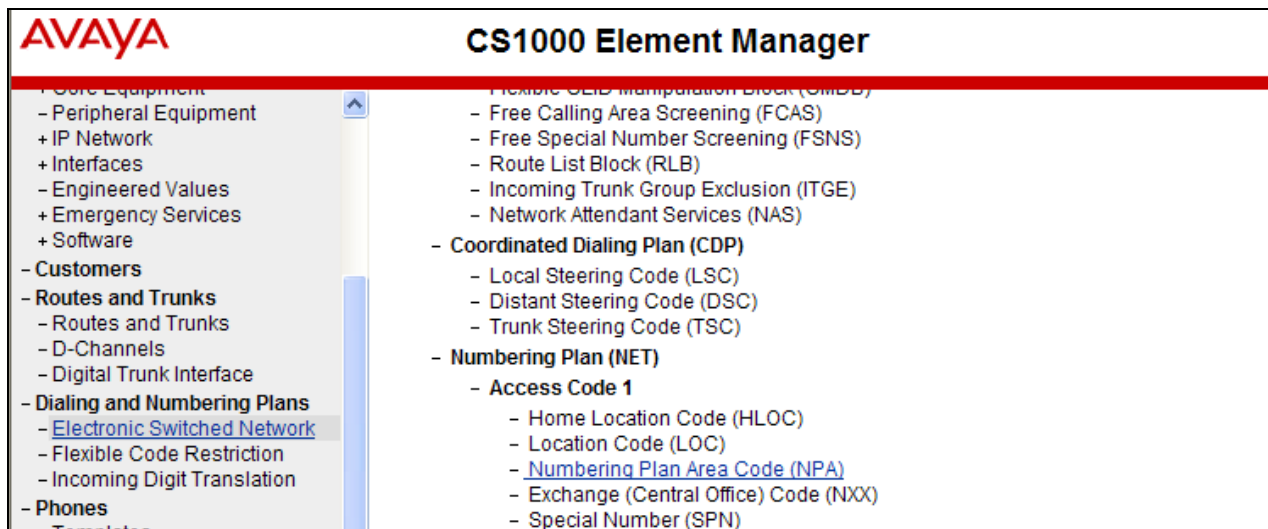
The screenshot shows a web form titled "ESN Access Codes and Basic Parameters". It contains the following fields and controls:

- "NARS/BARS Access Code 1:" with a text input field containing the value "9", which is highlighted with a red rectangular box.
- "NARS Access Code 2:" with an empty text input field.
- "NARS/BARS Dial Tone after dialing AC1 or AC2 access codes:" with a checked checkbox.
- "Expensive Route Warning Tone:" with a checked checkbox.
- "- Expensive Route Delay Time:" with a text input field containing "6" and a range indicator "( 0 - 10 )".
- "Coordinated Dialing Plan feature for this customer:" with a checked checkbox.
- "- Maximum number of Steering Codes:" with a text input field containing "10" and a range indicator "( 1 - 64000 )".
- "- Number of digits in CDP DN (DSC + DN or LSC + DN):" with a text input field containing "4" and a range indicator "( 3 - 10 )".
- "Routing Controls:" with an unchecked checkbox.
- "Check for Trunk Group Access Restrictions:" with a checked checkbox.

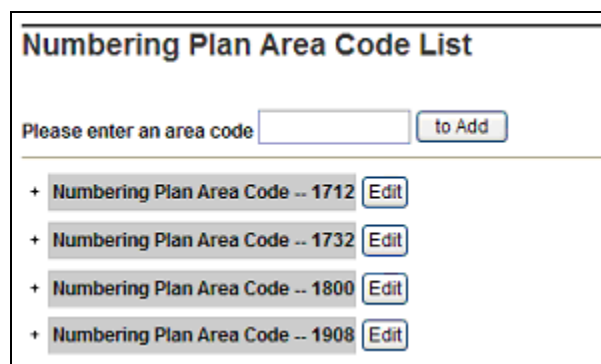
## 5.6.4 Numbering Plan Area Codes

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

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



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



**Step 3** - In the screen below, the entry for “1732” is displayed. In the **Route List Index** field, “15” is selected to use the route list associated with the SIP trunk to Session Manager (as defined in **Section 5.6.1, Step 2**). Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP trunk to Session Manager.

## Numbering Plan Area Code

### General Properties

Numbering Plan Area code translation: 1732

Route List Index: 15

Incoming Trunk group Exclusion Index:

### 5.6.5 Other Special Numbers to Route to Session Manager

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

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

**Step 2** - Scroll down and select **Special Number (SPN)** under the appropriate **Access Code** heading (e.g., **1** as shown in **Section 5.6.3, Step 3**).

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

## CS1000 Element Manager

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

### Special Number List

Please enter a Special Number

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

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

## Special Number (011)

### General Properties

Route list index: 15

Incoming trunk group exclusion index:

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

## 5.7. Routing of Inbound Numbers to Avaya CS1000E

Calls from PSTN will dial AT&T IP Flexible Reach DNIS numbers to reach stations on Avaya CS1000E. These DNIS numbers are converted to the associated extensions by the Avaya CS1000E 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 IPFR-EF dialed DID number.

**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**.

+ Geographic Redundancy  
+ Software  
**Customers**  
Routes and Trunks  
- Routes and Trunks  
- D-Channels  
- Digital Trunk Interface  
**Dialing and Numbering Plans**  
- Electronic Switched Network  
- Flexible Code Restriction  
- Incoming Digit Translation

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

### Incoming Digit Translation

- Customer: 00

Edit IDC

**Step 3** – From the listed Digit Conversion Trees, select either **New DCNO** or edit **DCNO**. In the reference configuration, **Digit Conversion Tree Number: 1** was selected. Note that the Digit Conversion Tree Number selected must also be defined in the trunk provisioning shown in **Section 5.5.5**.

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

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

### Customer 00 Incoming Digit Conversion Property

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

Refresh
Cancel

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

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

**Digit Conversion Tree 1 Configuration**

Regular IDC tree  
Send calling party DID disabled

	Incoming Digits *	Converted Digits	CPND Name	CPND language
33	<a href="#">7325553166</a>	4095		
34	<a href="#">7325553167</a>	4095		
35	<a href="#">7325553168</a>	4099		
36	<a href="#">7325553169</a>	4009		
37	<a href="#">7325553170</a>	2810		
38	<a href="#">7325553179</a>	4096		
39	<a href="#">7325553180</a>	2090		

**Note** – Due to an issue found during testing, the Incoming Digits field must be populated with 10 digits. See **Section 2.2.1, Item 7**, and **Section 6.3.1**.

**Note** – This method should not be used to redirect DIDs for PSTN access to the Call Pilot access extension. The procedures described in **Section 6.3.1, Step 3** cover this scenario.

## 5.8. Enabling Plug-Ins for Call Transfer Scenarios

Plug-ins allow specific Avaya CS1000E software feature behaviors to be changed. In the testing associated with these Application Notes, plug-in 501 is required for successful completion of Unattended Transfer calls (see **Section 2.2.1, Item 1**).

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

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

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



**AVAYA CS1000 Element Manager** Help

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - IP Network
    - Nodes: Servers, Media Cards
    - Maintenance and Reports
    - Media Gateways
    - Zones
    - Host and Route Tables
    - Network Address Translation
    - QoS Thresholds
    - Personal Directories
    - Unicode Name Directory
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - Software
    - Call Server PEPs
    - Loadware PEPs

An internal error has occurred! Severity:Major

[Enable](#) [Disable](#) [Print](#)

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

## 5.9. Customer Information

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

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

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

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

**AVAYA CS1000 Element Manager**

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - Software
  - **Customers**

Managing: 192.12.0.100 Username: admin

Customers

[Add...](#) [Delete](#)

Customer Number	Total Routes	Total Trunks
1 <input type="radio"/> 00	10	36

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

Customer Details

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

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

General Properties

Flexible trunk to trunk connection option:

Connections restricted

Flexible orbiting prevention timer:

14

Country code:

(0 - 9999)

Code for processing the called number

National access code:

International access code:

Options:

☐ Transfer on ringing of supervised external trunks  
☒ Connection of supervised external trunks

Network option:

☐ Coordinated dialing plan routing  
☒ Integrated services digital network

Microsoft converged office dialing plan:

Private dialing plan

Private dialing plan for non-DID users:

☐ Coordinated dialing plan  
☐ Uniform dialing plan

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

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

Integrated services digital network: ☒

Microsoft converged office dialing plan: Private dialing plan

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

**Calling Line Identification**

Information for incoming/outgoing calls: No manipulation is done

Size:  (0 - 4000)

Country code:  (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

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

**AVAYA CS1000 Element Manager**

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

**Calling Line Identification Entries**

**Search for CLID**

Start range :   
 End range :   
 \*End range\* should not exceed the CLID size specified

**Calling Line Identification Entries**

This will display all defined Call Ids. For example, CLID 0 will use the number 7325554097.

**Calling Line Identification Entries**

**Search for CLID**

Start range :   
 End range :   
 \*End range\* should not exceed the CLID size specified :

**Calling Line Identification Entries**

	<input type="checkbox"/> Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1	<input type="checkbox"/> 0	732	5554097			NO	
2	<input type="checkbox"/> 1	732	5554098			NO	
3	<input type="checkbox"/> 2	732	5554383			NO	
4	<input type="checkbox"/> 3	732	5554384			NO	
5	<input type="checkbox"/> 4	732	5554385			NO	
6	<input type="checkbox"/> 5	732	5554386			NO	



Click on any Entry ID to view or change further details (e.g., **Entry ID 5** is shown below). Note that the **Use DN as DID** is set to **NO**. This means that the local extension will not be used for the calling number.

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

### Edit Calling Line Identification 5

**General Properties**

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

Local Code: 5554386 (1-12 digits)  
Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID: NO

**Emergency Services Access**

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

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

**Calling Party Name Display**

Roman characters: ☒

CPND Name: Groucho Marx  
first name, last name

Expected Length: 24

Display Format: First name, Last name

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

## 5.10. Avaya CS1000E Stations

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

### 5.10.1 Example IP UNISTim Phone DN 4094,

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

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

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

**Step 3** – Click on the TN value (e.g., **096 0 01 03**). The **Phone Details** form will open. Note that the telephone type is an 1140 and that it is defined in Zone 3. A call between this telephone and another telephone in Zone 3 will use a “best quality” strategy (see **Section 5.4.2**) and therefore can use G.711mu-law. If this same telephone calls out to the PSTN via the SIP trunk, the call would use a “best bandwidth” strategy, and the call would use G.729A.


AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
    - Engineered Values
    - + Emergency Services
    - + Geographic Redundancy
    - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools

Phone Details



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

General Properties | Features | Keys | User Fields

Custom View: All

General Properties

Customer Number: 0 \*

Terminal Number: 096 0 01 03

Designation: NUL \* (1-6 characters)

Zone: 3 \*

Key Expansion Modules: 0

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

### 5.10.1.1 Features

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

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

#### 5.10.1.1.1 Setting Privacy

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

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

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

**NOTE** – The methods described above define a fixed value on station and cannot be manipulated by the end user. For ad hoc privacy, a dialing code such as \*67 should be used. See **Section 5.12**.

#### 5.10.1.1.2 Call coverage to Call Pilot

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

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

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

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

### 5.10.1.2 Keys

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

#### 5.10.1.2.1 Key 0 - Single Call Appearance

This key defines the first call appearance on the telephone.

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

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

### 5.10.1.2.2 Key 2 – Message Waiting Indicator

This defines the MWI lamp.

2	MIK - Message Waiting Indication
---	----------------------------------

### 5.10.1.2.3 Key 16 - Message Waiting

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

16	MWK - Message Waiting	Message Center DN: 2080 <input type="checkbox"/> Multiple Appearance Redirection Prime(MARP)
----	-----------------------	---


### 5.10.1.2.4 Key 19 - Forward All Calls

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

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

## 5.10.2 Analog Fax Line

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

Phone Details	
 System: EM on cots1 Phone Type: 2500 Sync Status: TRN	
General Properties   Features   Single Line Features   User Fields    Custom View: All	
<b>General Properties</b>	
Customer Number: 0 * Terminal Number: 000 1 10 00 Designation: ANALOG * (1-6 characters) Directory Number: 2779 * CLID entry:	

## 5.11. Changing RFC2833 DTMF Telephone Event Type

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

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

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

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

```
Password:
```

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

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

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

```
pdt> setRFC2833PT 100
```

The system will respond with the pdt> prompt.

```
pdt>
```

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

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

## 5.12. Ad Hoc Privacy Dialing

In the United States, central offices support ad hoc privacy by dialing \*67 followed by the called number. This dialing method can be implemented in the Avaya CS1000E as well.

**Step 1** – From the left hand UCM menu, select **Customers → Customer 00 → Flexible Feature Codes** (not shown).

**Step 2** – At the bottom of the **Flexible Feature Codes** page click on **Flexible Feature Code Entries** (not shown).

**Step 3** – Click on **Add** (not shown).

**Step 4** – In the **Flexible Feature Code type** field, enter **CPP** (Call Party Privacy), and in the **Value** field enter **\*67**.

### Add Flexible Feature Code

Flexible feature code type:
• [Lookup](#)

Value:
•

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

## 5.13. 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.

- Incoming Digit Translation
- **Phones**
- Templates
- Reports
- Views
- Lists
- Properties
- Migration
- **Tools**
- Backup and Restore
- [Call Server](#)

### Call Server Backup

**Action**

▼

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

```

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

```

The configuration of Avaya CS1000E is complete.

## 6. Configure Avaya Aura® Session Manager Release 6.3

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

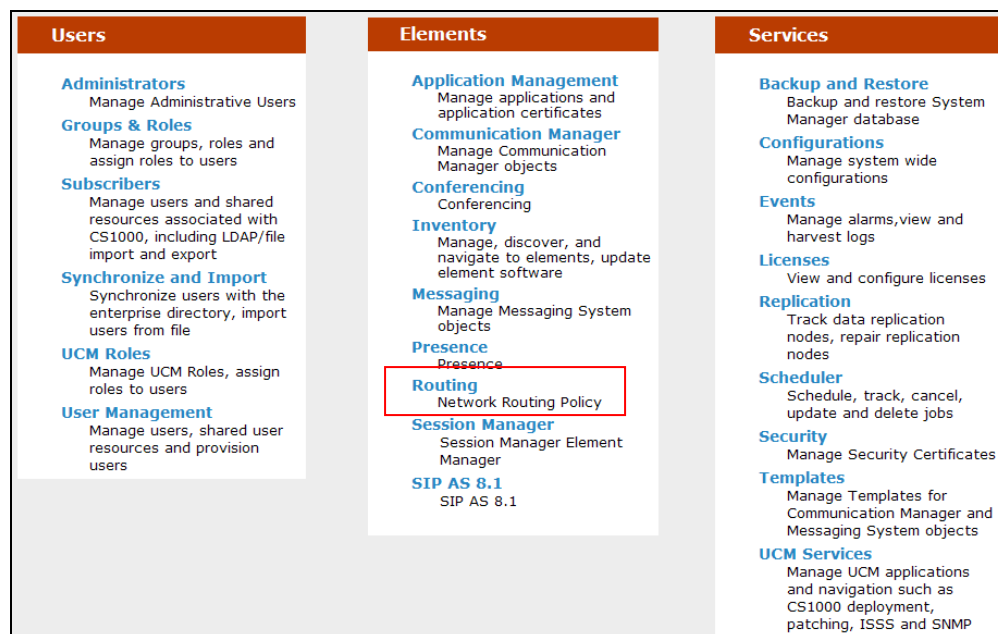
**Note** – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information, consult the references in **Section 11**.

The following administration activities will be described:

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

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

In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, a Release 6.3 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.





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

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

## 6.1. SIP Domain

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

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

Avaya Aura® System Manager 6.3

Last Logged on: September 13, 2013 11:14 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log adm](#)

Routing \* Home

Home / Elements / Routing / Domains

Domain Management

[New](#) [Edit](#) [Delete](#) [Duplicate](#) [More Actions](#)

[Refresh](#) [Filter: Enable](#)

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

Select : All, None

**Step 3** - Click **Commit** to save. Multiple SIP Domains may be defined if required.

## 6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g., 192.168.67.x for all devices on a particular subnet), or individual devices (e.g., 192.168.67.10 for a device's IP address). In the reference configuration the Avaya CS1000E is defined in one Location (172.16.6.x). The Avaya SBCE and Session manager were each defined in a second Location (192.168.67.x).

### 6.2.1 Location for Avaya CS1000E

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

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

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

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

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

<ul style="list-style-type: none"> <li>Locations</li> <li>Adaptations</li> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> </ul>	<div style="text-align: right;">Commit Cancel</div> <h3>Location Details</h3> <h4>General</h4> <p><b>* Name:</b> <input type="text" value="CS1K"/></p> <p><b>Notes:</b> <input type="text"/></p> <h4>Dial Plan Transparency in Survivable Mode</h4> <p><b>Enabled:</b> <input type="checkbox"/></p> <p><b>Listed Directory Number:</b> <input type="text"/></p> <p><b>Associated CM SIP Entity:</b> <input type="text"/></p> <h4>Overall Managed Bandwidth</h4> <p><b>Managed Bandwidth Units:</b> <input type="text" value="Kbit/sec"/></p> <p><b>Total Bandwidth:</b> <input type="text"/></p> <p><b>Multimedia Bandwidth:</b> <input type="text"/></p> <p><b>Audio Calls Can Take Multimedia Bandwidth:</b> <input checked="" type="checkbox"/></p> <h4>Per-Call Bandwidth Parameters</h4> <p><b>Maximum Multimedia Bandwidth (Intra-Location):</b> <input type="text" value="1000"/> Kbit/Sec</p> <p><b>Maximum Multimedia Bandwidth (Inter-Location):</b> <input type="text" value="1000"/> Kbit/Sec</p> <p><b>* Minimum Multimedia Bandwidth:</b> <input type="text" value="64"/> Kbit/Sec</p> <p><b>* Default Audio Bandwidth:</b> <input type="text" value="80"/> Kbit/sec</p> <h4>Alarm Threshold</h4> <p><b>Overall Alarm Threshold:</b> <input type="text" value="80"/> %</p> <p><b>Multimedia Alarm Threshold:</b> <input type="text" value="80"/> %</p> <p><b>* Latency before Overall Alarm Trigger:</b> <input type="text" value="5"/> Minutes</p> <p><b>* Latency before Multimedia Alarm Trigger:</b> <input type="text" value="5"/> Minutes</p> <h4>Location Pattern</h4> <p><input type="button" value="Add"/> <input type="button" value="Remove"/></p> <p>1 Item <input type="button" value="Refresh"/></p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>IP Address Pattern</th> <th>Notes</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>* 172.16.6.*</td> <td></td> </tr> </tbody> </table> <p>Select : All, None</p> <div style="text-align: right;">Commit Cancel</div>	<input type="checkbox"/>	IP Address Pattern	Notes	<input type="checkbox"/>	* 172.16.6.*	
<input type="checkbox"/>	IP Address Pattern	Notes					
<input type="checkbox"/>	* 172.16.6.*						

## 6.2.2 Location for the Avaya Session Border Controller for Enterprise

Repeat **Steps 1-3** in **Section 6.2.1** to create a location called **SBC** for the Avaya SBCE using address **192.168.67.\***.

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

## 6.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module designed for Avaya CS1000E to convert SIP headers in messages sent by Avaya Communication Server to the format used by other Avaya products and endpoints. In the reference configuration the following adaptations was used.

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

In addition, Module parameters **odstd** (to modify destination domain or IP addressing), **osrcd** (to modify source domain or IP addressing, **MIME=no** (to remove unnecessary Avaya CS1000E SIP headers), and **fromto=true** (to modify the From and To headers) are specified.

### 6.3.1 Adaptation for the Avaya CS1000E

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

- **Adaptation Name:** Enter an identifier for the Adaptation Module.
- **Module Name:** Select “**CS1000Adapter**” from drop-down menu (or add an adapter with name “CS1000Adapter” if not previously defined)
- **Module Parameter:** Enter **fromto=true** (Note – this parameter is set so that destination user information is copied from the R-URI into the To header for inbound calls to Call Pilot).

**General**

\* **Adaptation name:** CS1K

**Module name:** CS1000Adapter

**Module parameter:** fromto=true

**Egress URI Parameters:**

**Notes:**

**Step 2** – In the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from AT&T to the Avaya CS1000E. In some call scenarios the Avaya CS1000E may insert local extensions in the PAI and/or Contact headers of responses or ReInvites. In conjunction with the **fromto=true** Module Parameter specified in Step 1 above, Session Manager will replace the local extension with its corresponding IPFR-EF DNIS access number.

- **Matching Pattern** Enter an Avaya CS1000E extension (e.g., **2090**).
- **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 IPFR-EF access number associated with the extension (e.g., **7325553180**).
- Repeat for all extension/IPFR-EF number associations.

Digit Conversion for Incoming Calls to SM									
Add Remove									
5 Items Refresh		Filter: Enable							
<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 2090	* 4	* 4		* 4	7325553180	both		
<input type="checkbox"/>	* 4091	* 4	* 4		* 4	7325553166	both		
<input type="checkbox"/>	* 4093	* 4	* 4		* 4	7325553162	both		
<input type="checkbox"/>	* 4095	* 4	* 4		* 4	7325553166	both		
<input type="checkbox"/>	* 4096	* 4	* 4		* 4	7325553179	both		
Select : All, None									

**Step 3** - In the **Digit Conversion for Outgoing Calls from SM** section, click **Add** to configure entries for calls from AT&T to the Avaya CS1000E.

Note that incoming AT&T calls to Avaya CS1000E stations have the inbound DNIS digits converted to their associated local extensions in the Avaya CS1000E **Incoming Digit Translation** table (e.g., AT&T DNIS 7325553166 is converted to local extension 4095, see **Section 5.7**), so those digit conversions are not needed here.

In addition, for direct PSTN/AT&T access to the integrated Call Pilot messaging system, the DNIS number used to access Call Pilot (e.g., 7325553180) must be converted to the Call Pilot local access extension (2090). The **fromto=true** Module Parameter specified in Step 1 above, triggers this conversion.

- **Matching Pattern** Enter AT&T IP Flexible Reach DIDs (e.g., **7325553180**).
- **Min** Enter minimum number of digits (e.g., **10**)
- **Max** Enter maximum number of digits (e.g., **10**)
- **Phone Context** Leave blank.
- **Delete Digits** Enter “10”, to remove the AT&T DID digits.
- **Insert Digits** Enter the Call Pilot extension (e.g., **2090**).
- **Address to modify** Select “**both**”.

**Step 4** – Due to an issue found with the Avaya CS1000E Incoming Digit Translation table (see **Section 2.2.1, Item 7**), the seven digit DNIS number sent by the IPFR-EF service (e.g., 555-xxxx), must be converted to a ten digit number (e.g., 732-555-xxxx).

- **Matching Pattern** Enter part of the AT&T IP Flexible Reach DNIS number (e.g., **555**).
- **Min** Enter minimum number of digits (e.g., **7**)
- **Max** Enter maximum number of digits (e.g., **7**)
- **Phone Context** Leave blank.
- **Delete Digits** Enter **0**.
- **Insert Digits** Enter the Call Pilot extension (e.g., **2090**).
- **Address to modify** Select **destination**.

Digit Conversion for Outgoing Calls from SM									
Filter: Enable									
<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*7325553180	*10	*10		*10	2090	destination ▼		convert TO header for Call Pilot
<input type="checkbox"/>	*555	*7	*7		*0	732	destination ▼		PSTN to CS1K

Select : All, None

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

### 6.3.2 Adaptation for from the Avaya CS1000E to the Avaya SBCE Entity

The message body of an INVITE message sent from the Avaya CS1000E will contain a MIME Multipart message body containing the SDP information expected by AT&T, but also containing “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” application parts that are not processed by AT&T. Since AT&T has no use for this information, the Module Parameter **MIME=no** was used in the reference configuration to remove these headers. In addition, the **DiversionTypeAdapter** will convert History-Info headers to Diversion headers, which are required by the AT&T IP Flexible Reach service for Call Forward scenarios. Note that the Avaya SBCE is used to remove and/or alter additional Avaya CS1000E SIP headers (see **Section 7.4.3**).

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

- **Adaptation Name:** Enter an identifier for the Adaptation Module.

- **Module Name:** Select “**DiversionTypeAdapter**” from drop-down menu (or add an adapter with name “DiversionTypeAdapter” if not previously defined)
- **Module Parameter:** Enter the following three parameters separated by spaces.
  - Enter “**MIME=no**” to remove additional MIME Media Type headers that the Avaya CS1000E adds to its SIP signaling.

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

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

## 6.4. SIP Entities

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

### 6.4.1 SIP Entity for Avaya CS1000E

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

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

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

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

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

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

**SIP Entity Details** [Commit] [Cancel]

**General**

\* **Name:** CS1K

\* **FQDN or IP Address:** 172.16.6.110

**Type:** SIP Trunk

**Notes:**

**Adaptation:** CS1K

**Location:** CS1K

**Time Zone:** America/New\_York

**Override Port & Transport with DNS SRV:** ☐

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

**Credential name:**

**Call Detail Recording:** none

**SIP Link Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

## 6.4.2 SIP Entity for the Avaya SBCE

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

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

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

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

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



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

**SIP Entity Details** Commit

**General**

\* Name: SBCE\_and AT&T

\* FQDN or IP Address: 192.168.67.120

Type: Other

Notes:

Adaptation: CS1K\_to\_ATT\_via\_SBCE

Location: SBCE

Time Zone: America/New\_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

## 6.5. Entity Links

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

### 6.5.1 Entity Link to Avaya CS1000E Entity

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

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

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

**Entity Links** Commit Cancel

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* CS1K	* sm63	TCP	* 5060	* CS1K	* 5060	trusted

Select : All, None

### 6.5.2 Entity Link to the Avaya SBCE

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

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

Entity Links								Commit	Cancel
1 Item Refresh								Filter: Enable	
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy		
<input type="checkbox"/>	* A-SBCE	* sm63	TCP	* 5060	* A-SBCE	* 5060	trusted		
<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>									
Select : All, None									

## 6.6. Routing Policies

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

### 6.6.1 Routing Policy to the Avaya CS1000E

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

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

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

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

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

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

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

SIP Entities	<b>General</b>
Entity Links	* Name: <input type="text" value="CS1K"/>
Time Ranges	Disabled: <input type="checkbox"/>
Routing Policies	* Retries: <input type="text" value="0"/>
Dial Patterns	Notes: <input type="text"/>
Regular Expressions	<b>SIP Entity as Destination</b>
Defaults	<input type="button" value="Select"/>

Name	FQDN or IP Address	Type	Notes
CS1K	172.16.6.110	Other	

**Time of Day**

1 Item Refresh Filter: Enable

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

Select : All, None

## 6.6.2 Routing Policy to the Avaya SBCE

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

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

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

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

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

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

The following screen shows the Routing Policy for Avaya SBCE.

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

<ul style="list-style-type: none"> <li>SIP Entities</li> <li>Entity Links</li> <li>Time Ranges</li> <li>Routing Policies</li> <li>Dial Patterns</li> <li>Regular Expressions</li> <li>Defaults</li> </ul>	<h3>General</h3> <p>* Name: <input type="text" value="A-SBCE_to_ATT"/></p> <p>Disabled: <input type="checkbox"/></p> <p>* Retries: <input type="text" value="0"/></p> <p>Notes: <input type="text"/></p> <h3>SIP Entity as Destination</h3> <p><input type="button" value="Select"/></p> <table border="1"> <thead> <tr> <th>Name</th> <th>FQDN or IP Address</th> <th>Type</th> <th>Notes</th> </tr> </thead> <tbody> <tr> <td>A-SBCE</td> <td>192.168.67.120</td> <td>Other</td> <td></td> </tr> </tbody> </table> <h3>Time of Day</h3> <p> <input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="View Gaps/Overlaps"/> </p> <p>1 Item <input type="button" value="Refresh"/> Filter: <input type="button" value="Enable"/></p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Ranking ▲</th> <th>Name</th> <th>Mon</th> <th>Tue</th> <th>Wed</th> <th>Thu</th> <th>Fri</th> <th>Sat</th> <th>Sun</th> <th>Start Time</th> <th>End Time</th> <th>Notes</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>0</td> <td>24/7</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>00:00</td> <td>23:59</td> <td>Time Range 24/7</td> </tr> </tbody> </table> <p>Select : All, None</p>	Name	FQDN or IP Address	Type	Notes	A-SBCE	192.168.67.120	Other		<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes	<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7
Name	FQDN or IP Address	Type	Notes																																
A-SBCE	192.168.67.120	Other																																	
<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes																							
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7																							

## 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.

**Note** - In the reference configuration, the IPFR-EF service sent seven digits (e.g., 555-xxxx) in the R-URI. See **Sections 2.2.1, 5.7, and 6.3** for an issue/workaround regarding the use of seven digits.

### 6.7.1 Inbound AT&T calls to Avaya CS1000E Users

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

- **Pattern:** Enter dial pattern for calls to the Avaya CS1000E (e.g., **555xxxx**)
- **Min:** Enter the minimum number of digits (e.g., 7).
- **Max:** Enter the maximum number of digits (e.g., 7).
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

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

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

- In the **Originating Location** list, select the location defined for Avaya SBCE in **Section 6.2.2**.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya CS1000E in **Section 6.6.1**.

- Click **Select** to save these changes and return to **Dial Pattern Details** page.

**Step 4** - Click **Commit** to save. Repeat this procedure as needed for additional AT&T DNIS numbers.

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove Filter: Enable

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

Select : All, None

**Denied Originating Locations**

Add Remove 0 Items Refresh Filter: Enable

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

## 6.7.2 Outbound Calls to AT&T

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

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

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

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

- In the **Originating Location** list, select “**Apply the Selected Routing Policies to All Originating Locations**”. In the **Routing Policies** table, select the Routing Policy defined for Avaya SBCE in **Section 6.6.2**.

- Click **Select** to save these changes and return to **Dial Pattern Details** page.

**Step 4** - Click **Commit** to save. Repeat this procedure as needed for additional PSTN numbers to be routed to PSTN/AT&T network.

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

Dial Pattern Details

CommitCancel

General

\* Pattern: 1732

\* Min: 11

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

2 Items RefreshFilter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CS1K		A-SBCE_to_ATT	0	<input type="checkbox"/>	A-SBCE	

Select : All, None

Denied Originating Locations

AddRemove

0 Items RefreshFilter: Enable

<input type="checkbox"/>	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.

### 7.1. Initial Installation/Provisioning

**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.**

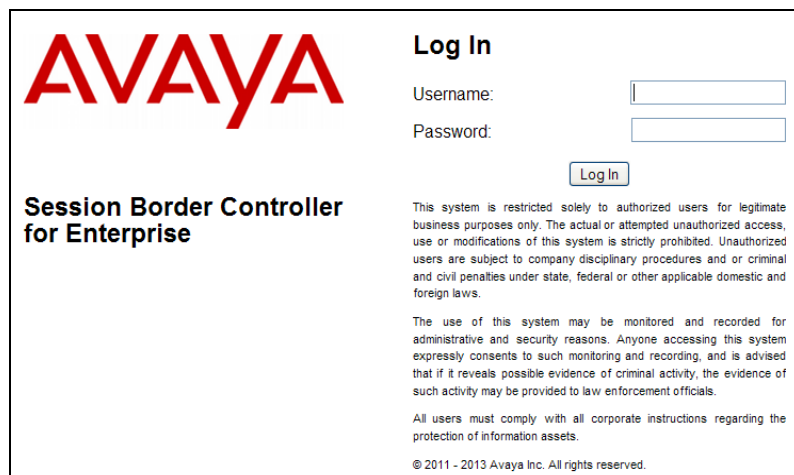
In the reference configuration, the Avaya SBCE interface B1 (192.168.64.130) was used for the public interface (toward AT&T), and interface A1 (192.168.67.120) was the private network interface.

### 7.2. Log into the Avaya SBCE

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

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

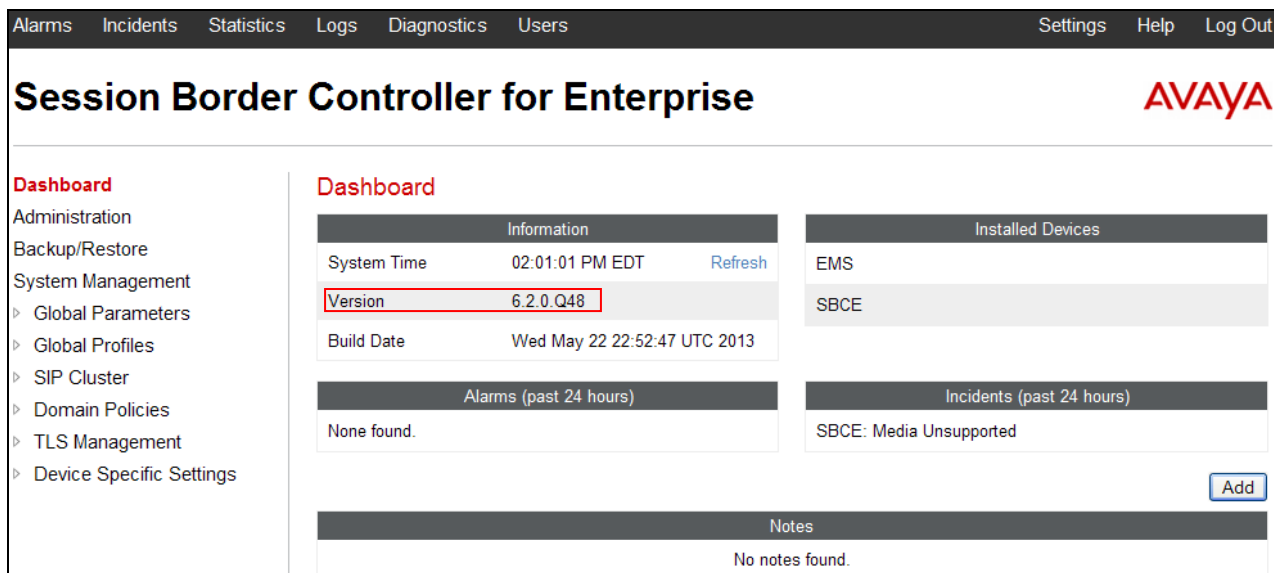
**Step 2** – Enter the appropriate credentials, and click on **Log In**.



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

Note the platform version is displayed in the center of the display (e.g., **6.2.0 Q48**).





## 7.3. Global Profiles

### 7.3.1 Server Interworking – Avaya Side

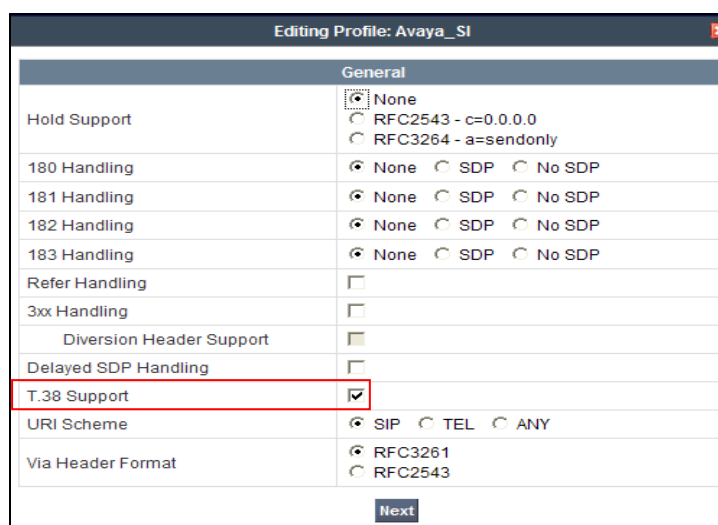
**Step 1** - Select **Global Profiles** → **Server Interworking** (not shown).

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

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

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

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



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

### 7.3.2 Server Interworking – AT&T Side

Repeat the steps shown in **Section 7.3.1** to add an Interworking Profile for the connection to AT&T.

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

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

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

### 7.3.3 Routing – Avaya Side

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

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

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

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

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

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

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

**Next Hop Routing**

URI Group: \*

Next Hop Server 1: 192.168.67.47

Next Hop Server 2:

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

Finish

### 7.3.4 Routing – AT&T Side

Repeat the steps in **Section 7.3.3** to add a Routing Profile for the AT&T primary Border Element.

**Note** – See **Appendix 1** for provisioning a route to the AT&T IPFR-EF service secondary Border Element, if applicable.

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

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

**Step 3** - Click **Next**, then enter the following:

- Set **Next Hop Server 1**: to **10.10.10.10** (AT&T Border Element IP address, see note in **Section 3.1** regarding this address).
- Select **Routing Priority Based on Next Hop Server**.
- Set **Outgoing Transport**: to **UDP**.

**Step 4** - Click **Finish**.

The screenshot shows the Avaya Session Manager configuration interface. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, and Routing. The main area is titled 'Routing Profiles: To\_ATT\_RP' and contains an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below this is a list of routing profiles: 'default', 'To\_ATT\_RP' (selected), and 'To\_SM\_RP'. The 'To\_ATT\_RP' profile is expanded, showing a table with columns: Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The table contains one row with Priority '1', URI Group '\*', Next Hop Server 1 '10.10.10.10', and Next Hop Server 2 empty. There are 'View' and 'Edit' links for this row. An 'Add' button is also present in the top right of the table area.

### 7.3.5 Server Configuration – To Session Manager

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

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

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

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

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

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

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

- Select **Enable Grooming**.
- For **Interworking Profile** select **Avaya\_SI** created in **Section 7.3.1**.
- For the **Signaling Manipulation Script** select the **CS1K\_headers** script defined in **Section 7.3.9**.
- Select **Finish**, accepting remaining default values.

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

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

### Server Configuration: SM\_SC

Add

Server Profiles

SM\_SC

General

Authentication

Heartbeat

Advanced

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

Edit

Rename
Clone
Delete

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

### Server Configuration: SM\_Trunk\_SC

Add

Server Profiles

SM\_SC

General

Authentication

Heartbeat

Advanced

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

Edit

Rename
Clone
Delete

### 7.3.6 Server Configuration – To AT&T Primary Border Element

**Note** – See **Appendix 1** for configuration of a Secondary AT&T IPFR-EF Border Element, if applicable.

Repeat the steps in **Section 7.3.5** to create a Server Configuration for the connection to the AT&T primary Border Element, using the following entries:

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

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

- Enter **IP Address: 10.10.10.10** (AT&T IP Flexible Reach primary border element. See the note in **Section 3.1** regarding this address).
- For **Supported Transports**: check **UDP**
- For **UDP Port**: enter **5060**
- Select **Next**

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

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

- Select **ATT\_SI** for **Interworking Profile** (created in **Section 7.3.2**).
- For the **Signaling Manipulation Script** select the **CS1K\_maxptime** script that was defined in **Section 7.3.9**.

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

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

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

Server Configuration: ATT\_Primary\_SC

Add

Server Profiles  
SM\_SC  
ATT\_Primary\_SC

General Authentication Heartbeat Advanced

Server Type Trunk Server

IP Addresses / FQDNs 10.10.10.10

Supported Transports UDP

UDP Port 5060

Edit

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

Server Configuration: ATT\_Secondary\_SC

Add

Server Profiles  
SM\_SC  
ATT\_Primary\_SC

General Authentication Heartbeat Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile ATT\_SI

Signaling Manipulation Script CS1K\_maxptime

UDP Connection Type SUBID

Edit

### 7.3.7 Topology Hiding – Avaya Side

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

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

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

- For the Header **To**,
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **cots1.ntlab.com**
- Repeat for the Header **From**
- Repeat for the Header **Request Line**

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

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

Topology Hiding Profiles: Avaya\_TH

Add

Topology Hiding Profiles  
default  
Avaya\_TH

Rename Clone Delete

Click here to add a description.

Topology Hiding

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

Edit

### 7.3.8 Topology Hiding – AT&T Side

Create a **Topology Hiding Profile** for the connection to AT&T, by repeating the steps in **Section 7.3.7** with the following changes:

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

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

### 7.3.9 Signaling Manipulation

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

**Note** – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 7.4.3**) does not meet the desired result. Refer to [11] for information on the Avaya SBCE scripting language.

**Step 1** - As described in **Section 2.2.1, Item 5**, the Avaya CS1000E inserts a telephone event type of 111 which AT&T does not support. This value is removed via the following script. In addition, in some call scenarios the Avaya CS1000E may insert a leading + in the calling/called number fields. This is also not required by AT&T, and is removed.

- Select **Global Profiles → Signaling Manipulation** from the menu on the left-hand side of the screen (not shown).
- Click **Add Script** (not shown) and the script editor window will open.
- Enter a name for the script in the **Title** box (e.g., **CS1K\_headers**). The script shown below defined.
- Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the Avaya Server Configuration in **Section 7.3.5, Step 6**.



Title CS1K\_headers Save

```
// Removes 111 telephone event.

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

    // Remove 111 from CS1K requests

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

  }
}

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

    // Remove 111 from CS1K responses

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

  }
}

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

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

**Step 2** - As described in **Section 2.2.1, Item 3**, AT&T sends Invites with the SIP parameter *maxptime:30*. In response, Avaya CS1000E will send *ptime:10* for any UNISTim or digital stations. The following script is used to change the *maxptime:30* parameter to *ptime:30*, thereby making Avaya CS1000E respond with *ptime:30* as required.

- Select **Global Profiles** → **Signaling Manipulation** from the menu on the left-hand side of the screen (not shown).
- Click **Add Script** (not shown) and the script editor window will open.
- Enter a name for the script in the **Title** box (e.g., **CS1K\_maxptime**). The script shown below defined.
- Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the Avaya Server Configuration in **Section 7.3.6, Step 4**.

Title

CS1K\_maxptime

Save

```

1 //Replace maxptime:30 with ptime:30 in calls to CS1K
2
3 within session "ALL"
4 {
5
6     act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
7
8     {
9
10        %BODY[1].regex_replace( "a=maxptime:30","a=ptime:30");
11
12    }
13 }

```

## 7.4. Domain Policies

### 7.4.1 Application Rules

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

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

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

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

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

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

Editing Rule: default-trunk

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

Miscellaneous

CDR Support

☒ None  
☐ CDR w/ RTP  
☐ CDR w/o RTP

RTCP Keep-Alive

☐

Finish

## 7.4.2 Media Rules

### 7.4.2.1 Avaya Media Rule

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

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

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

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

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

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

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

Click here to add a description.

Media NAT Media Encryption Media Anomaly Media Silencing **Media QoS**

Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

Audio DSCP AF11

Video QoS

Video DSCP AF11

Edit

### 7.4.2.2 AT&T Media Rule

**Step 1** – Repeat the steps in **Section 7.4.2.1** with the following changes:

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

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

## 7.4.3 Signaling Rules

As described in **Section 2.2.1, Item 4**, the Avaya SBCE is used to help reduce packet size by removed SIP headers not required by AT&T.

### 7.4.3.1 Avaya - Requests

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

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

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

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

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

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

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

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

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

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

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

### 7.4.3.2 Avaya - Responses

Following the steps shown in **Section 7.4.3.1**, Response Signaling Rules are defined to remove **AV-Global-Session-ID**, **History-Info**, **P-AV-Message-ID**, **Remote-Party-ID**, and **P-Location** headers for both **1xx** and **2xx** responses.

### Step 1 - Highlight the **CS1K\_with\_SM** rule created in **Section 7.4.3.1** and enter the following to remove the **AV-Global-Session-ID** proprietary header from **1XX** responses.

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

- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**

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

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

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

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

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

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

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

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

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

Filter By Device... [v] [Rename] [Clone] [Delete]

Click here to add a description.

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

Add In Header Control Add Out Header Control

Row	Header Name	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

### 7.4.3.3 AT&T – Requests

**Step 1** – Follow the steps in **Section 7.4.3.1**, and create a Request rule called **ATT\_SR**.

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

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

- Click **Finish**

#### 7.4.3.4 Avaya – Signaling QOS

**Step 1** - Highlight the **CS1K\_with\_SM** rule created in **Section 7.4.3.1** and enter the following:

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

#### 7.4.3.5 AT&T – Signaling QOS

**Step 1** - Highlight the **ATT\_SR** rule created in **Section 7.4.3.3** and repeat the procedure in **Section 7.4.3.4**.

#### 7.4.4 Endpoint Policy Groups – Avaya

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

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

- For **Name**: enter **Avaya\_default\_low\_PG**, then click **Next**.
- For **Application Rule**: enter **SIP\_Trunk\_AR** (see **Section 7.4.1**).
- For **Border Rule**: enter **default**.
- For **Media Rule**: enter **Avaya\_Trunk\_low\_med** (see **Section 7.4.2**).
- For **Security Rule**: enter **default-low**.
- For **Signaling Rule**: enter **CS1K\_SR\_with\_SM** (see **Section 7.4.3**).
- For **Time of Day**: enter **default**.



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

**Edit Policy Set**

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

**Finish**

## 7.4.5 Endpoint Policy Groups – AT&T

**Step 1** – Repeat the steps in **Section 7.4.4** with the following setting changes:

- For **Name**: enter **ATT\_default\_low\_PG**
- For **Signaling Rule**: enter **ATT\_SR** (see **Section 7.4.3.3**).

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

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

**Policy Groups**

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-subs...
- avaya-def-high-server
- ATT\_default-low\_PG**

**Policy Group**

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

**Edit Clone**

## 7.5. Device Specific Settings

### 7.5.1 Network Management

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

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

Dashboard  
Administration  
Backup/Restore  
System Management  
  Global Parameters  
  Global Profiles  
  SIP Cluster  
  Domain Policies  
    Application Rules  
    Border Rules  
    Media Rules  
    Security Rules  
    Signaling Rules  
    Time of Day Rules  
    End Point Policy  
    Groups  
    Session Policies  
  TLS Management  
  Device Specific Settings  
    Network Management

**Network Management: SBCE**

Devices  
SBCE

**Network Configuration** **Interface Configuration**

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

A1 Netmask: 255.255.255.0    A2 Netmask:    B1 Netmask: 255.255.255.0    B2 Netmask:   

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

## 7.5.2 Media Interface

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

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

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

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

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

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

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

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

**Media Interface: SBCE**

Devices  
SBCE

**Media Interface**

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

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

## 7.5.3 Signaling Interface

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

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

- For **Name**: enter **Inside\_Trunk\_SI**

- For **Media IP:** enter **192.168.67.120** (Avaya SBCE internal address toward Session Manager)
- For **TCP Port:** enter **5060**
- For **UDP Port:** enter **5060**

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

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

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

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

The screenshot shows the Avaya Session Manager configuration interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The 'Signaling Interface' option is highlighted. The main area is titled 'Signaling Interface: SBCE'. It contains a 'Devices' tab with 'SBCE' selected. Below this is a 'Signaling Interface' table with columns: Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. There are two entries: 'Inside\_Trunk\_SI' and 'Outside\_Trunk\_SI'. Each entry has 'Edit' and 'Delete' links. An 'Add' button is in the top right of the table area.

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

## 7.5.4 Endpoint Flows – To Avaya (Session Manager)

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

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

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

- For **Name:** enter **Avaya\_Trunk**
- For **Server Configuration:** enter **SM\_Trunk\_SC** (see Section 7.3.5)
- For **URI Group:** enter \* (default)
- For **Transport:** enter \* (default)
- For **Remote Subnet:** enter \* (default)
- For **Received Interface:** enter **Outside\_Trunk\_SI** (see Section 7.5.3)
- For **Signaling Interface:** enter **Inside\_Trunk\_SI** (see Section 7.5.3)
- For **Media Interface:** enter **Inside\_Trunk\_MI** (see Section 7.5.2)
- For **End Point Policy Group:** enter **Avaya\_default\_low\_PG** (see Section 7.4.4)
- For **Routing Profile:** enter **To\_ATT\_RP** (see Section 7.3.4)
- For **Topology Hiding Profile:** enter **Avaya\_TH** (see Section 7.3.7)
- For **File Transfer Profile:** enter **None**

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

## 7.5.5 Endpoint Flows – To AT&T Primary

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

**Step 1** – Repeat the steps in Section 7.5.4 with the following changes:

- For **Name:** enter **ATT\_Primary**
- For **Server Configuration:** enter **ATT\_Primary\_SC** (see Section 7.3.6)

- For **Received Interface**: enter **Inside\_Trunk\_SI** (see **Section 7.5.3**)
- For **Signaling Interface**: enter **Outside\_Trunk\_SI** (see **Section 7.5.3**)
- For **Media Interface**: enter **Outside\_Trunk\_MI** (see **Section 7.5.2**)
- For **End Point Policy Group**: enter **ATT\_default\_low\_PG** (see **Section 7.4.5**)
- For **Routing Profile**: enter **To\_SM\_RP** (see **Section 7.3.3**)
- For **Topology Hiding Profile**: enter **ATT\_TH** (see **Section 7.3.8**)

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

## 8. AT&T IP Flexible Reach Service

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

### 8.1. AT&T Provisioning

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

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

## 9. Verification Steps

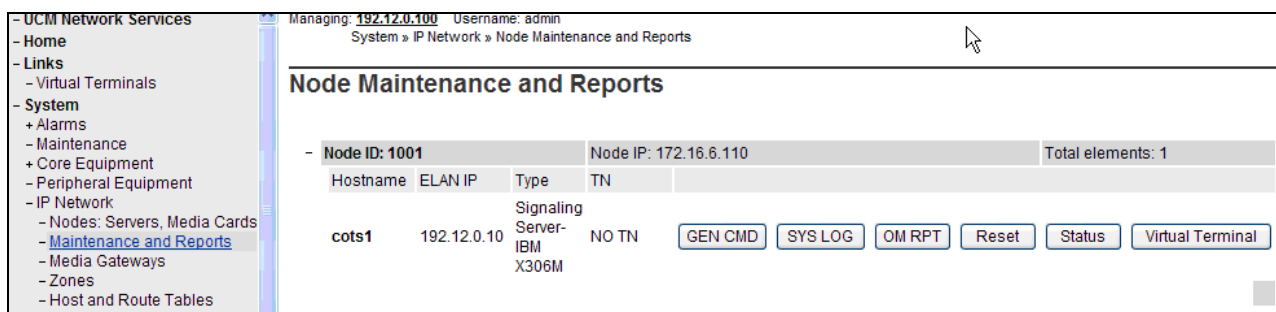
This section provides example verifications of the Avaya configuration with AT&T IP Flexible Reach service.

### 9.1. Avaya CS1000E Verifications

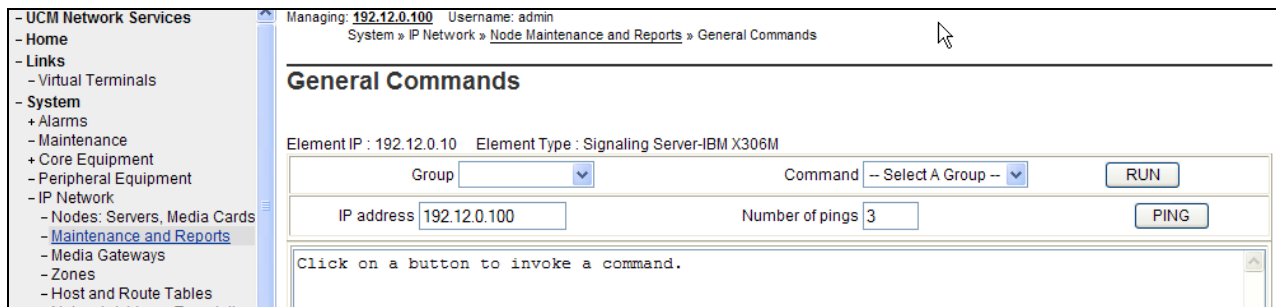
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

#### 9.1.1 IP Network Maintenance and Reports Commands

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



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



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

For example, to check the status of the SIP Gateway to Session Manager in the sample configuration, select “**Sip**” from the **Group** menu and “**SIPGwShow**” from the **Command** menu. Click **Run**. The example output below shows that the Session Manager (192.168.67.47, port 5060, TCP) has “SIPNPM Status” Active.

**General Commands**

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

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

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

```

SIPNPM Status      : Active
Primary Proxy IP address : 192.168.67.47
Primary Proxy port      : 5060
Primary Proxy Transport : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port      : 5060
Secondary Proxy Transport : TCP
Primary Proxy2 IP address : 192.168.67.47
Primary Proxy2 port      : 5060
Primary Proxy2 Transport : TCP
Active Proxy         : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 12 / 12
Stack version         : 5.5.0.13
TLS Security Policy   : Security Disabled
  
```

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

**General Commands**

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

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

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

Set Information

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

Total sets = 4

## 9.1.2 System Maintenance Commands

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



Managing: **10.7.8.61** Username: admin  
System » Maintenance

# Maintenance

☒ Select by Overlay
☐ Select by Functionality

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

# Maintenance

☒ Select by Overlay
☐ Select by Functionality

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

<Select Group>  
**D-Channel Diagnostics**  
MSDL Diagnostics  
TMDI Diagnostics

On the preceding screen, if “**LD 96 - D-Channel**” is selected on the left menu with “**D-Channel Diagnostics**” selected on the right menu, a screen such as the following is displayed. D-Channels **15** (Sip GW) and **20** (SIPLine), show as established (**EST**) and active (**ACTV**).

# D-Channel Diagnostics

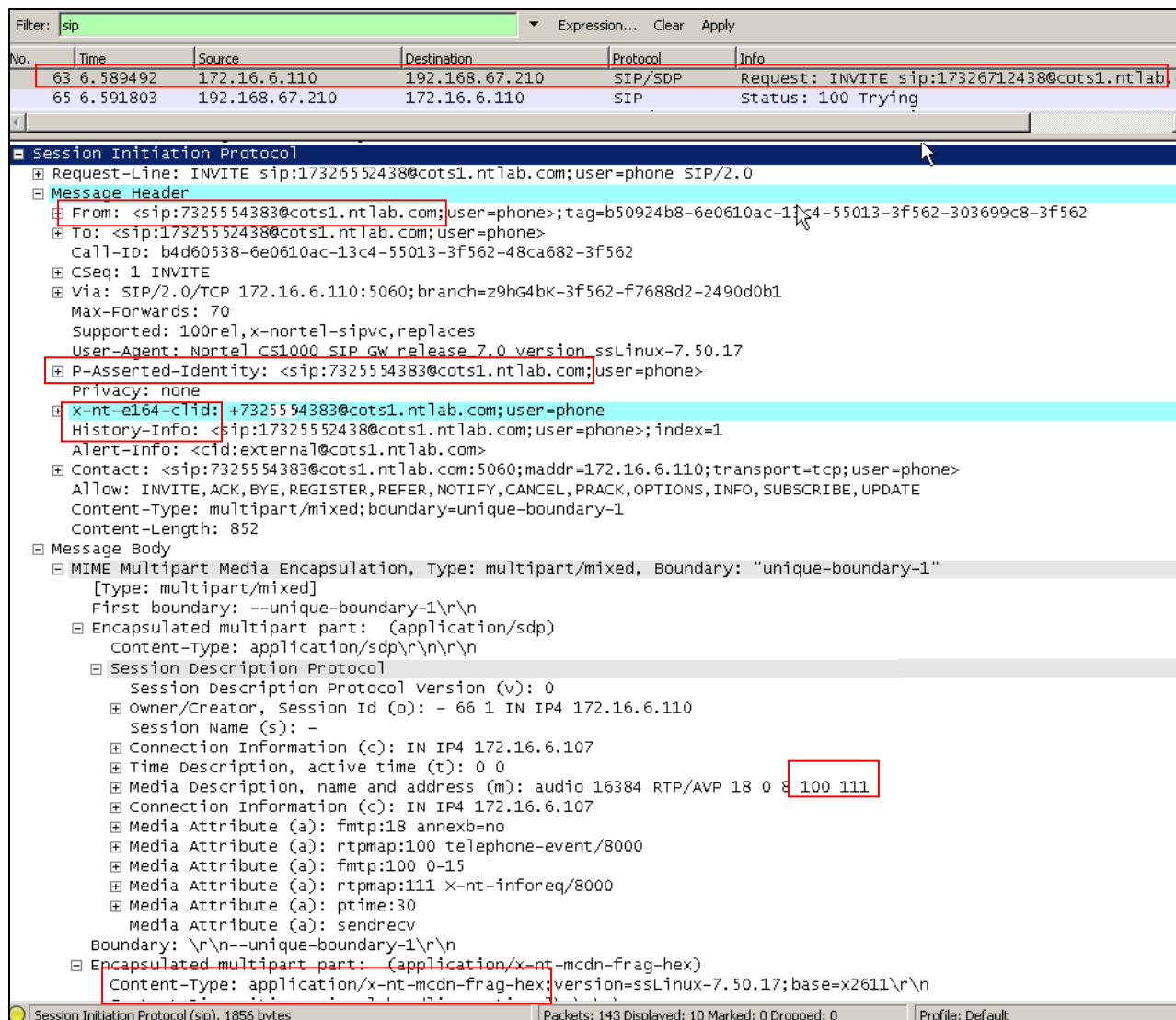
Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	<input type="button"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

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

## 9.2. SIP Protocol Traces

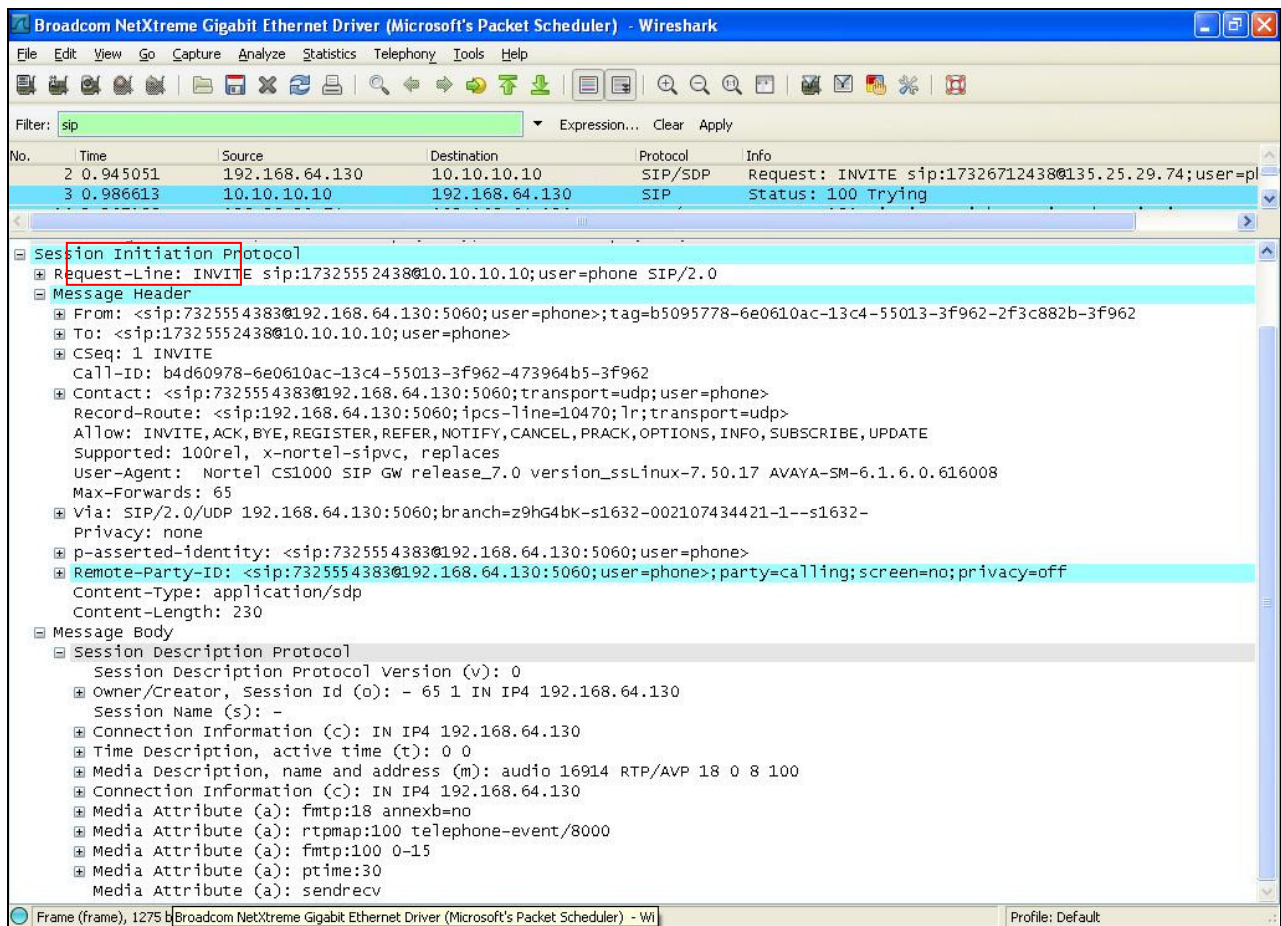
The following screen capture shows a Wireshark trace captured on the CPE private network, filtered on SIP messages. This section illustrates an example outbound call to PSTN from an Avaya CS1000E 1140E IP UNISim telephone with Directory Number 4095. The INVITE message sent by Avaya CS1000E to Session Manager is selected.

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

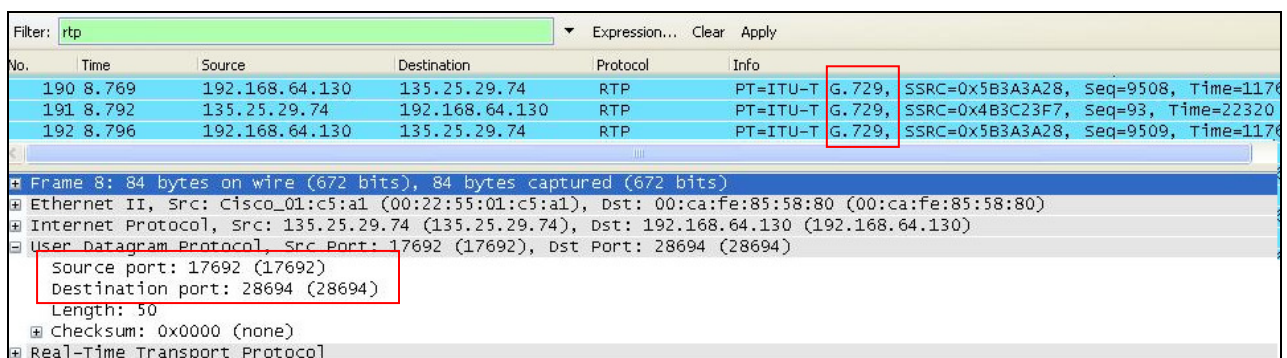


The following screen capture shows the subsequent INVITE message sent by Avaya SBCE to the AT&T border element. As can be observed in the example below:

- The Avaya CS1000E proprietary header “**x-nt-e164-clid**” was removed by the Avaya SBCE.
- The **111** telephone event was removed by Avaya SBCE.
- The Avaya CS1000E **MIME** headers were removed by Session Manager.
- The **History-Info** header was removed by Avaya SBCE.



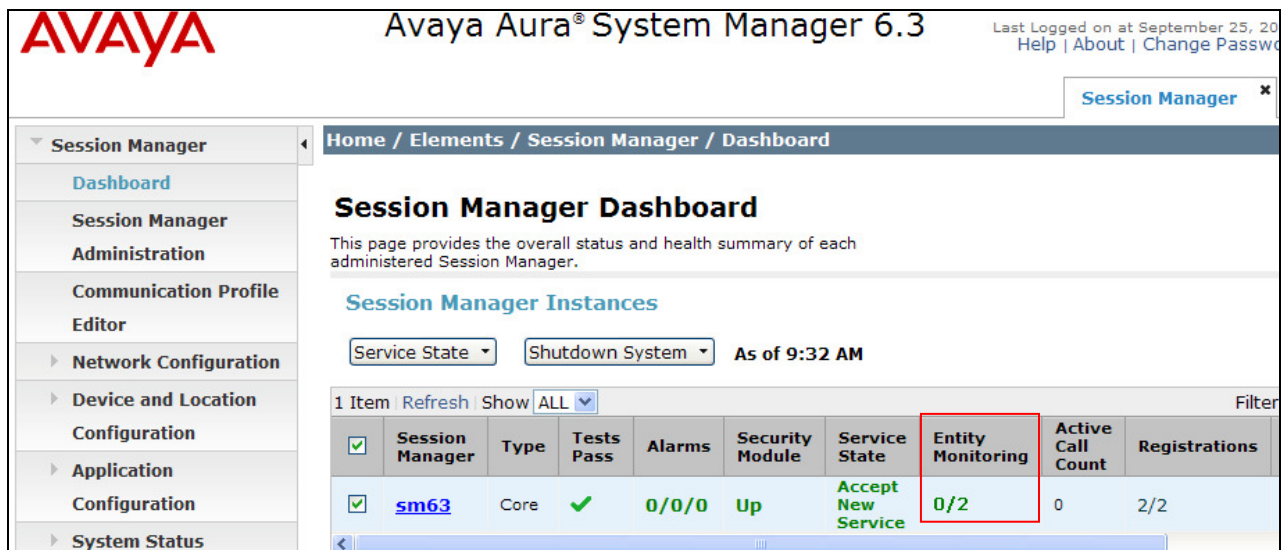
Changing the display filter to **rtp**, the media streams for this call are displayed. Note that the UDP ports used are within the range defined in **Section 7.5.2**. Also note that G.729 was the codec used.



## 9.3. System Manager / Session Manager Verification

### 9.3.1 Verify Service State and Entity Link Status

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



Avaya Aura® System Manager 6.3

Last Logged on at September 25, 2013  
Help | About | Change Password

Session Manager

Session Manager Dashboard

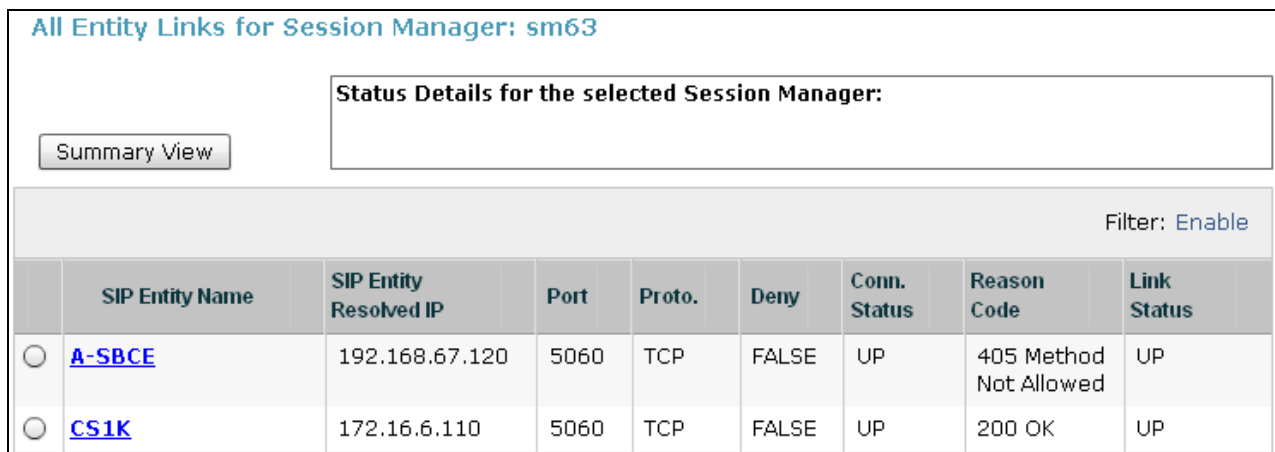
This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State Shutdown System As of 9:32 AM

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

Click on the **Entity Monitoring** display (e.g., 0/2), and a list of all the provisioned SIP Entities, and their states, are displayed. Under normal operating conditions, the **Conn. Status** should be “**Up**” as shown in the example screen below. The **Reason Code** column indicates that the Avaya SBCE has responded to SIP OPTIONS from Session Manager with a SIP 405 message which is sufficient for SIP Link Monitoring to consider the link up.



All Entity Links for Session Manager: sm63

Status Details for the selected Session Manager:

Summary View

Filter: Enable

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



### 9.3.2 Call Routing Test

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

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

### Call Routing Test

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

#### SIP INVITE Parameters

555

**Called Party URI**

**Calling Party Address**

**Calling Party URI**

**Session Manager Listen Port**

**Day Of Week**

**Time (UTC)**

**Transport Protocol**

**Called Session Manager Instance**

#### Routing Decisions

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

#### Routing Decision Process

NRP Adaptations: CS1K\_AT&T\_AA-SBC applied.

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

Originating Location is AA-SBC. Using digits < 7325554383 > and host < cots1.ntlab.com > for routing.

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

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

NRP Dial Patterns: Found a Dial Pattern match for pattern < 732555 > Min/Max length 10/10 and domain < null >.

NRP Routing Policies: Ranked destination NRP Sip Entities: CS1K

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP Sip Entities: CS1K

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

Adapting and proxying for SIP Entity CS1K.

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

NRP Adaptations: CS1K applied.

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

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

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

JF; Reviewed:  
SPOC 11/25/2013

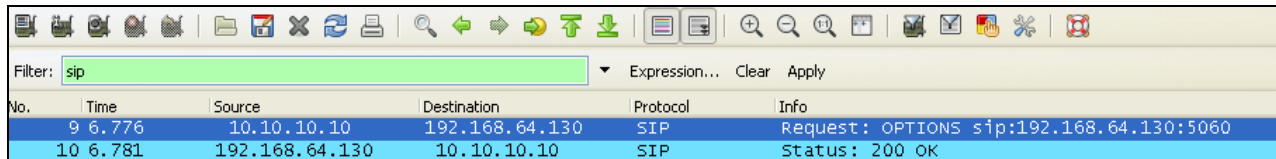
Solution & Interoperability Test Lab Application Notes  
©2013 Avaya Inc. All Rights Reserved.

92 of 99  
CS1K76SMSBCEFR

## 9.4. Avaya Session Border Controller for Enterprise Verification

### 9.4.1 Verify Avaya SBCE Connectivity to AT&T IP Flexible Reach

Verify that your entity links from Avaya SBCE (192.168.64.130) to AT&T IP Flexible Reach border element (10.10.10.10) are up and communicating with SIP OPTION messages and a response messages.



The image shows a Wireshark packet capture interface. The filter is set to 'sip'. The packet list shows two packets: a SIP Request (OPTIONS) from 10.10.10.10 to 192.168.64.130 at time 9.6.776, and a SIP Status (200 OK) from 192.168.64.130 to 10.10.10.10 at time 10.6.781.

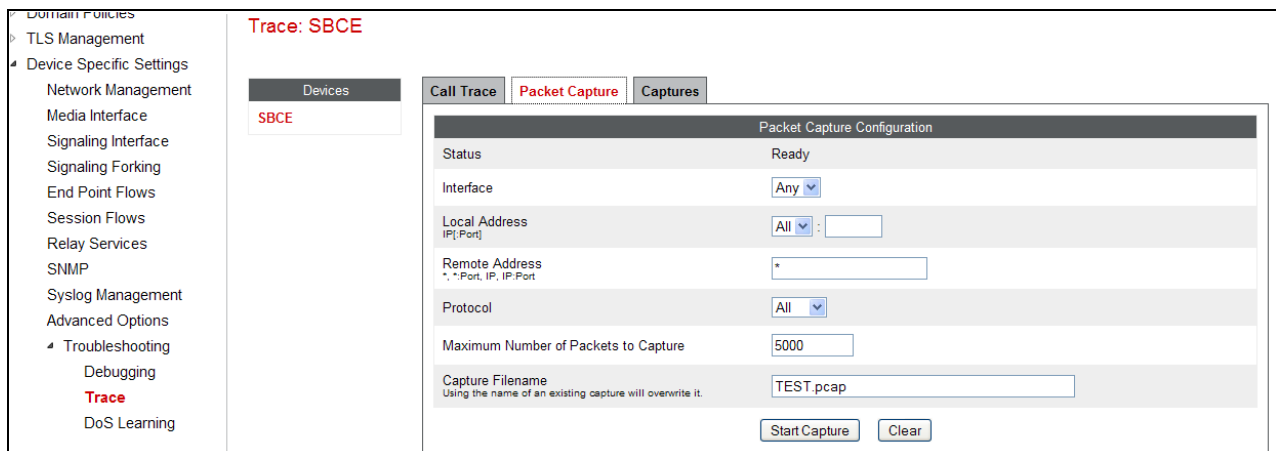
No.	Time	Source	Destination	Protocol	Info
9	6.776	10.10.10.10	192.168.64.130	SIP	Request: OPTIONS sip:192.168.64.130:5060
10	6.781	192.168.64.130	10.10.10.10	SIP	Status: 200 OK

### 9.4.2 Internal Tracing

**Step 1** – Using the left hand column menu described in **Section 7**, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**.

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

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



The image shows the Avaya SBCE configuration interface for packet capture. The left sidebar shows the navigation menu with 'Trace' selected under 'Troubleshooting'. The main area is titled 'Trace: SBCE' and has tabs for 'Devices', 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, showing the 'Packet Capture Configuration' form. The form includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (\*), Protocol (All), Maximum Number of Packets to Capture (5000), and Capture Filename (TEST.pcap). There are 'Start Capture' and 'Clear' buttons at the bottom.

The capture process will initialize, (“Please wait while your settings are saved and the capture is started”), and then display will say “**In Progress**”.

Trace: SBCE

Devices  
SBCE

Call Trace
Packet Capture
Captures

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

Packet Capture Configuration	
Status	In Progress
Interface	Any
Local Address IP[:Port]	All :
Remote Address *, *.Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	5000
Capture Filename Using the name of an existing capture will overwrite it.	TEST.pcap
Stop Capture	

**Step 3** – Run the test.

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

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

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

Trace: SBCE

<div> Devices SBCE </div>	<div> Call Trace Packet Capture Captures </div>
-------------------------------	---

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



## 10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server Release 7.6, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.2 can be configured to interoperate successfully with AT&T IP Flexible Reach service via either AVPN or MIS-PNT transport, within the constraints specified in **Section 2.2.1**. This solution allows Avaya Communication Server 1000E user access to the PSTN using an AT&T IP Flexible Reach service connection.

## 11. References

### 11.1. Avaya

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

#### Avaya Communication Server 1000E

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

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

- [6] *Administering Avaya Aura® Session Manager*, Release 6.3, December, 2012
- [7] *Implementing Avaya Aura® Session Manager*, Release 6.3, March, 2013
- [8] *Implementing Avaya Aura® System Manager*, Release 6.3, Issue 1, December, 2012
- [9] *Administering Avaya Aura® System Manager*, Release 6.3, Issue 1.0, December, 2012

#### Avaya Session Border Controller for Enterprise

- [10] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 20
- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013

### 11.2. AT&T IP Flexible Reach service.

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

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

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

The AT&T IP Flexible Reach - Enhanced Features SIP Trunk 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 **10.10.10.10** and **10.10.10.11**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to 10.10.10.11 (the primary trunk connection to 10.10.10.10 is defined in **Sections 7.3.4** and **7.3.6**).

### 12.1.1 Configure the Secondary Border Element Server Configuration

Repeat the steps in **Section 7.3.6** to create a Server Configuration for the connection to the AT&T secondary Border Element, using the following entries:

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

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

- Enter **IP Address: 10.10.10.11** (See the note in **Section 3.1** regarding this address).
- For **Supported Transports**: check **UDP**
- For **UDP Port**: enter **5060**
- Select **Next**

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

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

- Select **ATT\_SI** for **Interworking Profile** (created in **Section 7.3.2**).
- For the **Signaling Manipulation Script** select the **CS1K\_maxptime** script that was defined in **Section 7.3.9**.

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

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

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

Server Configuration: ATT\_Secondary\_SC

Add      Rename    Clone    Delete

Server Profiles

- ATT\_Primary\_SC
- SM\_Trunk\_SC
- ATT\_Secondary\_SC**

General    Authentication    Heartbeat    Advanced

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

Edit

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

### Server Configuration: ATT\_Secondary\_SC

Add
Rename
Clone
Delete

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

General
Authentication
Heartbeat
Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	CS1K_maxptime
UDP Connection Type	SUBID

Edit

## 12.1.2 Add Secondary Border Element IP Address to Routing

Repeat the steps in **Section 7.3.4** to add a Routing Profile for the AT&T secondary Border Element.

**Step 1** – Select the profile created in **Section 7.3.4** (e.g., To\_ATT\_RP).

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

- Set **Next Hop Server 2:** to **10.10.10.11** (AT&T Border Element IP address, see note in **Section 3.1** regarding this address).

**Step 3** - Click **Finish**.

Edit Routing Rule

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

Next Hop Routing

URI Group
\*

Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port
10.10.10.10

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

Routing Priority based on Next Hop Server
☒

Use Next Hop for In Dialog Messages
☐

Ignore Route Header for Messages Outside Dialog
☐

NAPTR
☐

SRV
☐

Outgoing Transport
☐ TLS
☐ TCP
☒ UDP

Finish

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

**Step 1** – Repeat the steps in **Section 7.5.5**, with the following changes, to add an Endpoint Flow for the AT&T secondary Border Element:

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

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

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

End Point Flows: SBCE

Devices  
SBCE

Subscriber Flows Server Flows

Click here to add a row description.

Server Configuration: ATT\_Primary\_SC

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

Server Configuration: ATT\_Secondary\_SC

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

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

---

©2013 Avaya Inc. All Rights Reserved.

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

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