



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 6.3 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 6.3, 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 6.3 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.

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

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

Table of Contents

1	Introduction.....	5
2	General Test Approach and Test Results.....	5
2.1	Interoperability Compliance Testing	6
2.2	Test Results.....	6
2.3	Support.....	9
3	Reference Configuration.....	9
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	CS1000E Provisioning.....	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.....	27
5.5.1	Provision SIP Gateway	27
5.5.2	Integrated Services Digital Network (ISDN).....	30
5.5.3	Virtual D-Channel Configuration	30
5.5.4	SIP Routes Configuration	32
5.5.5	SIP Trunk Configuration.....	35
5.6	Routing of Outbound Dialed Numbers to Session Manager	36
5.6.1	Route List Block	36
5.6.2	Digit Manipulation Block	38
5.6.3	NARS Access Code	39
5.6.4	Numbering Plan Area Codes	40
5.6.5	Other Special Numbers to Route to Session Manager.....	41
5.7	Routing of Inbound Numbers to CS1000E.....	42
5.8	Enabling Plug-Ins for Call Transfer Scenarios	44
5.9	Customer Information.....	44
5.9.1	Calling Number Provisioning for calls to the AT&T IP Flexible Reach Service....	44
5.10	CS1000E Stations	47
5.10.1	Sample IP UNISlim Phone DN 4095.....	47
5.10.2	Analog Fax Line	50
5.11	Changing RFC2833 DTMF Telephone Event Type.....	50
5.12	Ad Hoc Privacy Dialing.....	51

5.13	Configuration Backup	51
6	Configure Avaya Aura® Session Manager Release 6.3	52
6.1	SIP Domain	53
6.2	Locations	53
6.3	Configure Adaptations	54
6.3.1	Adaptation for Calls to the CS1000E	55
6.3.2	Adaptation for calls from the CS1000E to AT&T	57
6.4	SIP Entities	58
6.4.1	SIP Entity for the CS1000E	58
6.4.2	SIP Entity for the Avaya SBCE	59
6.4.3	SIP Entity for Session Manager	60
6.5	Entity Links	60
6.5.1	Entity Link to CS1000E Entity	60
6.5.2	Entity Link to the Avaya SBCE	61
6.6	Routing Policies	61
6.6.1	Routing Policy to the CS1000E	61
6.6.2	Routing Policy to the Avaya SBCE	62
6.7	Dial Patterns	63
6.7.1	Inbound AT&T calls to the CS1000E	63
6.7.2	Outbound Calls to AT&T	64
7	Configure Avaya Session Border Controller for Enterprise	65
7.1	System Management/Status	66
7.2	Global Profiles	67
7.2.1	Server Interworking – Avaya	67
7.2.2	Server Interworking – AT&T	69
7.2.3	Signaling Manipulation	69
7.2.4	Server Configuration – Session Manager	71
7.2.5	Server Configuration – AT&T	72
7.2.6	Routing – To Session Manager	72
7.2.7	Routing – To AT&T	73
7.2.8	Topology Hiding – Avaya Side	74
7.2.9	Topology Hiding – AT&T Side	74
7.3	Domain Policies	75
7.3.1	Application Rules	75
7.3.2	Media Rules	75
7.3.3	Signaling Rules	76
7.3.4	Endpoint Policy Groups – Avaya Connection	79
7.3.5	Endpoint Policy Groups – AT&T Connection	80
7.4	Device Specific Settings	80
7.4.1	Network Management	80
7.4.2	Advanced Options	80
7.4.3	Media Interfaces	81
7.4.4	Signaling Interface	82
7.4.5	Endpoint Flows	82
8	AT&T IP Flexible Reach Service	84
9	Verification Steps	85
9.4	CS1000E Verifications	85
9.4.1	IP Network Maintenance and Reports Commands	85

9.4.2	System Maintenance Commands	86
9.5	Avaya Aura® Session Manager.....	87
9.6	Avaya Session Border Controller for Enterprise	88
9.6.1	System Status	88
9.6.2	Protocol Traces	88
10	Conclusion	90
11	References	91
12	Addendum 1 – Redundancy to Multiple AT&T Border Elements	92
12.1	Configure the Secondary Border Element Server Configuration	92
12.2	Add Secondary Border Element IP Address to Routing.....	93
12.3	Configure Secondary AT&T Border Element End Point Flow	93

1 Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.6 (CS1000E), Avaya Aura® Session Manager Release 6.3 (Session Manager), and the Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE), with the AT&T IP 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 6.3 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach - Enhanced Features 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- Enhanced Features service 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 AVPN¹ or MIS/PNT² transport services.

2 General Test Approach and Test Results

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

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPFR-EF and the Customer Premises Equipment (CPE) containing the CS1000E, Session Manager, and the Avaya SBCE (see **Section 3.2** for call flow examples).

The test environment consisted of:

- A simulated enterprise including the CS1000E, Session Manager, System Manager (for Session Manager provisioning), the Avaya SBCE, Avaya phones, and fax machine emulation software (Ventafax application).
- An IPFR-EF service production circuit, to which the simulated enterprise was connected via AVPN transport.

¹ AVPN supports compressed RTP (cRTP).

² MIS/PNT does not support cRTP.

2.1 Interoperability Compliance Testing

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

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPFR-EF network. Calls were made between the PSTN, via the IPFR-EF network, and the CPE.

The following SIP trunking VoIP features were tested with the IPFR-EF service:

- Inbound/Outbound voice calls between PSTN, the IPFR-EF service, the Avaya SBCE, Session Manager, and the CS1000E. Avaya 1140E SIP and IP telephones, as well as M3904 Digital telephones, were used.
- Inbound/Outbound fax calls using T38 or G.711.
- Various outbound PSTN destinations were tested including long distance, international, and toll-free.
- Requests for privacy (i.e., caller anonymity) for CS1000E outbound calls to the PSTN, as well as privacy requests for inbound calls from the PSTN to CS1000E users.
- SIP OPTIONS messages used to monitor the health of the SIP trunks between the CPE and AT&T.
- Incoming and outgoing calls using the G.729(A & B) and G.711 ULAW codecs.
- Call redirection with Diversion Header.
- Operator assistance and 911 calls.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful PSTN and CS1000E voice menu navigation.
- CS1000E stations call coverage to Avaya Call Pilot® for message generation and retrieval (including Message Wait Indicator).
- Telephony features such as hold, transfer, and conference.
- Proper UDP port ranges for RTP media (16384-32767) were verified.
- IPFR-EF network service features (see **Section 2.2, Item 9**).
 - Simultaneous Ring
 - Sequential Ring

2.2 Test Results

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

1. **CS1000E Unattended Call Transfers** - To allow the CS1000E user to transfer a call from PSTN user A to PSTN user B, before user B has answered the call (unattended transfer), CS1000E plug-in 501 must be enabled as shown in **Section 5.8**. However, while plug-in 501 will allow the 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 IPFR-EF service does not support SIP History-Info headers. However, the IPFR-EF 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 7.3.3**).
3. **Maxptime:30 and Ptime:10** – For inbound calls, the IPFR-EF service sends Invites with the SIP parameter *maxptime:30*. In response, the CS1000E will send *ptime:10* for any UNISim 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 CS1000E respond with *ptime:30* as required (see **Section 7.2.3**).
4. **Removal of CS1000E MIME headers** – The CS1000E includes MIME type headers in Invite messages. The AT&T IPFR-EF will reject calls that include these headers. The MIME headers are removed by Session Manager Adaptations (see **Section 6.3.2**).
5. **The Avaya SBCE issues a Remote-Address header even though the option to do so is disabled** - During testing it was found that the Avaya SBCE was including a Remote-Address header to SIP Invite messages leaving the Avaya SBCE (inbound or outbound, depending on call direction), even though the option was disabled.
 - a. No issues were caused by the inclusion of this header; however the Avaya SBCE was provisioned to remove this header (see **Section 7.3.3**, and **Item 6** below) for calls to AT&T, to reduce overall packet size.
6. **Removal of Unnecessary SIP Headers** – Depending on the call flow and the endpoints involved, the CS1000E and Session Manager may send multiple SIP headers that are not used by AT&T. The following headers are removed in the interest of reducing packet overhead (see **Section 7.3.3**):
 - a. Alert-Info, x-nt-e164-clid, Remote-Party-ID, Resource-Priority, AV-Global-Session-ID, P-AV-Message-ID, and P-Location.
7. **CS1000E Telephone Events 101 and 111** - The CS1000E uses Telephone Event type 101 by default. This value is changed to the AT&T recommended value of 100 in the CS1000E (see **Section 5.11**). Telephone event type 111 is also sent by the CS1000E. This value is removed by the Avaya SBCE (see **Section 7.2.3**).
8. **Avaya 1140E SIP phone DTMF Telephone Event and PTIME values** – The Avaya 1140E SIP phone uses a fixed DTMF Telephone Event value of 101, as well as affixed PTIME value of 20. While the IPFR-EF service uses a DTMF Telephone Event of 100, and recommends the use of PTIME= 30, no issues were found during testing.

9. **Some IPFR-EF feature access methods are not currently supported by the CS1000E** – During testing, two issues were found related to support of some IPFR-EF features.
- a. **Network based Blind Transfer (Call Redirection using PBX generated REFER)** – The CS1000E does not support Refer.
 - b. **Network based Call Forward scenarios cannot be signaled by the 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 special codes beginning with * (e.g., *71), in the R-URI of the Invite sent to AT&T. The CS1000E does not have the capability to send * as part of the dialed string in the R-URI.
 - 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 state manually.
10. **The 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 CS1000E Incoming Digit Translation (IDT) table (see **Section 5.7**), the 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 PAI header prior to sending the subsequent call responses back to AT&T (see **Section 6.3.1**). As a result, the PAI is populated with the associated IPFR-EF DNIS number.
11. **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.
12. **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) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor. While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 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/voice-services/null/sip-trunking/>

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 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).
- Avaya desk phones are represented with Avaya 1140E UNISlim IP, 1140E SIP, and Digital M3904 telephones.
- Session Manager provides core SIP routing and integration services that enable communication between the CS1000E and the Avaya SBCE/IPFR-EF service. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP to communicate with the CS1000E.
- System Manager 6.3 provides the provisioning/management interface for Session Manager.
- 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 IPFR-EF service.
- An integrated Avaya Call Pilot® system provides the 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).

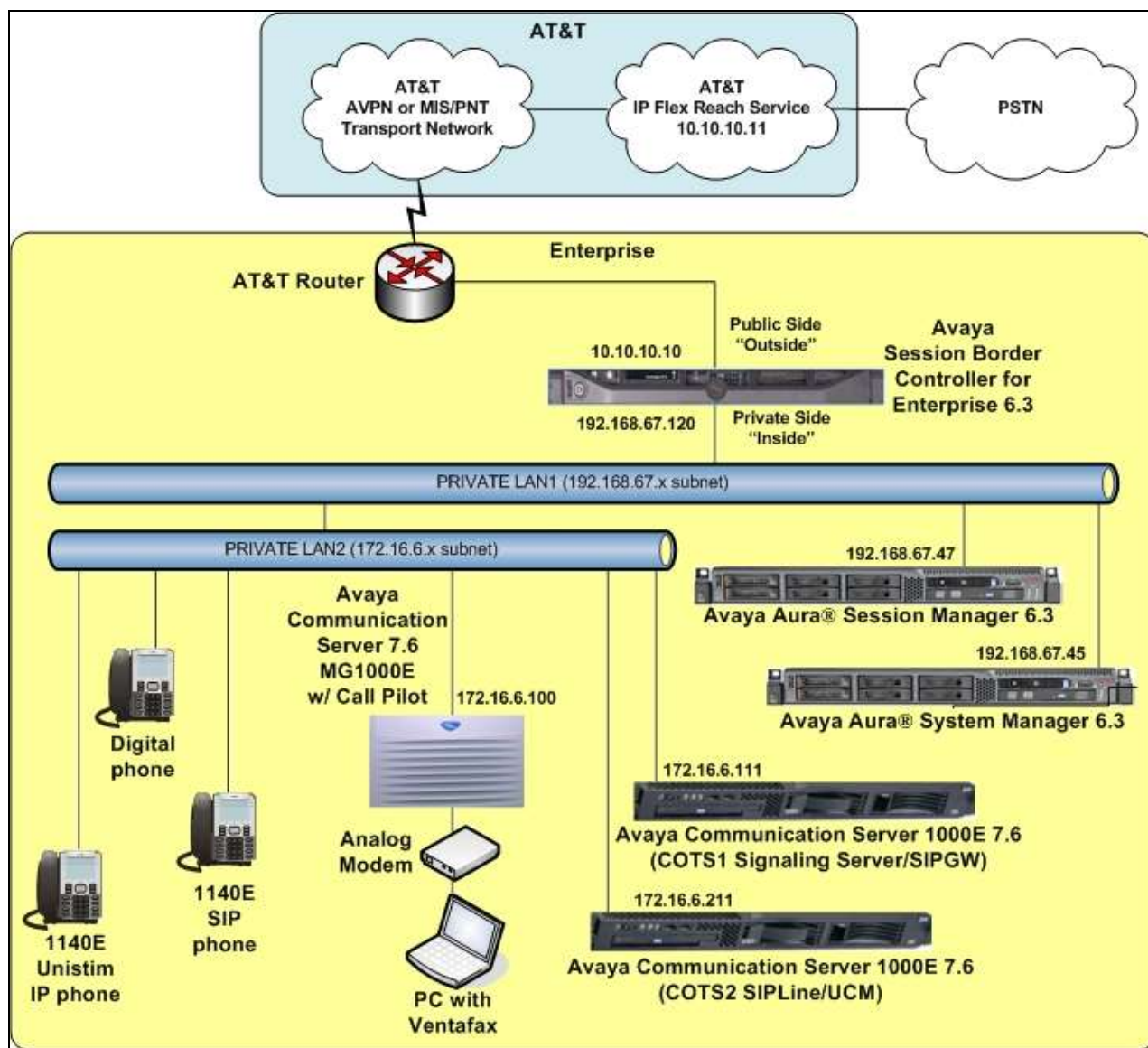


Figure 1: Reference Configuration

3.1 Illustrative Configuration Information

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

Note – The 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
CS1000E	
COTS1 SIP Signaling Server (TLAN)	172.16.6.110
COTS2 SIP Line (TLAN)	172.16.6.210
MGC Media (DSP) (TLAN)	172.16.6.115
Avaya Call Pilot®	
Call Pilot Application	172.16.6.12
Avaya SBCE	
“Outside” (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service)	10.10.10.10 (see note below)
“Inside” (Private) Interface (connected to Session Manager)	192.168.67.120
AT&T IP Flexible Reach Service	
Border Element (Primary & Secondary)	10.10.10.11 (see note below)

Table 1: Illustrative Network Values Used in these Application Notes

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

3.2 Call Flows

To understand how inbound/outbound IPFR-EF 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 IPFR-EF service call that arrives at Avaya SBCE, to Session Manager, and is subsequently routed to the CS1000E, which in turn routes the call to a phone or fax.

1. A PSTN phone originates a call to an IPFR-EF service number.
2. The PSTN routes the call to the IPFR-EF service network.
3. The IPFR-EF 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 CS1000E.
6. Depending on the called number, the CS1000E routes the call to a phone or fax.

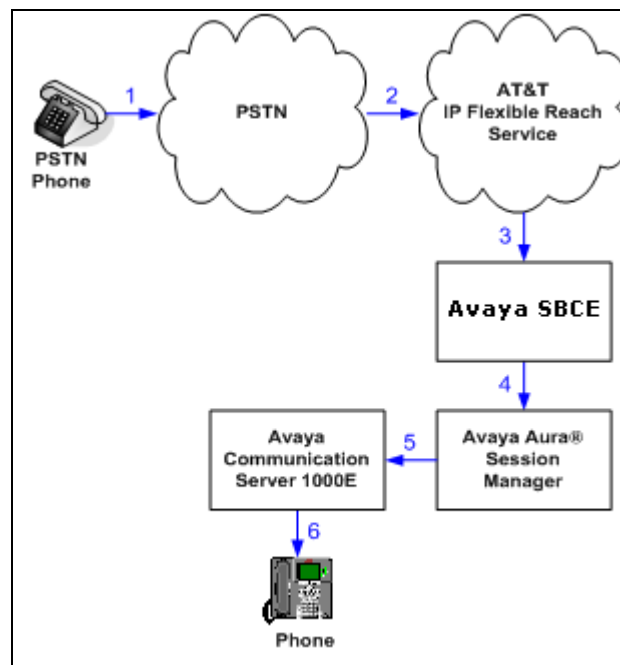


Figure 2: Inbound AT&T IP Flexible Reach Call

3.2.2 Outbound

The second call scenario illustrated is an outbound call initiated on the CS1000E, routed to Session Manager and is subsequently sent to the Avaya SBCE for delivery to the IPFR-EF service.

1. A CS1000E phone or fax originates a call to an IPFR-EF service number for delivery to PSTN.
2. The 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 IPFR-EF service.
5. The IPFR-EF service delivers the call to PSTN.
6. The PSTN delivers the call to the PSTN Phone.

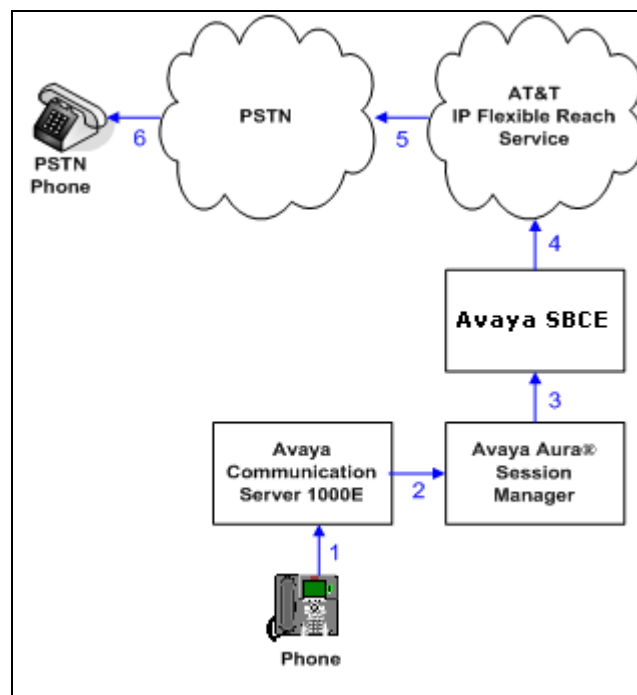


Figure 3: Outbound AT&T IP Flexible Reach Call

3.2.3 Call Forward Re-direction

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

Note – In cases where calls are forwarded to an alternate destination such as an 8xx numbers, the IPFR-EF 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 CS1000E phone has set Call Forward to another IPFR-EF service number, the CS1000E initiates a new call back out to Session Manager, Avaya SBCE, and to the IPFR-EF service network.
3. The IPFR-EF service places a call to the alternate destination and upon answering; CS1000E connects the calling party to the target party.

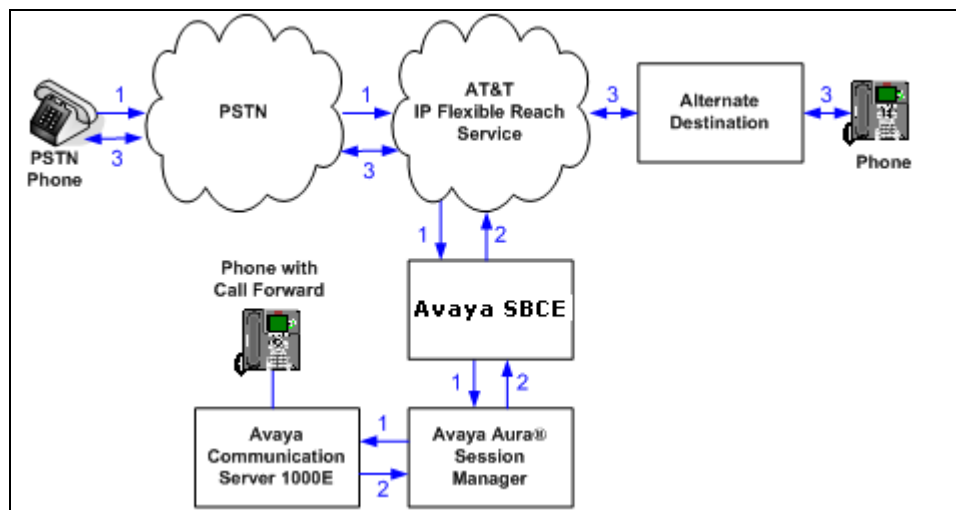


Figure 4: Re-directed (e.g., Call Forward) AT&T IP Flexible Reach Call

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 CS1000E.

1. Same as the first call scenario in **Section 3.2.1**.
2. The called CS1000E phone does not answer the call, and the call covers to the phone's voicemail. The 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.

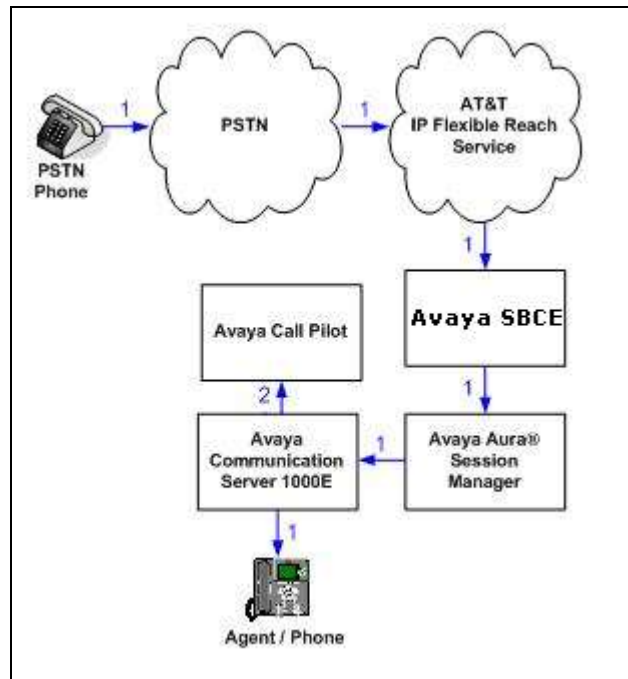


Figure 5: Coverage to Voicemail

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">System PlatformAvaya Aura® System Manager	<ul style="list-style-type: none">6.3.6.1005.06.3.13.10.3336 (SP13)
IBM 8800 server <ul style="list-style-type: none">Avaya Aura® Session Manager	<ul style="list-style-type: none">6.3.13.0.631304 (SP13)
CS1000E Platform	<ul style="list-style-type: none">Version 4021, Release 765P+Service_Pack CPM_7.65.16.00Call Pilot 5.00.41
Dell R210 <ul style="list-style-type: none">Avaya Session Border Controller for Enterprise	<ul style="list-style-type: none">6.3.2-08-5478 (SP2)
Avaya 1140E Series IP Deskphones (UNISTim)	<ul style="list-style-type: none">0625C8Q
Avaya 1140E Series IP Deskphones (SIP)	<ul style="list-style-type: none">SIP1140e04.04.20.00.bin
Avaya M3904 Series Digital Deskphones	-
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none">7.0.202.494

Table 2: Equipment and Software Versions

5 CS1000E Provisioning

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

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

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

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

5.1 Logging In and Selecting the System Element

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

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

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

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

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

5.2 Administer Telephony Node

5.2.1 Node Information and IP Addresses

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

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

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

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

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 CS1000E in **Section 6.4.1**.

AVAYA CS1000 Element Manager

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

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

Node ID: 1001 * (8-9999)
Call server IP address: 192.12.0.100 *
TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6
Embedded LAN (ELAN)
Gateway IP address: 192.12.0.1 *
Subnet mask: 255.255.255.0 *
Telephony LAN (TLAN)
Node IPv4 address: 172.16.6.110 *
Subnet mask: 255.255.255.0 *
Node IPv6 address:
* Required Value. Save Cancel

Associated Signaling Servers & Cards

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

AVAYA CS1000 Element Manager

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

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

Subnet mask: 255.255.255.0 *
Subnet mask: 255.255.255.0 *
Node IPv6 address:
* Required Value. Save Cancel

IP Telephony Node Properties

- [Voice Gateway \(VGW\) and Codecs](#)
- [Quality of Service \(QoS\)](#)
- [LAN](#)
- [SIP](#)
- [Numbering Zones](#)
- [MCDN Alternative Routing Treatment \(IM, T\) Causes](#)

Applications (click to edit configuration)

- [SIP Line](#)
- [Terminal Proxy Server \(TPS\)](#)
- [Gateway \(SIPGw\)](#)
- [Personal Directories \(PD\)](#)
- [Presence Publisher](#)
- [IP Media Services](#)

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. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, and Customers. The main area displays 'IP Telephony Node Properties' with a list of applications including SIP Line, Terminal Proxy Server (TPS), Gateway (SIPGW), Personal Directories (PD), Presence Publisher, and IP Media Services. The 'Terminal Proxy Server (TPS)' is highlighted with a red box. Below this, the 'Associated Signaling Servers & Cards' section shows a table with columns: Hostname, Type, Deployed Applications, ELAN IP, TLAN IPv4, and Role. A table entry for 'cots1' is shown as a 'Signaling_Server' with various applications. At the bottom, there is a note about server availability.

5.2.2 Enable Terminal Proxy Server

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

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

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

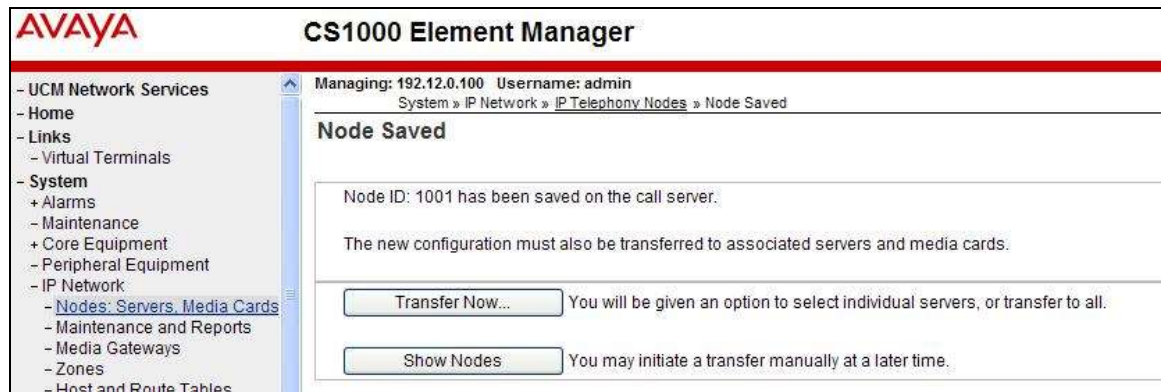
The screenshot shows the 'UNISTim Line Terminal Proxy Server (LTPS) Configuration Details' page. The breadcrumb trail indicates the path: System > IP Network > IP Telephony Nodes > Node Details > UNISTim Line Terminal Proxy Server (LTPS) Configuration. The page has tabs for Firmware, DTLS, and Network Connect Server. Under the 'Network Connect Server' tab, there is a checkbox labeled 'Enable proxy service on this node' which is checked and highlighted with a red box. Below this, there are input fields for IP address (0.0.0.0), Full file path (download/firmwa), Server Account/User ID, and Password. At the bottom, there is a 'DTLS' section with a dropdown menu.

5.2.3 Synchronize Configuration

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

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

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

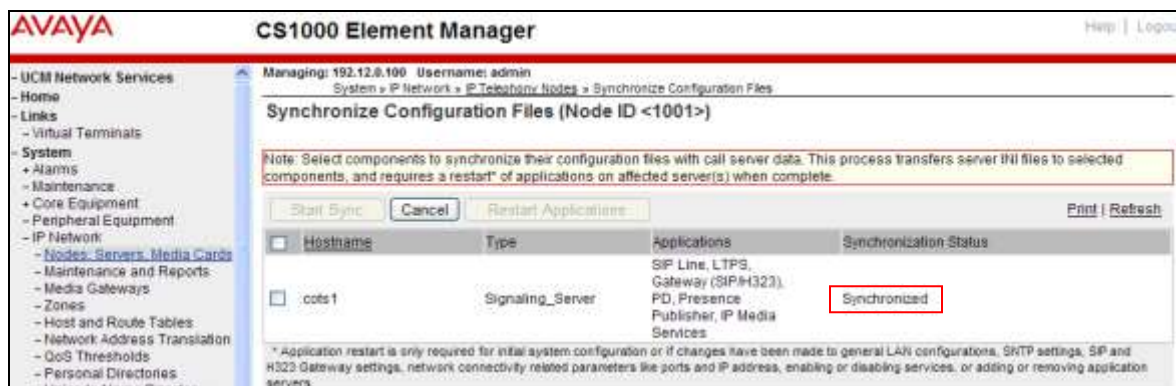


Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

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



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



Step 5 - After synchronization completes, click on the **Refresh** button in the right hand corner, Select the appropriate Hostname (e.g., cots1), and click **Restart Applications**.

Note - When the applications restart, the phones will also reset.



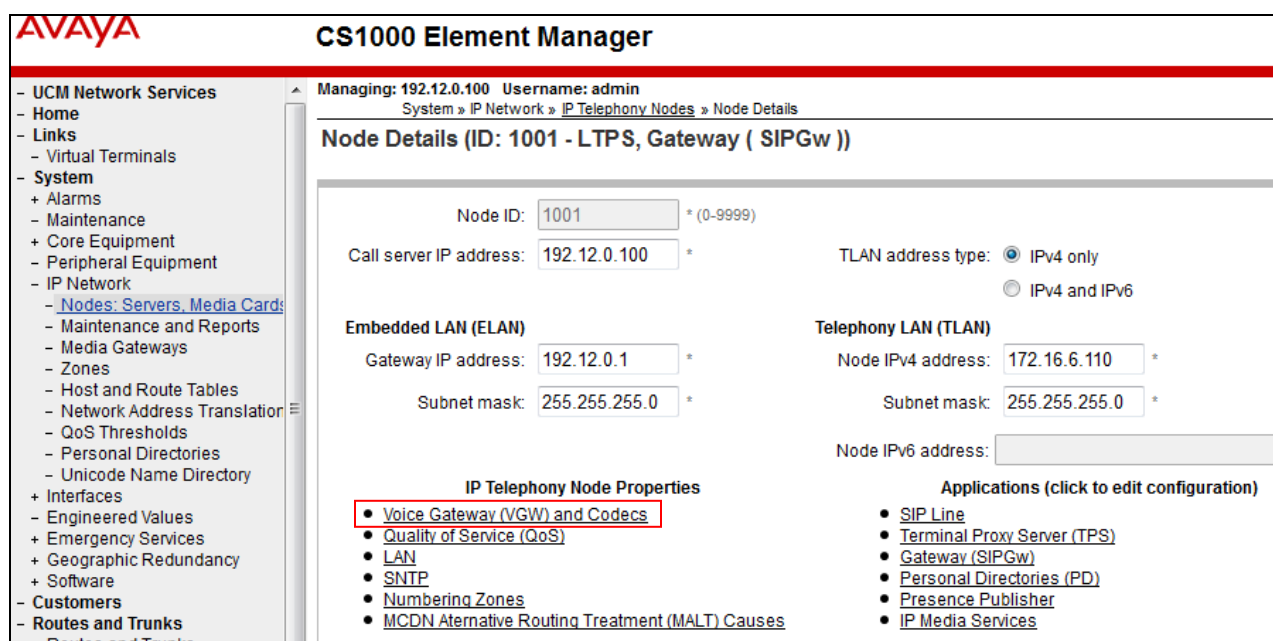
5.3 Voice Codecs

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

5.3.1 IP Telephony Node Codec Configuration

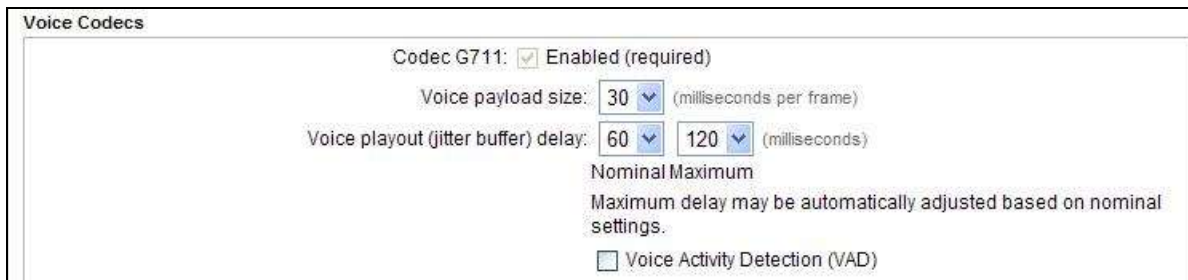
Step 1 – As shown in Section 5.2, expand **System** → **IP Network**, select **Node, Server, Media Cards**, and select node **1001**.

Step 2 – Scroll down the upper half of the form and under the **IP Telephony Node Properties** heading, select **Voice Gateway (VGW) and Codecs**.



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

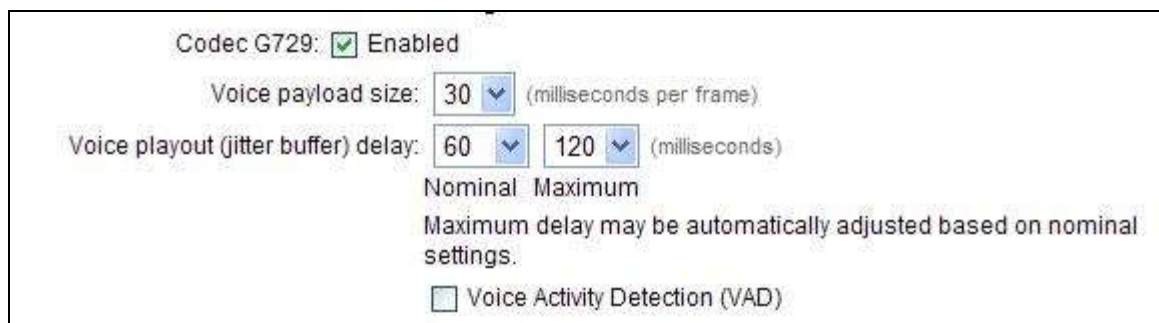
Step 3 - Use the scroll bar on the right side of the form to find the heading **Voice Codecs**. Set the **Voice payload size** to **30**. Note that **Codec G.711** is enabled by default.



The screenshot shows the 'Voice Codecs' configuration section. At the top, 'Codec G711' is checked and labeled 'Enabled (required)'. Below it, 'Voice payload size' is set to '30' (milliseconds per frame). 'Voice playout (jitter buffer) delay' has two dropdowns: 'Nominal' set to '60' and 'Maximum' set to '120' (milliseconds). A note states: 'Maximum delay may be automatically adjusted based on nominal settings.' At the bottom, 'Voice Activity Detection (VAD)' is unchecked.

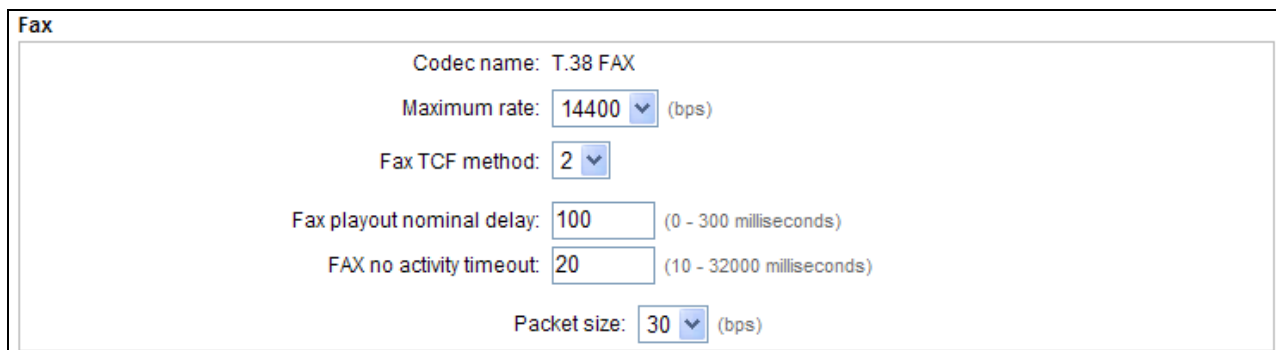
Step 4 – Scroll down to the G729 codec section and check the selection box. Set the **Voice payload size** to **30**.

Note – Although not shown, annexB=yes may be enabled by selecting the **VAD** (Voice Activity Detection) box. However, if enabled here, it should also be enabled in **Section 5.3.2**.



The screenshot shows the 'Codec G729' configuration section. 'Codec G729' is checked and labeled 'Enabled'. 'Voice payload size' is set to '30' (milliseconds per frame). 'Voice playout (jitter buffer) delay' has two dropdowns: 'Nominal' set to '60' and 'Maximum' set to '120' (milliseconds). A note states: 'Maximum delay may be automatically adjusted based on nominal settings.' At the bottom, 'Voice Activity Detection (VAD)' is unchecked.

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

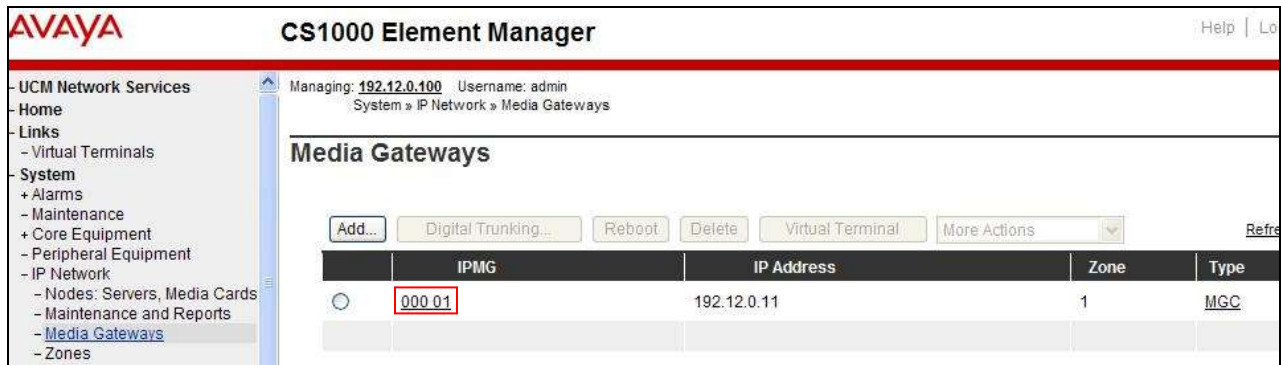


The screenshot shows the 'Fax' configuration section. 'Codec name' is 'T.38 FAX'. 'Maximum rate' is set to '14400' (bps). 'Fax TCF method' is set to '2'. 'Fax playout nominal delay' is set to '100' (0 - 300 milliseconds). 'FAX no activity timeout' is set to '20' (10 - 32000 milliseconds). 'Packet size' is set to '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).

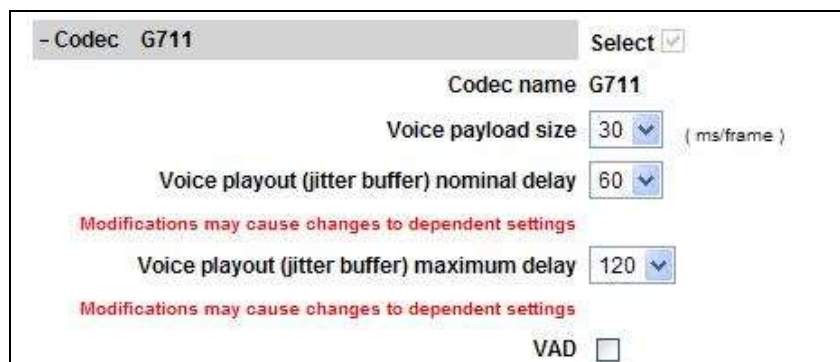


This will open the **Property Configuration** screen (not shown). Click on **Next** (not shown). This will open the **Media Gateway Controller (MGC) Configuration** screen.

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



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.



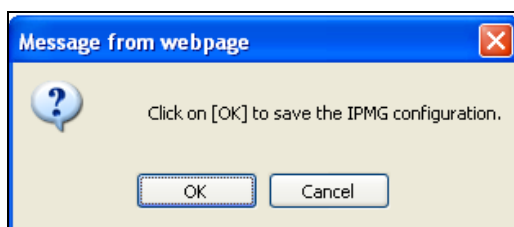
Step 4 – Scroll down, click on and expand the **Codec G729A** field. Check the selection box and set the **Voice payload size (PTIME)** to **30**.

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**.

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

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**.



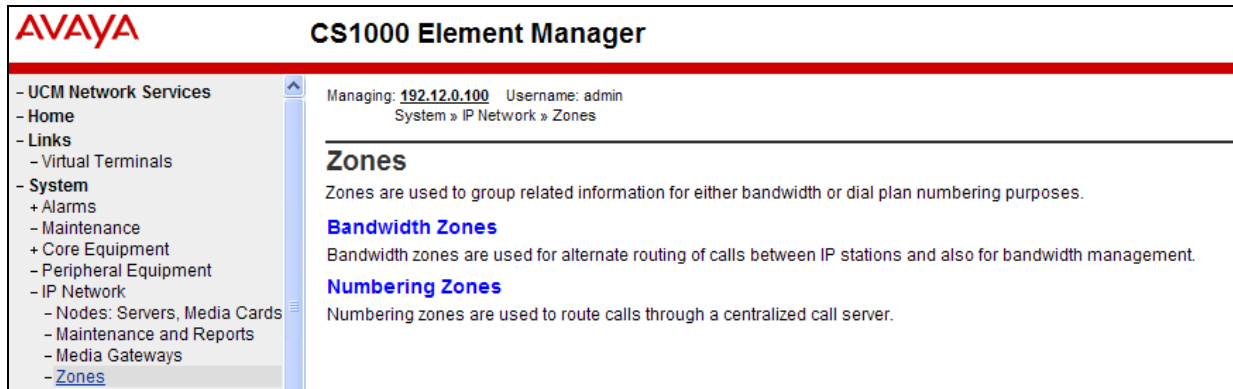
Step 8 –Select the Media Gateway ID (e.g., 000 01), and click on the **Reboot** button. The Media Gateway will reboot and deploy the new configuration.

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.



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.

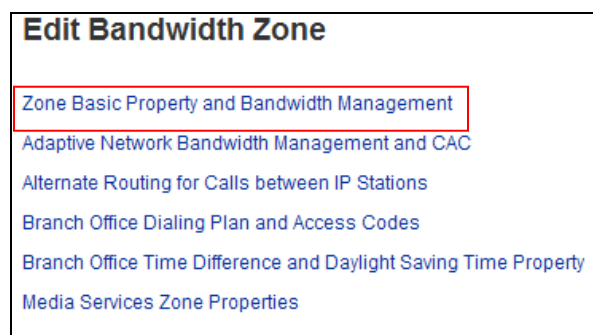
5.4.1 Zone 5 – SIP Trunk

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.



	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.



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

Submit Refresh Cancel

5.4.2 Zone 3 – IP Telephones

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

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

5.5 SIP Trunk Gateway

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

5.5.1 Provision SIP Gateway

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

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value.

Save Cancel

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

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

The values defined for the sample configuration are shown below.

Node ID: 1001 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: customera.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: SS_1001 *

Gateway password: *

Application node ID: 1001 * (0-9999)

Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below

Monitor IP: Add

Monitor addresses: Remove

* Required Value.

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

Save Cancel

Step 3 - Scroll down to the section: **SIP Gateway Settings → Proxy Or Redirect Server**. Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface (e.g., **192.168.67.47**).
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**

Note - The Secondary TLAN IP address was not used.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, and IP Network. The main content area displays the 'Node ID: 1001 - Virtual Trunk Gateway Configuration Details'. The 'SIP Gateway Settings' tab is selected, showing fields for Port (5060), Transport protocol (TCP), and Primary TLAN IP address (192.168.67.47). There are also checkboxes for 'Enable Shared Bandwidth Management', 'Support registration', and 'Primary CDS proxy'.

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

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, and IP Network. The main content area displays the 'Node ID: 1001 - Virtual Trunk Gateway Configuration Details'. The 'SIP Gateway Services' tab is selected, showing fields for Number translation (Strip, Prefix, CLID display format) and SIP URI Map (Public E.164 domain names, Private domain names). There are also checkboxes for 'SIP Converged Desktop' and 'Enable CD service'.

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

5.5.2 Integrated Services Digital Network (ISDN)

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

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

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

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

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

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

Feature Package	Package Number
Digital Private Network Signaling System 1	123
Flexible Tones and Cadences	125
Multifrequency Compelled Signaling	128
International Supplementary Features	131
Enhanced Night Service	133
Integrated Services Digital Network	145

Integrated Services Digital Network: ☒

Virtual private network identifier: (1 - 16383)

Private network identifier: (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 tree has 'Routes and Trunks' expanded, and 'D-Channels' is selected. The main area displays the 'D-Channels' configuration page. It 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 existing D-Channels: Channel 15 (Type: DCH, Card Type: DCIP, Description: VDCH) and Channel 20 (Type: DCH, Card Type: DCIP, Description: SIPLINE). Each row has an 'Edit' button.

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

D-Channels

Maintenance

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

Configuration

Choose a D-Channel Number: and type:

Channel	Type	Card Type	Description	Action
Channel: 15	Type: DCH	Card Type: DCIP	Description: VDCH	<input type="button" value="Edit"/>
Channel: 20	Type: DCH	Card Type: DCIP	Description: SIPLINE	<input type="button" value="Edit"/>

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

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

Step 3 - Scrolling down, in the **Basic Options** section, the following settings are used.

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

Step 4 - Scrolling down, in the **Advanced Options** section, the following settings are used.

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

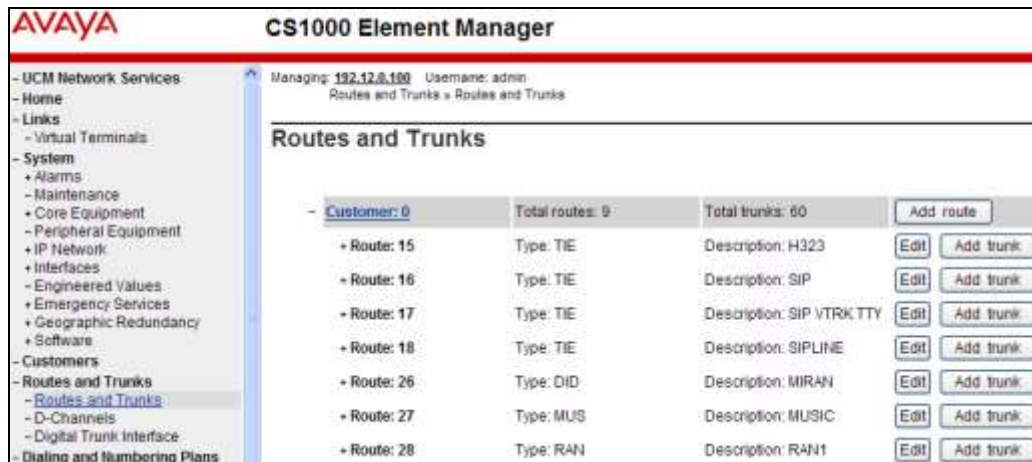
Step 5 - Click on **Submit** (not shown).

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

5.5.4 SIP Routes Configuration

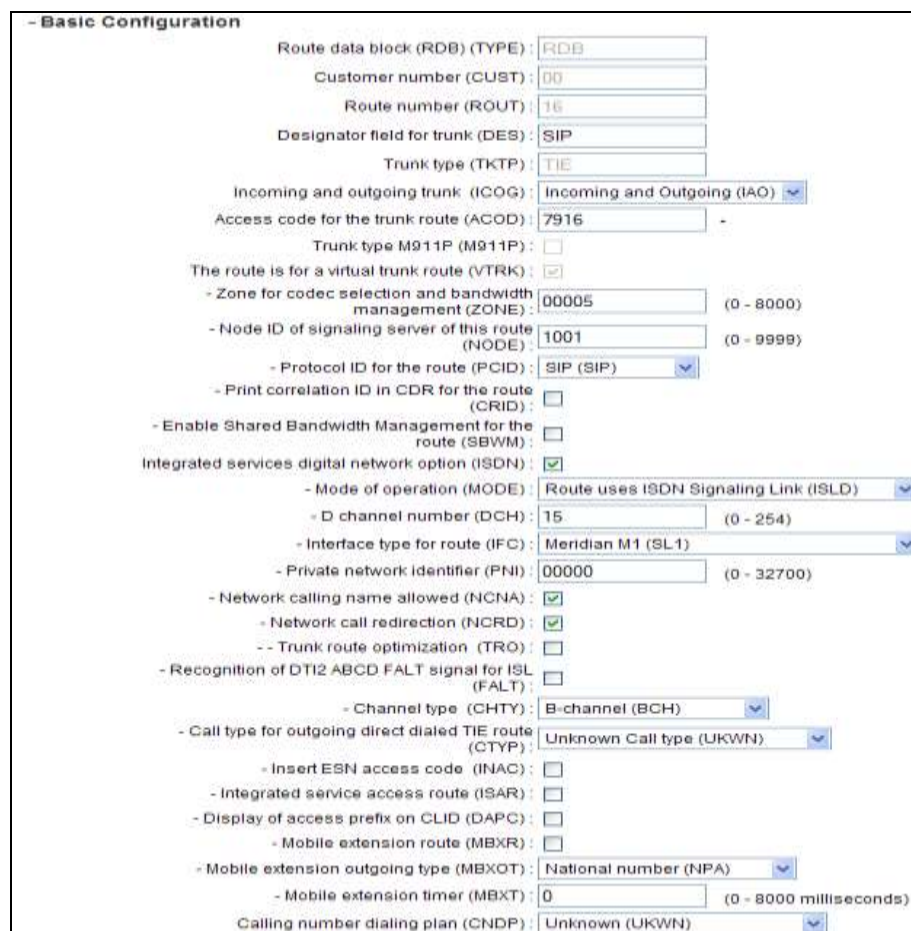
Step 1 - Select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In the reference configuration, **Customer 0** is used. Click on **Customer:0** to display defined routes, or click on **Add route**, to add additional routes.

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: 192.12.8.100 Username: admin			
Routes and Trunks > Routes and Trunks			
Routes and Trunks			
- Customer: 0	Total routes: 9	Total trunks: 60	Add route
+ Route: 15	Type: TIE	Description: H323	Edit Add trunk
+ Route: 16	Type: TIE	Description: SIP	Edit Add trunk
+ Route: 17	Type: TIE	Description: SIP VTRK TTY	Edit Add trunk
+ Route: 18	Type: TIE	Description: 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

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



- Basic Configuration

Route data block (RDB) (TYPE) : RDB

Customer number (CUST) : 00

Route number (ROUT) : 16

Designator field for trunk (DES) : SIP

Trunk type (TKTP) : TIE

Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO) ▼

Access code for the trunk route (ACOD) : 7916 -

Trunk type M211P (M211P) : ☐

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

- Zone for codec selection and bandwidth management (ZONE) : 00005 (0 - 8000)

- Node ID of signaling server of this route (NODE) : 1001 (0 - 9999)

- Protocol ID for the route (PCID) : SIP (SIP) ▼

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

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

Integrated services digital network option (ISDN) : ☒

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

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

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

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

- Network calling name allowed (NCNA) : ☒

- Network call redirection (NCRD) : ☒

- Trunk route optimization (TRO) : ☐

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

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

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

- Insert ESN access code (INAC) : ☐

- Integrated service access route (ISAR) : ☐

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

- Mobile extension route (MBXR) : ☐

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

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

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

Step 2 - Scrolling down, click on **Basic Route Options**. The following settings are used in the reference configuration.

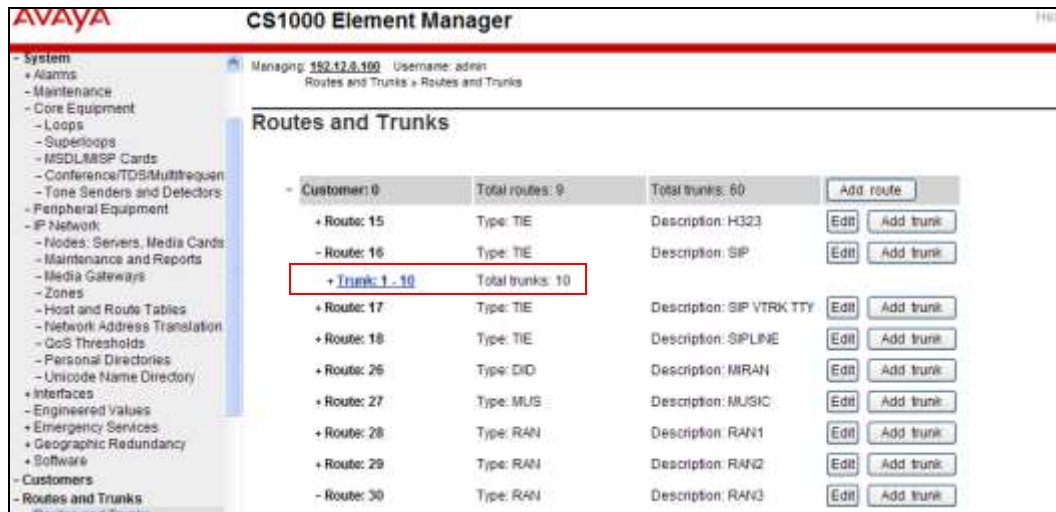
Step 3 – Going back to the screen shown in **Step 1**, select the **Edit** button next to **Route 16** to verify the configuration, as shown below. Verify **SIP (SIP)** has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.2**. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging.

Step 4 - 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).

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

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.



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



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:

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 CS1000E and Session Manager for calls destined for the AT&T IP Flexible Reach service. The routing defined in this section is simply an example and not intended to be prescriptive. The example will focus on the configuration enabling a 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.

AVAYA CS1000 Element Manager

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

Electronic Switched Network (ESN)

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

Left Panel:

- 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

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

AVAYA CS1000 Element Manager

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

Route List Blocks

Please enter a route list index (0 - 1999)

- + Route List Block Index -- 10
- + **Route List Block Index -- 15**
- + Route List Block Index -- 16
- + Route List Block Index -- 17
- + Route List Block Index -- 18
- + Route List Block Index -- 19
- + Route List Block Index -- 20

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 Control & Services » Route List Block

Route List Block

General Properties

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

Please choose the

- + **Data Entry Index -- 0**
- + Data Entry Index -- 1

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:

Indexes

Time of Day Schedule:

Facility Restriction Level: (0 - 7)

Digit Manipulation Index: 15

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

Free Calling Area Screening Index:

Free Special Number Screening Index:

Business Network Extension Route: ☐

Incoming CLID Table: (0 - 0)

Options

Local Termination entry: ☐

Route Number: 16

Skip Conventional Signaling: ☐

Use Tone Detector: ☐

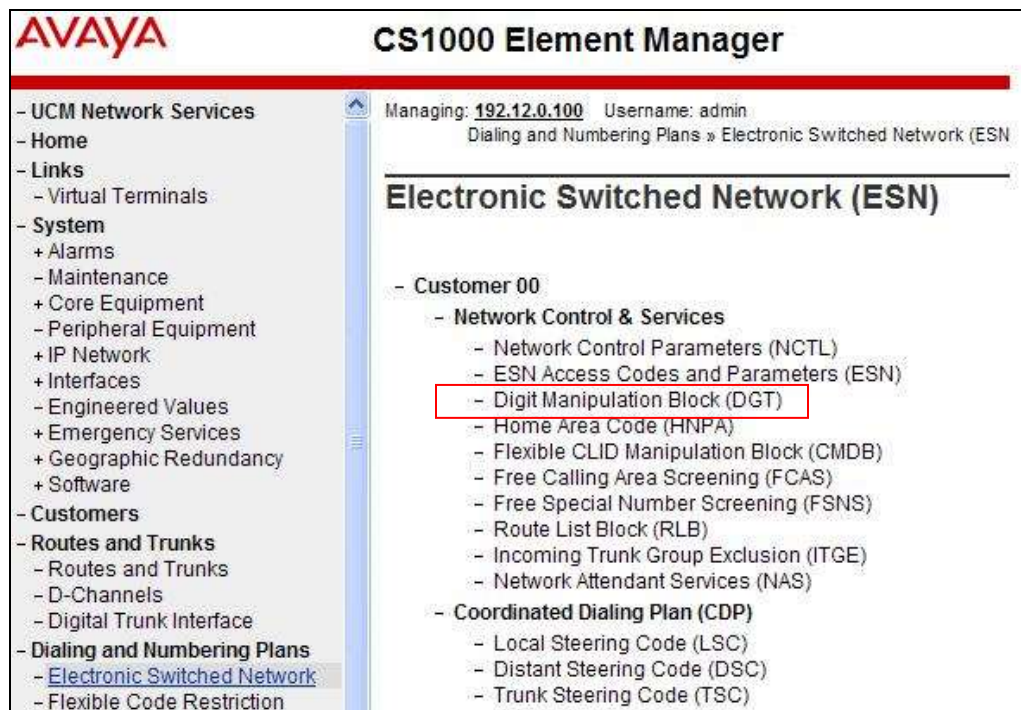
Conversion to LDN: ☐

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**.

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

Digit Manipulation Block List

Please choose the Digit Manipulation Block Index 3 to Add

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

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

Digit Manipulation Block

Digit Manipulation Index numbers: 15

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

Insert:

IP Special Number : ☐

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

Submit Refresh Delete Cancel

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).

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1:

NARS Access Code 2:

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

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

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

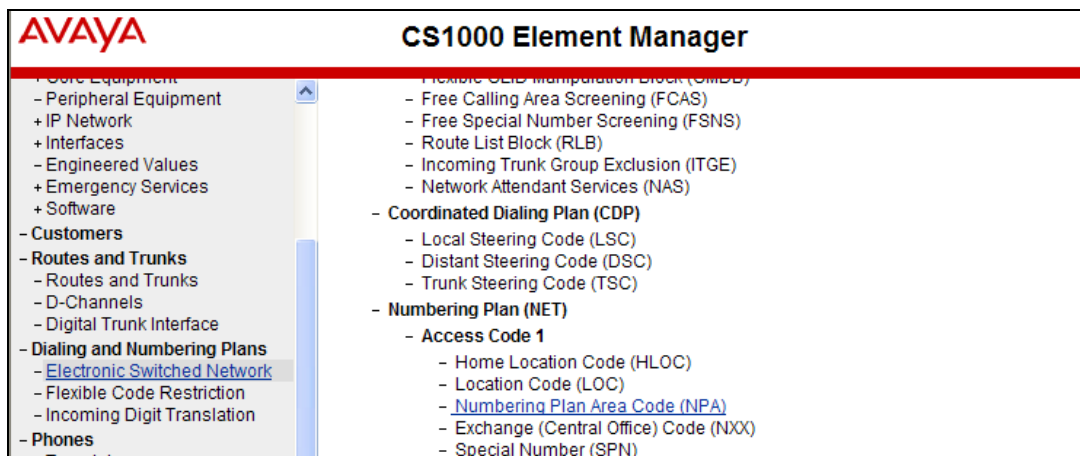
Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☒

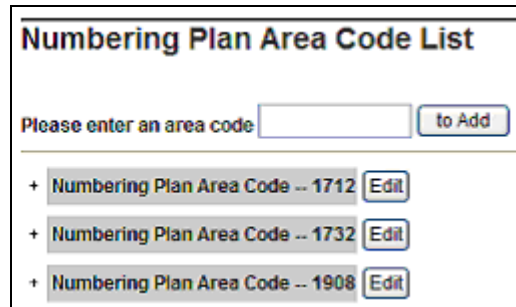
5.6.4 Numbering Plan Area Codes

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.

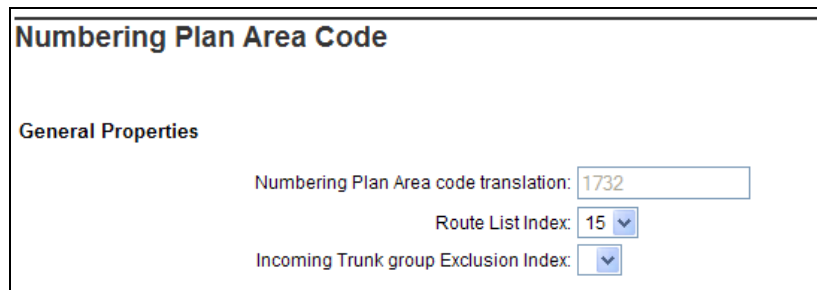


Step 2 - Add a new **NPA** by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured.



The screenshot shows a window titled "Numbering Plan Area Code List". At the top, there is a text input field labeled "Please enter an area code" followed by a "to Add" button. Below this, there is a list of three entries, each with a plus icon, the text "Numbering Plan Area Code --", a value, and an "Edit" button. The entries are: "1712", "1732", and "1908".

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



The screenshot shows a window titled "Numbering Plan Area Code". Under the "General Properties" section, there are three fields: "Numbering Plan Area code translation:" with a text input field containing "1732", "Route List Index:" with a dropdown menu showing "15", and "Incoming Trunk group Exclusion Index:" with a dropdown menu.

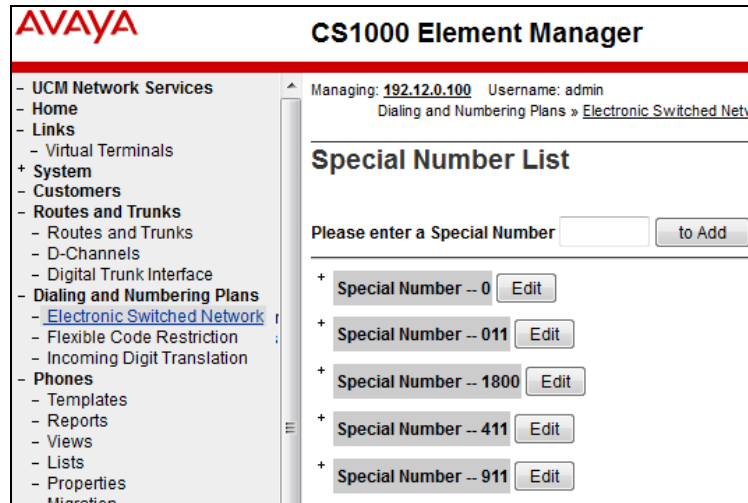
5.6.5 Other Special Numbers to Route to Session Manager

Service numbers such as **0** (operator), **x11** (information/emergency), **011** (international), and **18xx** (toll free) calls were also routed to Session Manager and ultimately to the IPFR-EF service. Although not intended to be prescriptive, the method used in the reference configuration is described below.

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.



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. Click on **Submit** (not shown).

Special Number (011)

General Properties

Route list index: 15

Incoming trunk group exclusion index:

5.7 Routing of Inbound Numbers to CS1000E

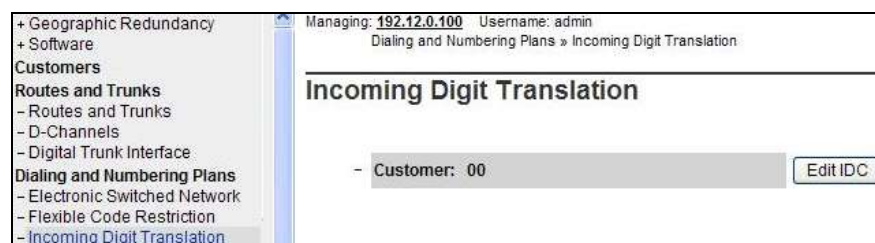
Calls from PSTN will dial IPFR-EF DID numbers to reach stations on CS1000E. The IPFR-EF service will then deliver associated DNIS numbers, in SIP Invite messages, to the CPE. These DNIS numbers are converted to the associated extensions by the CS1000E Incoming Digit Translation (IDT) table.

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.

Note – In the reference configuration, although AT&T assigned 10 digit DID numbers (e.g., 732555xxxx), the IPFR-EF service delivered 7 digit DNIS numbers (e.g., 555xxxx). Therefore the 7 digit number is used for call routing in the CPE, but the 10 digit number is used for CPE caller identification (e.g., PAI).

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

Step 2 – Select the appropriate **Customer ID** (e.g., 00) and click on **Edit IDC**.



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

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

Customer 00 Incoming Digit Conversion Property

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

[Refresh] [Cancel]

Step 4 – The IDC Tree form will open. Click on the **Add** button. In the **Incoming Digits** field, enter an IPFR-EF DNIS number (e.g., **5553170**). In the **Converted Digits** field, enter the associated CS1000E extension (e.g., **4095**). Allow the other fields to default. Click on **Save**.

AVAYA CS1000 Element Manager

Managing: 192.12.0.100 Username: admin
Dialing and Numbering Plans > Incoming Digit Translation > Customer 00 > Digit Conversion Tree 1 Configuration > Add Incoming Digits

Add Incoming Digits

Incoming Digits: 5553170
Converted digits: 4095 (a - 5553170)

Force storage or removal of data: ☐

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

CPND language: ☒ Roman characters

CPND Name:

Expected length:

Display format: First name, Last name

☐ Katakana characters

CPND Name:

Expected length:

Display format: First name, Last name

[Save] [Cancel]

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

[Add...] [Delete IDC] [Delete IDC tree]

	Incoming Digits	Converted Digits	CP
1	5553170	4095	
2	5553171	4093	
3	5553172	4099	*
4	5553176	4096	*
5	5553177	2090	*

Note – Due to the issue described in **Section 2.2, Item 10**, Session Manager must modify the DNIS digits that the CS1000E places in the PAI headers. See **Section 6.3.1**.

5.8 Enabling Plug-Ins for Call Transfer Scenarios

Plug-Ins allow specific 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, 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.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is 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, 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, and Loadware PEPs. The main area displays a message 'An internal error has occurred! Severity:Major' and buttons for 'Enable' and 'Disable'. Below this is a table of Plug-Ins.

<input type="checkbox"/>	Number	Description	MPLR Number	Status
86	223	PI:ICUM REJECTS QSIG CUBS REQUEST WITH NO CALLING NUMBER	MPLR12290	Disabled
87	224	PI:No busy treatment on external transfer through application if OUT_T306 > 0	MPLR24676	Disabled
88	225	PI:PKG 179, Taurus, electronic look, Mail and CallPilot softkeys	MPLR22389	Disabled
89	226	PI:ACLDID should display more than 10 digits	MPLR15783	Disabled
90	228	PI: TTY 0 on CPU card (8/1/N) causes cursor to go up on VDU	MPLR07613	Disabled
91	230	PI: Unplugged telset disables after midnight routines.	MPLR11700	Disabled
92	231	PI: BRI 64K data not possible over DTI2. With mix of spans (both DTI and DTI2) THIS is not supported.	MPLR10878	Disabled
93	232	PI: QSIG GF: No diverting and originally called number in DL12 APDU on calls from MCDN TRO-BA.	MPLR24273	Disabled
94	233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506	Disabled
95	235	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
96	500	NO DESCRIPTION	MPLR21979	Disabled
97	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Enabled

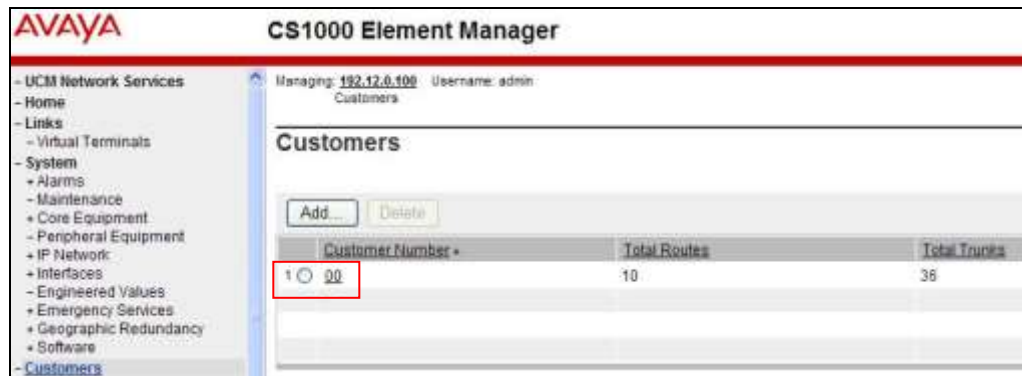
5.9 Customer Information

In the reference configuration, specific calling number information is required based on the destination of the call. For Calls to the IPFR-EF service, AT&T assigned DID's are required in the From and PAI headers.

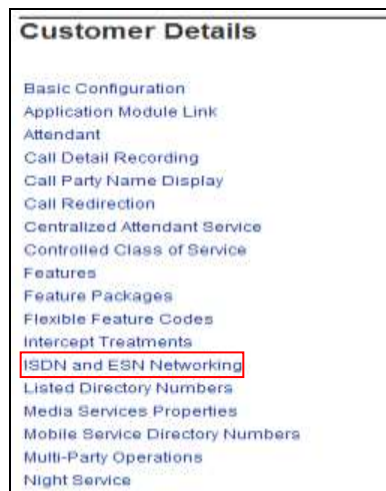
5.9.1 Calling Number Provisioning for calls to the AT&T IP Flexible Reach Service

The IPFR-EF 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 (e.g., 732555xxxx).

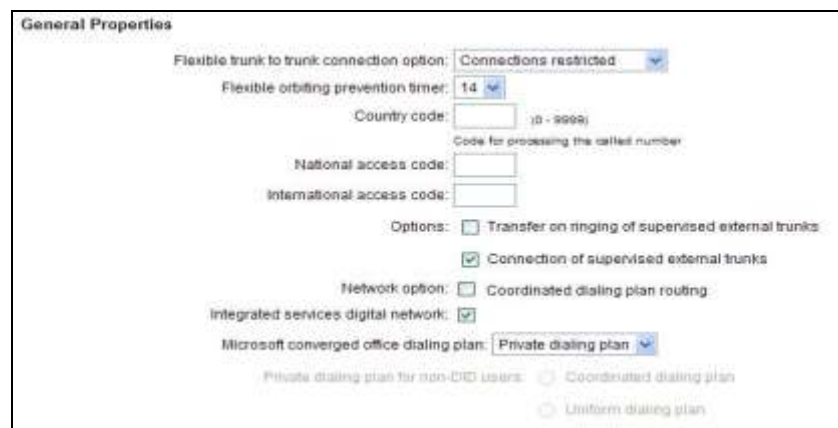
Step 1 - Select **Customers** from the left navigation menu, and click on the appropriate **Customer Number** (e.g., 00)



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



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



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

The **Calling Line Identification Entries** table will open.

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

Click on **Add** to create a new entry, or click on any existing **Entry Id** to view or make changes (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 as the calling number.

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

5.10 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 Sample IP UNISTim Phone DN 4095

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**).

Step 3 - Click on **Search**.

Step 4 - The system will respond with the phone information. Click on the TN value (e.g., **096 0 01 06**).

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.

Phone Details

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

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

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

Zone: *

Key Expansion Modules: *

5.10.1.1 Features

Scroll further down the **Phone Details** form and locate the **Features** section of the form. In this section, various CS1000E telephone features are defined. 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 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
CFIA	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 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 – Scroll through the Feature options and set the **FDN** (*Flexible Call Forward No Ans DN*) feature to the Call Pilot access extension (e.g., **2090**).

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., **2090**).

Feature	Description
FDN	Flexible Call Forward No Ans DN 2090
FNA	Call Forward No Answer Allowed
HUNT	Hunt DN - All Calls, or Internal Calls for CFTA 2090

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

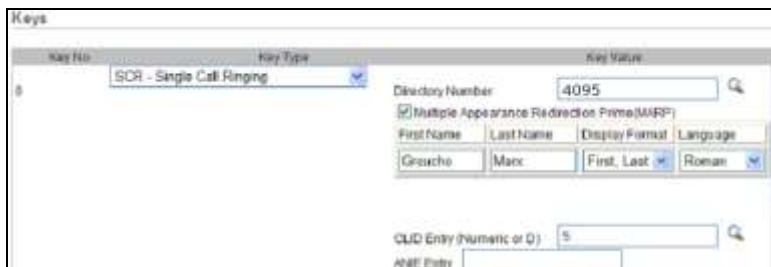
5.10.1.2 Keys

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 4095 was assigned CLID 5 and therefore will use 7325554386 as its calling number.



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 CS1000E will dial to reach the messaging system (e.g., Call Pilot extension **2090**).

15	MWK - Message Waiting	Message Center DN	2090
<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 for this station.

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

5.10.1.3 Saving Changes

Once all changes have been made, at the bottom of the form, click on **Save** (not shown).

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	
 <div>System: 601 on c0407</div> <div>Phone Type: 2500</div> <div>Sync Status: TRM</div>	
General Properties Features Analog Line Features Mail Fields <div>Custom View: All</div>	
General Properties	
Customer Number	
Terminal Number	000 7 10 00
Designation	ANALOG (10 characters)
Directory Number	2779
CLID entry	

5.11 Changing RFC2833 DTMF Telephone Event Type

The CS1000E uses RFC2833 DTMF Telephone Event type 101. The IPFR-EF service recommends the value 100 (see **Section 2.2, Item 7**). Therefore the CS1000E value is changed to 100 as follows:

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

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

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

```
Password:
```

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

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

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

```
pdt> setRFC2833PT 100
```

The system will respond with the pdt> prompt.

```
pdt>
```

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

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

5.12 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 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**.



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.



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

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

6 Configure Avaya Aura® Session Manager Release 6.3

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

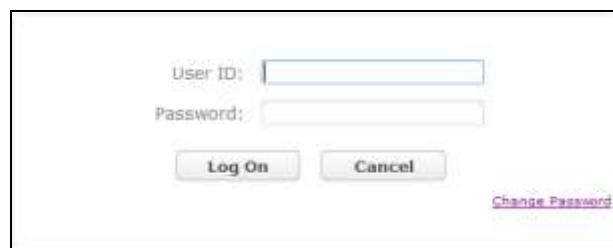
Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information, consult the references in **Section 11**.

The following administration activities will be described:

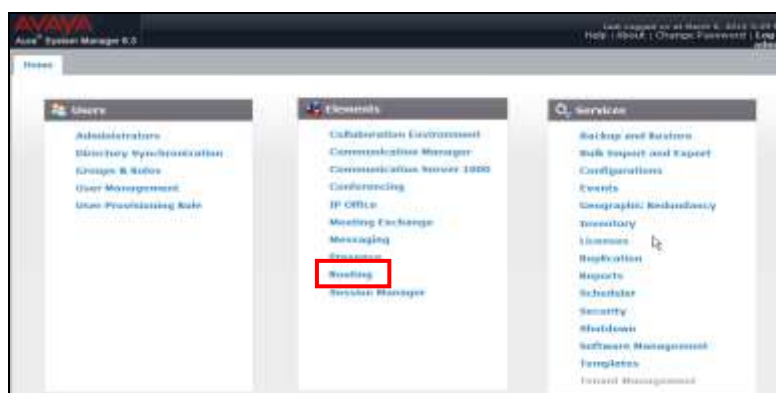
- Define SIP Domain
- Define Locations for CS1000E and for the Avaya SBCE
- Configure the Adaptation Modules that will be associated with the SIP Entities for CS1000E and the Avaya SBCE
- Define SIP Entities corresponding to CS1000E and Avaya SBCE
- Define Entity Links describing the SIP trunk between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

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

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



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



6.1 SIP Domain

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

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



6.2 Locations

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

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

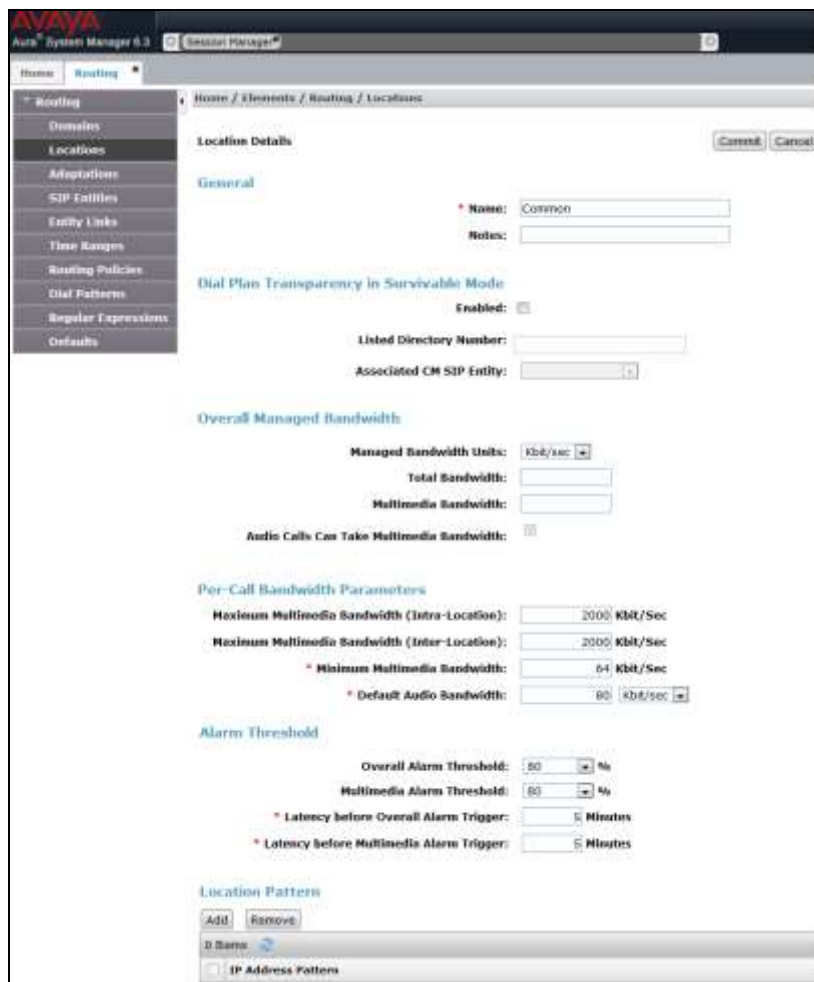
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown).

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

- **Name:** Enter a descriptive name for the location (e.g., **Common**).
- Use default values for remaining fields.

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

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



6.3 Configure Adaptations

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

- **DiversionTypeAdapter** – This adaptation is used to convert History-Info headers sent by the CS1000E in Call Forward scenarios to AT&T (which requires the use of Diversion header with Call Forward).
- **CS1000Adapter** – This adaptation is used to provide translation between various CS1000E generated headers, into formats used by other Avaya products and endpoints.
- **DigitConversionAdapter** – This adaptation modifies digit strings in the Request-URI. While this adaptation is not specified specifically in the reference configuration, its functionality is included as part of all other adaptations.

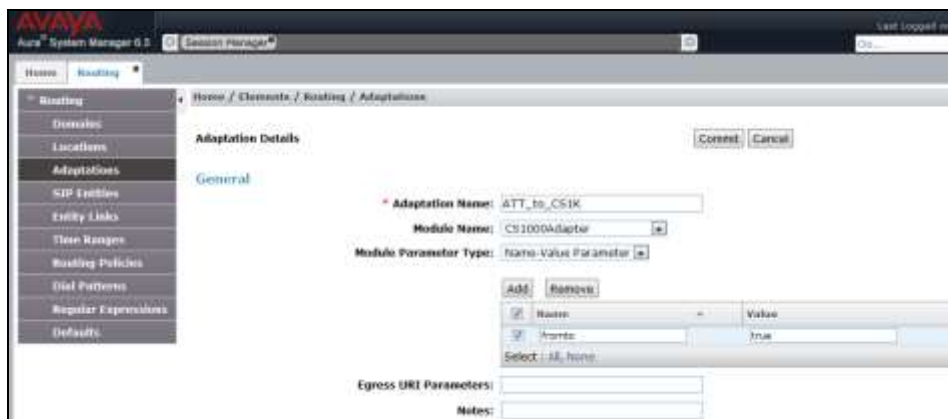
In addition, Module parameters **odstd** (to modify destination domain or IP addressing), **osrcd** (to modify source domain or IP addressing), **MIME=no** (to remove unnecessary CS1000E MIME headers), and **fromto=true** (to modify the From and To headers) are specified.

6.3.1 Adaptation for Calls to the 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 Type:** Select **Name-Value Parameter**
- Click on **Add** and the Module option fields will open. Enter the following:
 - In the **Name** field enter **fromto**
 - In the **Value** field enter **true**.
- Click on **Commit**.

Note – The **fromto** parameter is set so that destination user information is copied from the R-URI into the To header for inbound calls to Call Pilot.



Step 2 - In the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from AT&T to the CS1000E. In some call scenarios the CS1000E may insert local extensions in the PAI headers of responses or ReInvites. Session Manager will replace the local extension with its corresponding IPFR-EF 10 digit DID access number in the PAI header.

- **Matching Pattern** Enter a CS1000E extension (e.g., **4095**).
- **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., **7325553170**).
- **Address to modify** Enter **both**.
- Repeat for all extension/IPFR-EF number associations.

Note – In the reference configuration, although AT&T assigned 10 digit DID numbers (e.g., 732555xxxx), the IPFR-EF service delivered 7 digit DNIS numbers (e.g., 555xxxx). Therefore the 7 digit number is used for call routing in the CPE, but the 10 digit number is used for CPE caller identification (e.g., PAI).

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 2090	* 4	* 4		* 4	7325553177	both		Call Pilot PAI
* 2810	* 4	* 4		* 4	7325553178	both		Fax PAI
* 4093	* 4	* 4		* 4	7325553171	both		Digital PAI
* 4095	* 4	* 4		* 4	7325553170	both		UNISlim PAI
* 4099	* 4	* 4		* 4	7325553172	both		SIP PAI

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

Note that incoming AT&T calls to CS1000E stations have the inbound DNIS digits converted to their associated local extensions in the CS1000E **Incoming Digit Translation** table (e.g., AT&T DNIS 5553170 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., 5553177) must be converted to the Call Pilot local access extension (2090). However for Call Pilot to accept the call, the DNIS digits must be changed to 10 digits. The **fromto=true** Module Parameter specified in **Step 1** above, triggers this conversion by entering 7325553177 in the table..

- **Matching Pattern** Enter IPFR-EF DIDs (e.g., **5553177**).
- **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 **destination**.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 7327373177	* 10	* 10		* 10	2090	destination		Call Pilot

Step 4- Click **Commit** (not shown) so save changes to the form.

6.3.2 Adaptation for calls from the CS1000E to AT&T

The message body of an INVITE message sent from the 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. 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 IPFR-EF service for Call Forward scenarios. Note that the Avaya SBCE is used to remove and/or alter additional SIP headers sent by the CS1000E (see **Sections 7.2.3 and 7.3.3**).

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

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., **CS1K_to_ATT**).
- **Module Name:** Select **DiversionTypeAdapter** from drop-down menu (or add an adapter with name **DiversionTypeAdapter** if not previously defined)
- **Module Parameter Type:** Select **Name-Value Parameter** from the drop down menu, then enter the following parameters:
 - In the **Name** field enter **MIME**.
 - In the **Value** field enter **no**.

Note – Neither **Digit Conversion for Incoming Calls to SM** nor **Conversion for Outgoing Calls from SM Digit** were required in the reference configuration for the Avaya SBCE SIP Entity form.

The screenshot shows the 'Adaptation Details' form in the Avaya SIP Entity configuration interface. The form is divided into several sections:

- General:** Contains fields for 'Adaptation Name' (CS1K_to_ATT), 'Module Name' (DiversionTypeAdapter), and 'Module Parameter Type' (Name-Value Parameter). Below these are 'Add' and 'Remove' buttons, a table for parameters, and 'Egress URI Parameters' and 'Notes' fields.
- Digit Conversion for Incoming Calls to SM:** Includes 'Add' and 'Remove' buttons and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes.
- Digit Conversion for Outgoing Calls from SM:** Similar to the incoming section, with 'Add' and 'Remove' buttons and a table with the same columns.

The parameter table in the General section contains one entry:

Name	Value
MIME	no

6.4 SIP Entities

SIP Entities are added for CS1000E and Avaya SBCE. A SIP Entity is created for Session Manager as part of the Session Manager installation, so its configuration is shown in this section as well for completeness.

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

6.4.1 SIP Entity for the CS1000E

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

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

- **Name:** Enter an identifier for the SIP Entity (e.g., **CS1K**).
- **FQDN or IP Address:** Enter the TLAN IP address of the CS1000E SIP GW.
- **Type:** Select **Other**
- **Adaptation:** Select the Adaptation Module defined in **Section 6.3.1**.
- **Location:** Select the Location defined in **Section 6.2**.

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

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

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

The screenshot shows the Avaya System Manager 6.3 configuration interface for a SIP Entity. The left navigation pane includes options like Routing, Domains, Locations, Adaptation, SIP Entities, Entity Links, Time Ranges, Routing Policies, Mail Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and 'General'. Fields include Name (CS1K), FQDN or IP Address (172.16.6.110), Type (Other), Adaptation (ATT_30_CS1K), Location (Common), Time Zone (America/New_York), SIP Timer S/T (On seconds) (4), Credential name, Call Detail Recording (None), and Codec Profile Type Preference. Below these are sections for Loop Detection (Loop Detection Mode: Off), SIP Link Monitoring (SIP Link Monitoring: Use Session Manager Configuration), Supports Call Admission Control, Shared Bandwidth Manager, Primary Session Manager Bandwidth Association, and Backup Session Manager Bandwidth Association. The Entity Links section has an 'Override Port & Transport with DNS SRV' checkbox. At the bottom, there are tables for 'SIP Responses to an OPTIONS Request' and 'SIP Responses to an OPTIONS Request' with columns for Response Code & Reason Phrase, Mark Entity Up/Down, and Notes.

6.4.2 SIP Entity for the Avaya SBCE

Repeat the steps in Section 6.4.1 with the following changes:

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

The screenshot shows the 'SIP Entity Details' configuration window for an entity named 'A-SBCE'. The window is divided into several sections: General, Loop Detection, SIP Link Monitoring, Entity Links, and SIP Responses to an OPTIONS Request. The General section contains fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, SIP Timer B/F, Credential name, Call Detail Recording, and CommProfile Type Preference. The Loop Detection section has a Loop Detection Mode dropdown. The SIP Link Monitoring section has a SIP Link Monitoring dropdown and checkboxes for Supports Call Admission Control and Shared Bandwidth Manager. The Entity Links section has an Override Port & Transport with DNS SRV checkbox. The SIP Responses to an OPTIONS Request section has an Add button and a table for responses.

SIP Entity Details [Commit] [Cancel]

General

* Name: A-SBCE

* FQDN or IP Address: 192.168.70.120

Type: Other

Notes:

Adaptation: CS1K_to_ATT

Location: Common

Time Zone: America/New_York

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove

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

SIP Responses to an OPTIONS Request

Add Remove

0 Items

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

6.4.3 SIP Entity for Session Manager

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

The screenshot shows the 'SIP Entity Details' form with the following sections and fields:

- General**
 - Name: sm63
 - FQDN or IP Address: 192.168.67.47
 - Type: Session Manager
 - Notes: (empty)
 - Location: Common
 - Outbound Proxy: (empty)
 - Time Zone: America/New_York
 - Credential name: (empty)
- SIP Link Monitoring**
 - SIP Link Monitoring: Use Session Manager Configuration
- Entity Links**
 - Buttons: Add, Remove
 - Table with columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service. Filter: Enable.
 - Footer: Select: All, None; Page 1 of 2
- Port**
 - TCP Failover port: (empty)
 - TLS Failover port: (empty)
 - Buttons: Add, Remove
 - Table with columns: Port, Protocol, Default Domain, Notes. Filter: Enable.
 - Footer: Select: All, None
- SIP Responses to an OPTIONS Request**
 - Buttons: Add, Remove
 - Table with columns: Response Code & Reason Phrase, Mark Entity Up/Down, Notes. Filter: Enable.
 - Footer: 0 Items

6.5 Entity Links

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

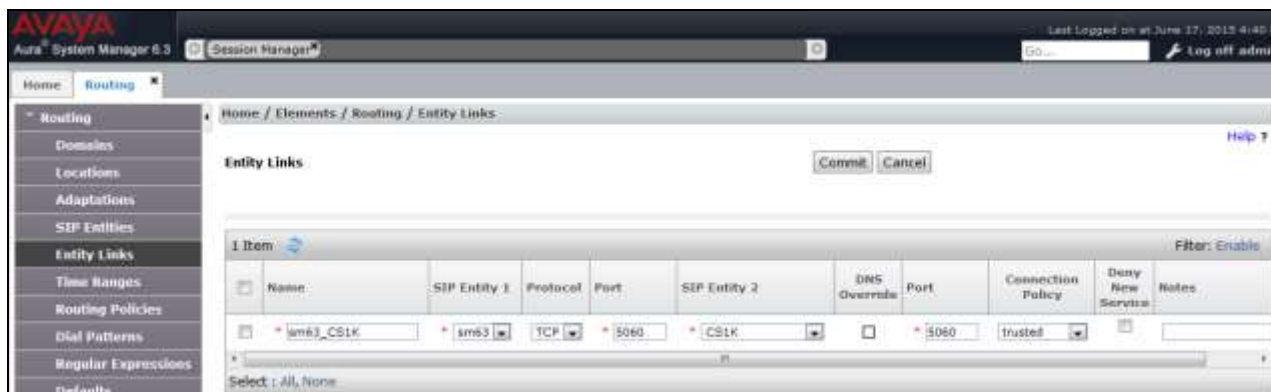
Note – As mentioned previously, Entity Links created for the CS1000E and the Avaya SBCE will appear on their corresponding CS100E and Avaya SBCE SIP Entity forms. In addition, they will also appear on the Session Manager SIP Entity form.

6.5.1 Entity Link to CS1000E Entity

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

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

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



6.5.2 Entity Link to the Avaya SBCE

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



6.6 Routing Policies

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

6.6.1 Routing Policy to the 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 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.

Step 4 - Use default values for remaining fields.

Step 5 - 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.

6.6.2 Routing Policy to the Avaya SBCE

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

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

6.7 Dial Patterns

Dial patterns are used to route calls to the appropriate routing policies, and ultimately to the appropriate SIP Entities.

Note - The dialed AT&T DID numbers may not be the same as the AT&T DNIS numbers sent in the SIP Request-URI headers. The DNIS numbers used in the Request-URIs are the numbers to be defined here in the **Pattern** fields. As mentioned previously, in the reference configuration, the IPFR-EF service sent 7 digit DNIS numbers (555-xxxx).

6.7.1 Inbound AT&T calls to the CS1000E

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

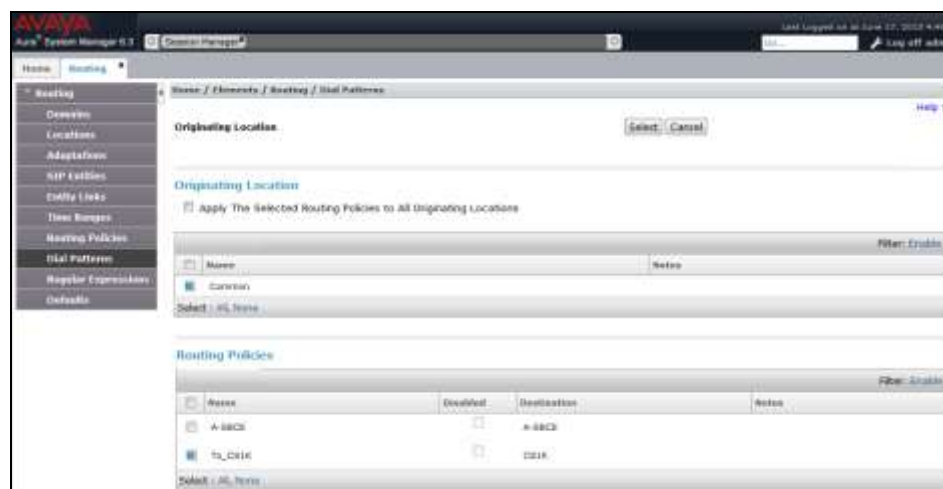
Step 2 - In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to the 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 **All**
- **Notes:** Enter a brief description. [Optional]

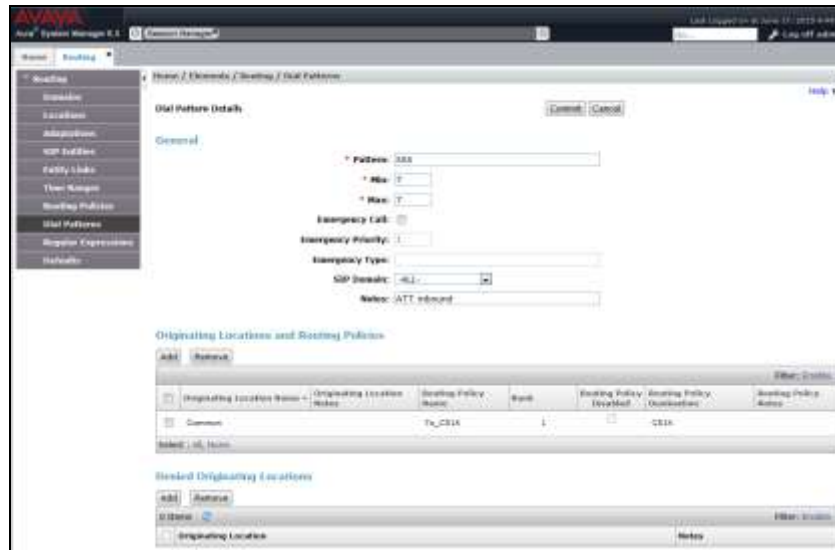
Step 3 - In the **Originating Locations and Routing Policies** section, click **Add**.

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

- In the **Originating Location** list, select the location defined in **Section 6.2**.
- In the **Routing Policies** table, select the Routing Policy defined for CS1000E in **Section 6.6.1**.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.



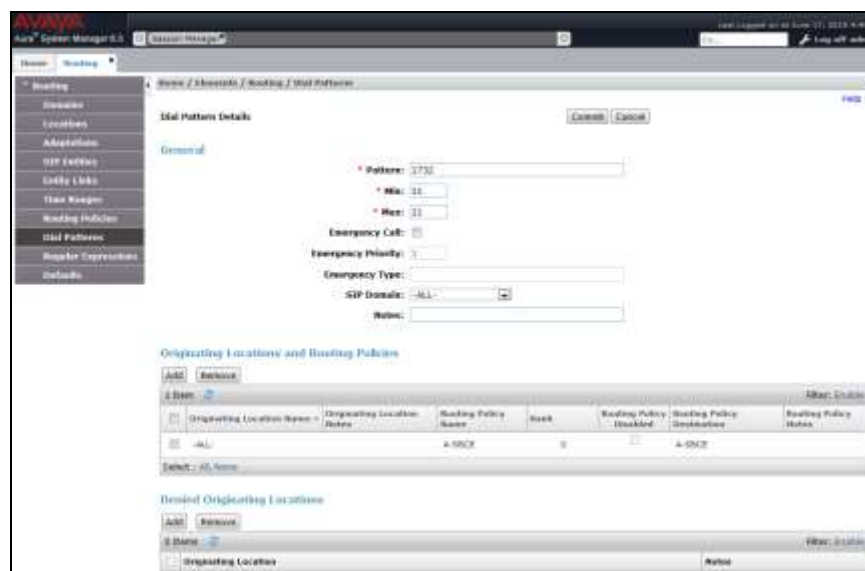
Step 5 - Click **Commit** to save. Repeat this procedure as needed for any other patterns sent to the CS1000E.



6.7.2 Outbound Calls to AT&T

Step 1 - Repeat the steps in **Section 6.7.1** with the following changes:

- **Pattern:** Enter dial pattern for calls destined to PSTN via the AT&T network (e.g., 1732).
- **Min:** Enter the minimum number of digits (e.g., 11).
- **Max:** Enter the maximum number of digits (e.g., 11).
- 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**.



Step 2 - Repeat this procedure as needed for additional PSTN numbers to be routed to PSTN/AT&T network, (e.g., Toll Free calls – **1800** with Min/Max = **11**, International calls – **011** with Min = **12**, Max = **16**).

7 Configure Avaya Session Border Controller for Enterprise

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

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

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

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

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

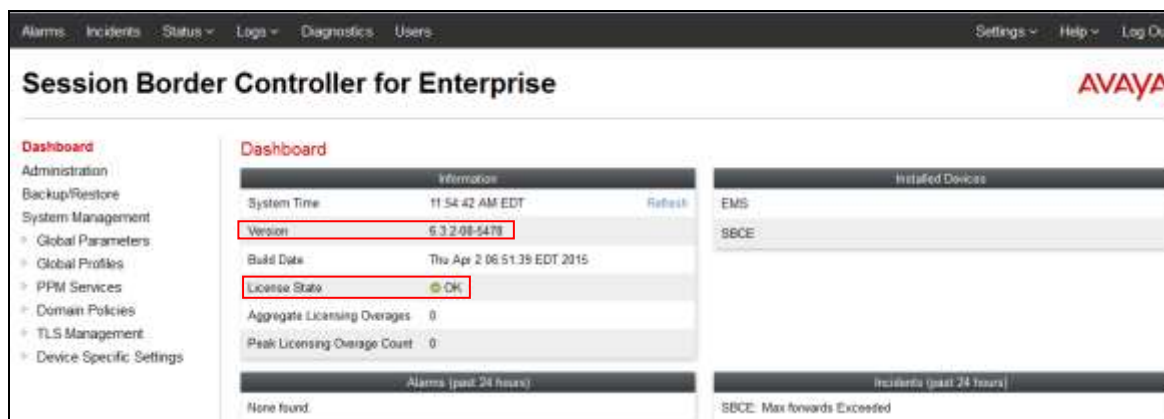
Step 1 - Access the web interface by typing “https://x.x.x.x” (where x.x.x.x is the management IP address of the Avaya SBCE).

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

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

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

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



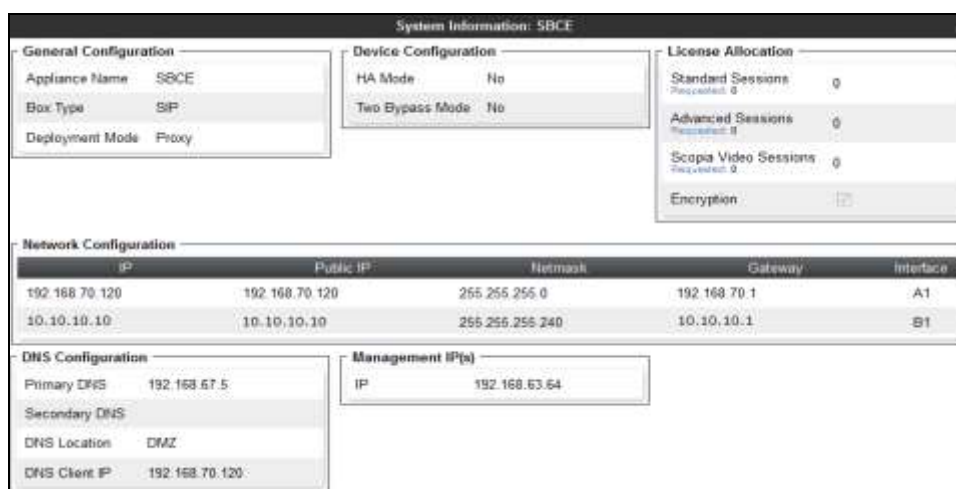
7.1 System Management/Status

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

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



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



7.2 Global Profiles

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

7.2.1 Server Interworking – Avaya

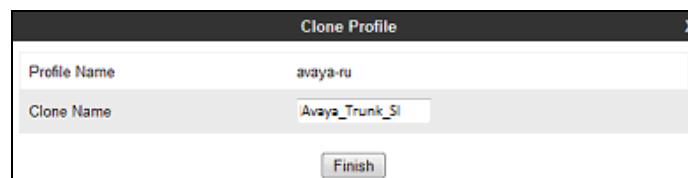
Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Session Manager.

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

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



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



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



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

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

The screenshot shows the 'Editing Profile: Avaya_Trunk_SI' window with the 'General' tab selected. The window contains various configuration options for SIP and T38. The 'T38 Support' option is checked, and the 'Next' button is at the bottom right.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC3254 - c=0.0.0 <input type="radio"/> RFC3254 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Tox Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3251 <input type="radio"/> RFC2543

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

The screenshot shows the 'Editing Profile: IPO_SI' window with the 'Privacy/DTMF' tab selected. The window contains options for Privacy and DTMF. The 'Finish' button is at the bottom right.

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

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

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

The screenshot shows a window titled "Editing Profile: IPO_SI" with a close button (X) in the top right corner. The window contains a list of configuration options, each with a checkbox or radio button. The options are:

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

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

7.2.2 Server Interworking – AT&T

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

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

7.2.3 Signaling Manipulation

Note – The use of Signaling Manipulation scripts demands higher processing requirements for the Avaya SBCE. Therefore, the use of Signaling Rules (**Section 7.3.3**) is the preferred method for header/message manipulation. Signaling Manipulations should only be used in cases where the use of Signaling Rules does not meet the desired result. Refer to [8] for information on the Avaya SBCE scripting language.

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

- Remove the Telephone Event 111 sent by the CS1000E (see **Section 2.2, item 7**).
- Modify AT&T Maxptime=30 to Ptime=30 (see **Section 2.2, item 3**).
- Remove Remote-Address headers added by the Avaya SBCE (see **Section 2.2, item 5**).

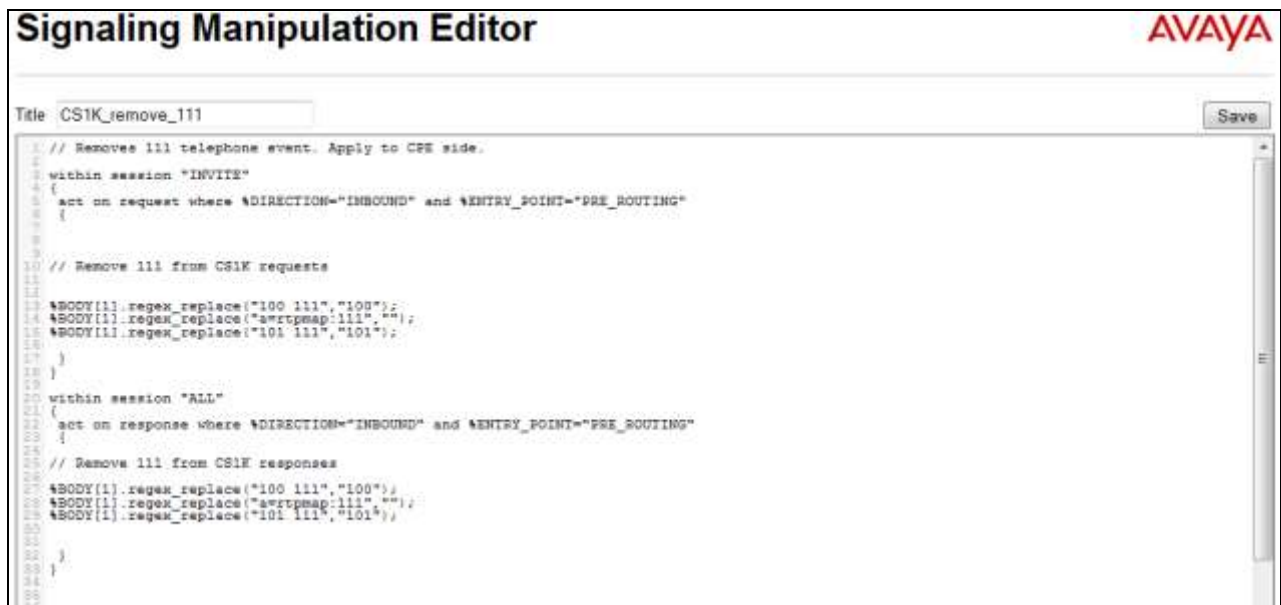
7.2.3.1 Remove Telephone Event 111

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

Step 2 - Select **Signaling Manipulation**.

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

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



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

7.2.3.2 Modify Maxptime and Remove Remote-Address

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



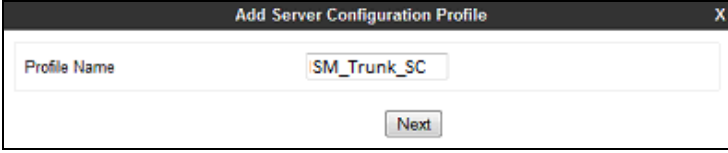
This script is applied to the AT&T Server Configuration in **Section 7.2.5**.

7.2.4 Server Configuration – Session Manager

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

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

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



The screenshot shows a window titled "Add Server Configuration Profile". It has a text input field labeled "Profile Name" containing the text "SM_Trunk_SC". Below the input field is a "Next" button.

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

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



The screenshot shows a window titled "Edit Server Configuration Profile - General". It contains a message: "Server Type can not be changed while this Server Configuration profile is associated to a Server Flow." Below this is a "Server Type" dropdown menu set to "Call Server". To the right of the dropdown is an "Add" button. Below the dropdown is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "192.168.67.47", "5060", and "TCP". To the right of the table is a "Delete" button.

IP Address / FQDN	Port	Transport
192.168.67.47	5060	TCP

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

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

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

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

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



The screenshot shows a window titled "Edit Server Configuration Profile - Advanced". It contains several settings:

- Enable DoS Protection**: ☐
- Enable Grooming**: ☒
- Interworking Profile**: Avaya_Trunk_SI
- TLS Client Profile**: AvayaSBCEClient
- Signaling Manipulation Script**: CS1K_remove_111
- Connection Type**: SUBID

At the bottom is a "Finish" button.

7.2.5 Server Configuration – AT&T

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

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

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

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

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

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

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

IP Address / FQDN	Port	Transport
12.194.131.41	5060	UDP

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	CS1K_maxptime_Remote_Address
Connection Type	SUBID

7.2.6 Routing – To Session Manager

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

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

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

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

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

Profile : SM_RP - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	SM_Trunk_SC	192.168.67.47:5060 (TCP)	None

Delete

7.2.7 Routing – To AT&T

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

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

Profile : ATT_RP - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>

Add

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

Delete

Finish

Routing Profiles: ATT_RP

Add Rename Clone Delete

Click here to add a description.

Routing Profile

Update Priority Add

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

Edit Delete

7.2.8 Topology Hiding – Avaya Side

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

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

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

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

The screenshot shows the 'Topology Hiding Profile' window. It has a table with four columns: Header, Criteria, Replace Action, and Overwrite Value. The first row contains 'Request-Line' in the Header column, 'IP/Domain' in the Criteria column, 'Auto' in the Replace Action column, and an empty text box in the Overwrite Value column. To the right of the text box is a 'Delete' button. Above the table is an 'Add Header' button. Below the table are 'Back' and 'Finish' buttons.

The screenshot shows the 'Topology Hiding Profile' window with a list of headers. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The headers listed are Request-Line, From, To, Record-Route, Via, SDP, Refer-To, and Referred-By. Each header has 'IP/Domain' in the Criteria column, 'Auto' in the Replace Action column, and an empty text box in the Overwrite Value column. Each row has a 'Delete' button to its right. The 'Add Header' button is no longer visible. 'Back' and 'Finish' buttons are at the bottom.

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

The screenshot shows the 'Edit Topology Hiding Profile' window. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The headers listed are Refer-To, SDP, Record-Route, Via, To, Referred-By, Request-Line, and From. Each header has 'IP/Domain' in the Criteria column, 'Overwrite' in the Replace Action column, and 'customerera.com' in the Overwrite Value column. Each row has a 'Delete' button to its right. 'Back' and 'Finish' buttons are at the bottom.

7.2.9 Topology Hiding – AT&T Side

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

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

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

7.3 Domain Policies

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

7.3.1 Application Rules

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

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

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

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

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Time of Day Rules
End Point Policy
Groups
Session Policies

Application Rules: SIP_Trunk_AR

Add Filter By Device: Parameters Clone Delete

Click here to add a description

Application Type	Is	Opt	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Maximum Concurrent Sessions

CDR Support: None

RTCP Keep-Alive: No

Edit

7.3.2 Media Rules

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

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

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

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

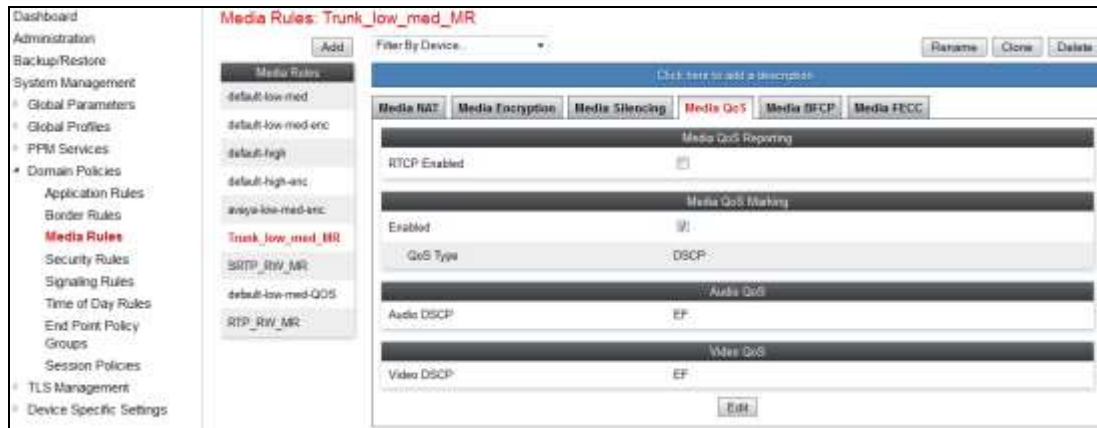
- In the **Clone Name** field enter **Avaya-low-med_MR**
- Click **Finish**. The newly created rule will be displayed.

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

- Select the **Media QOS** tab (not shown).

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

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



7.3.3 Signaling Rules

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

7.3.3.1 Avaya – Signaling Rules

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

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

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

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

7.3.3.1.1 Avaya – Signaling Rule - Request Headers Tab

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

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

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

Step 2 - Click **Finish**.

Step 3 - Repeat Steps Steps 1 & 2 to create a rule to remove the following headers:

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

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

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

7.3.3.1.2 Avaya – Signaling Rule Response Headers Tab

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

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

- **P-Location header from 1xx responses:**
 - Select the **Response Headers** tab (not shown).
 - Click the **Edit** button and the **Edit Header Control** window will open.
 - Check the **Proprietary Request Header** box.
 - In the **Header Name** field, enter **P-Location**.
 - From the **Response Code** menu select **1xx**.
 - From the **Method Name** menu select **Invite**.

- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**.
- **P-Location header from 2xx responses.**
 - From the **Response Code** menu select **2xx**.
 - Click **Finish**.

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

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

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

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

Step 3 - Highlight the **Avaya_SR** rule, select the **Signaling QoS** tab and enter the following:

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

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

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

7.3.3.2 AT&T – Signaling Rule Request Headers Tab

The Remote-Address header inserted by the Avaya SBCE is removed prior to sending it to AT&T (see **Section 2.2, Item 5**). Repeat the steps in **Section 7.3.3.1.1** to remove the Remote-Address header. The completed Request Headers form is shown below. Note that the Direction column says “OUT”.

The screenshot shows the 'Signaling Rules: ATT_SR' configuration page. The left sidebar lists various system management options. The main area has tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'Request Headers' tab is active, displaying a table with columns: Row, Header Name, Method Name, Header Criteria, Action, Proprietary, and Direction. A single row is visible with the following data: Row 1, Header Name 'Remote-Address', Method Name 'ALL', Header Criteria 'Forbidden', Action 'Remove Header', Proprietary 'Yes', and Direction 'OUT'. Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' are at the top. Below the table are buttons for 'Add In Header Control' and 'Add Out Header Control'.

Note - No Response Header manipulation is required.

Step 1 - Highlight the **ATT_SR** rule, select the **Signaling QoS** tab and repeat **Steps 3 & 4** from **Section 7.3.3.1.2**.

The screenshot shows the 'Signaling QoS' configuration page. It has tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'Signaling QoS' tab is active, showing a form with fields for 'Signaling QoS' (checked), 'QoS Type' (DSCP), and 'DSCP' (EF). An 'Edit' button is at the bottom.

7.3.4 Endpoint Policy Groups – Avaya Connection

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

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

Step 3 - Select **Add**.

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

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

The screenshot shows the 'Policy Groups: Avaya_default-low_PG' configuration page. The left sidebar lists various policy categories. The main area has tabs for 'Policy Groups', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-subc', 'avaya-def-high-senior', 'ATT_default-low_PG', and 'Avaya_default-low...'. The 'Policy Groups' tab is active, displaying a table with columns: Order, Application, Border, Media, Security, and Signaling. A single row is visible with the following data: Order 1, Application 'SIP_Trunk_AR', Border 'default', Media 'Trunk_low_med_MR', Security 'default-low', and Signaling 'CS1K_SR'. Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' are at the top. Below the table is a 'Summary' button.

7.3.5 Endpoint Policy Groups – AT&T Connection

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

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



Order	Application	Border	Media	Security	Signaling	
1	SIP_Trunk_AR	default	Trunk_low_med_MR	default-low	ATT_SR	Edit

7.4 Device Specific Settings

7.4.1 Network Management

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

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



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

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



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

7.4.2 Advanced Options

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

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

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

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

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

Advanced Options: SBCE

Devices: SBCE

Port Range Configuration

Port Range Configuration	Port Range
Signaling Port Range	12555 - 16000
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	9000 - 9999
HTTP Port Range	10000 - 10000
OCS FTP Listen Port Range	6881 - 6901
OCS Alternate FTP Listen Port Range	11175 - 11185

Save

7.4.3 Media Interfaces

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

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

Step 2 - Select **Media Interface**.

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

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

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

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

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

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

Media Interface: SBCE

Media Interface

Add

Name	Media IP Address	Port Range	
Inside_Trunk_MI	192.168.70.120 (Network_A1 (A1, VLAN 1))	16384 - 32767	Edit Delete
Outside_Trunk_MI	10.10.10.10 (Network_B1 (B1, VLAN 1))	16384 - 32767	Edit Delete

7.4.4 Signaling Interface

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

Step 2 - Select **Signaling Interface**.

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

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

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

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

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

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



7.4.5 Endpoint Flows

Endpoint flows combine the previously defined Device Specific Settings for both the CS1000E and AT&T.

7.4.4.1 Endpoint Flows – For Session Manager

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

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

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

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

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

View Flow: SM_Trunk																	
<div>Criteria</div> <table> <tr><td>Flow Name</td><td>SM_Trunk</td></tr> <tr><td>Server Configuration</td><td>SM_Trunk_SC</td></tr> <tr><td>URI Group</td><td>*</td></tr> <tr><td>Transport</td><td>*</td></tr> <tr><td>Remote Subnet</td><td>*</td></tr> <tr><td>Received Interface</td><td>Outside_Trunk_SI</td></tr> </table>		Flow Name	SM_Trunk	Server Configuration	SM_Trunk_SC	URI Group	*	Transport	*	Remote Subnet	*	Received Interface	Outside_Trunk_SI				
Flow Name	SM_Trunk																
Server Configuration	SM_Trunk_SC																
URI Group	*																
Transport	*																
Remote Subnet	*																
Received Interface	Outside_Trunk_SI																
<div>Profile</div> <table> <tr><td>Signaling Interface</td><td>Inside_Trunk_SI</td></tr> <tr><td>Media Interface</td><td>Inside_Trunk_MI</td></tr> <tr><td>End Point Policy Group</td><td>Avaya_default-low_PG</td></tr> <tr><td>Routing Profile</td><td>ATT_RP</td></tr> <tr><td>Topology Hiding Profile</td><td>Avaya_TH</td></tr> <tr><td>File Transfer Profile</td><td>None</td></tr> <tr><td>Signaling Manipulation Script</td><td>None</td></tr> <tr><td>Remote Branch Office</td><td>Any</td></tr> </table>		Signaling Interface	Inside_Trunk_SI	Media Interface	Inside_Trunk_MI	End Point Policy Group	Avaya_default-low_PG	Routing Profile	ATT_RP	Topology Hiding Profile	Avaya_TH	File Transfer Profile	None	Signaling Manipulation Script	None	Remote Branch Office	Any
Signaling Interface	Inside_Trunk_SI																
Media Interface	Inside_Trunk_MI																
End Point Policy Group	Avaya_default-low_PG																
Routing Profile	ATT_RP																
Topology Hiding Profile	Avaya_TH																
File Transfer Profile	None																
Signaling Manipulation Script	None																
Remote Branch Office	Any																

7.4.4.2 Endpoint Flows – For AT&T

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

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

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

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

End Point Flows: SBCE																													
<div>Dashboard</div> <div>Administration</div> <div>Backup/Restore</div> <div>System Management</div> <div>Global Parameters</div> <div>PPM Services</div> <div>Domain Policies</div> <div>TLS Management</div> <div>Device Specific Settings</div> <div>Network Management</div> <div>Media Interface</div> <div>Signaling Interface</div> <div>End Point Flows</div> <div>Session Flows</div>	<div>SBCE</div> <div>Subscriber Flows</div> <div>Server Flows</div> <div>Add</div> <div>Server Configuration: ATT_SC</div> <table> <thead> <tr> <th>Priority</th> <th>Flow Name</th> <th>URI Group</th> <th>Received Interface</th> <th>Signaling Interface</th> <th>End Point Policy Group</th> <th>Routing Profile</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>ATT</td> <td>*</td> <td>Inside_Trunk_SI</td> <td>Outside_Trunk_SI</td> <td>ATT_default-low_PG</td> <td>SM_RP</td> </tr> </tbody> </table> <div>Server Configuration: SM_Trunk_SC</div> <div>Update</div> <table> <thead> <tr> <th>Priority</th> <th>Flow Name</th> <th>URI Group</th> <th>Received Interface</th> <th>Signaling Interface</th> <th>End Point Policy Group</th> <th>Routing Profile</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SM_Trunk</td> <td>*</td> <td>Outside_Trunk_SI</td> <td>Inside_Trunk_SI</td> <td>Avaya_default-low_PG</td> <td>ATT_RP</td> </tr> </tbody> </table>	Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP	Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default-low_PG	ATT_RP
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile																							
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP																							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile																							
1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default-low_PG	ATT_RP																							

8 AT&T IP Flexible Reach Service

The IPFR-EF service provided DID/DNIS numbers for the reference configuration. The DNIS numbers terminated to the CS1000E location via the IPFR-EF service. Any DID and DNIS numbers shown in these application notes are examples. Customers will be assigned DIDs by AT&T. It should be noted that the DID numbers dialed, and the DNIS numbers inserted into SIP headers may not be the same digit strings.

The IPFR-EF service also provided a network border element IP address for the reference configuration. Customers will be assigned a border element IP address by AT&T.

9 Verification Steps

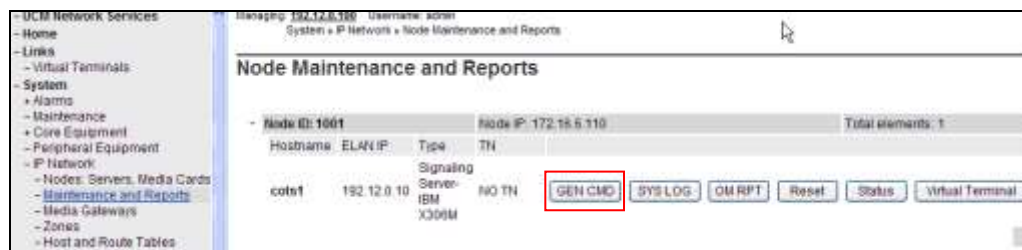
This section provides example verifications of the Avaya configuration with IPFR-EF service.

9.4 CS1000E Verifications

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

9.4.1 IP Network Maintenance and Reports Commands

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

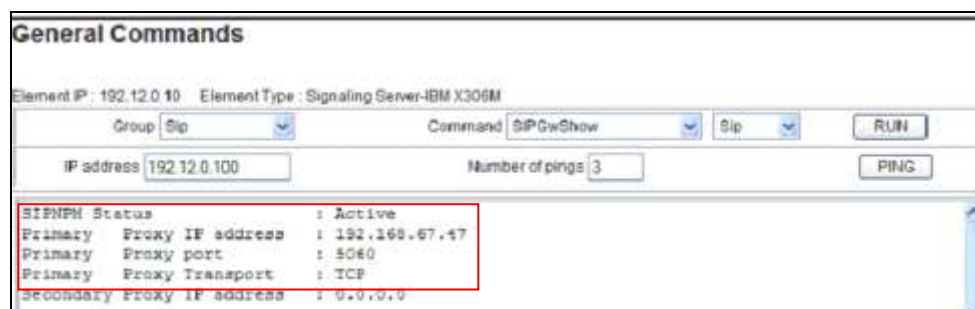


Step 2 - In the resultant screen on the right, click the **GEN CMD** button. The **General Commands** page is displayed as shown below.



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

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



9.4.2 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

<Selected by Overlay>

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

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

When **D-Channel Diagnostics** is selected on the right menu above, a screen such as the following is displayed. D-Channels **15** (Sip GW) and **20** (SIPLine), show as established (**EST**) and active (**ACTV**).

D-Channel Diagnostics

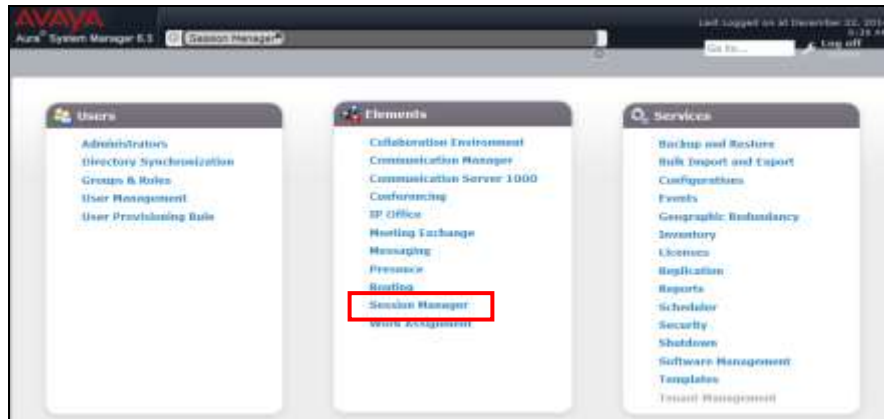
Diagnostic Commands		Command Parameters	Action
Status for D-Channel (STAT DCH)			<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)		<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)		<input type="checkbox"/> FDL	<input type="button"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

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

9.5 Avaya Aura® Session Manager

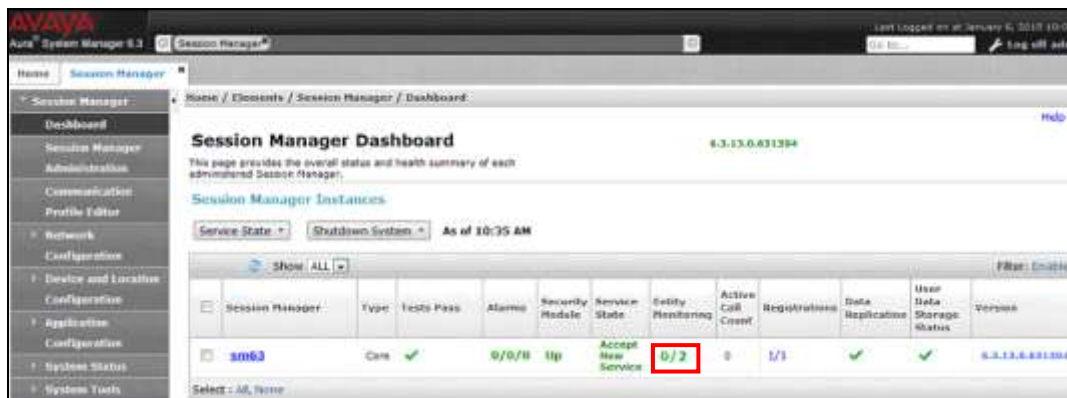
The Session Manager configuration may be verified via System Manager.

Step 1 – Using the procedures described in **Section 5**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



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

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



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



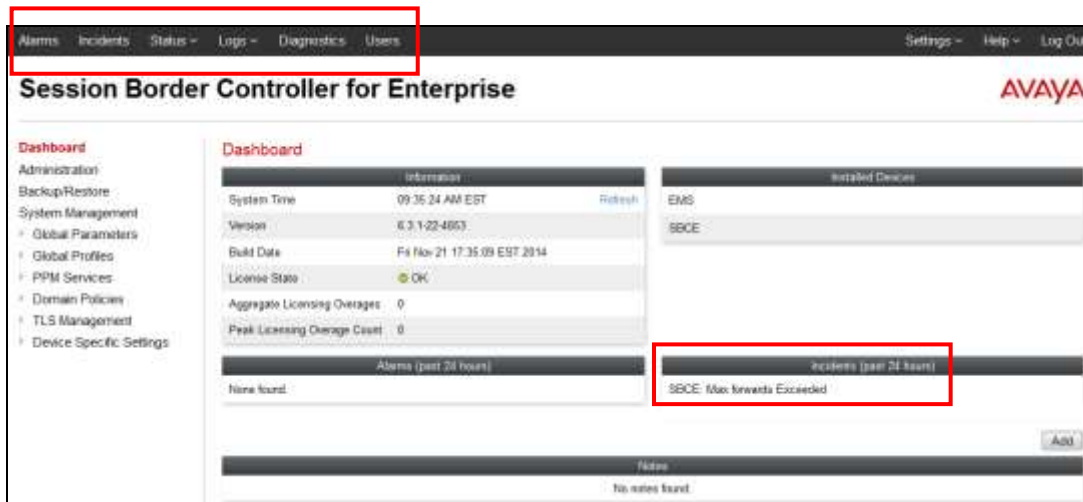
Note - the **A-SBCE** Entity from the list of monitored entities above. The **Reason Code** column indicates that Session Manager has received a **SIP 405 Method Not Allowed** response to the SIP OPTIONS it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Also note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

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

9.6 Avaya Session Border Controller for Enterprise

9.6.1 System Status

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



9.6.2 Protocol Traces

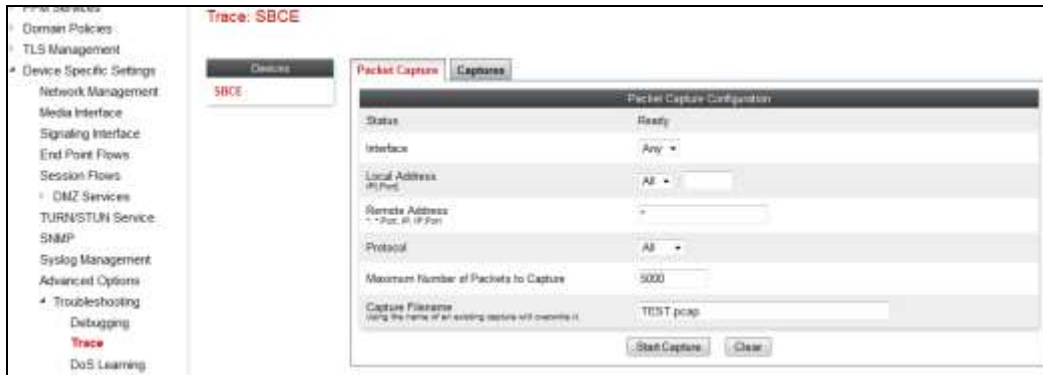
The Avaya SBCE can take internal traces of specified interfaces.

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

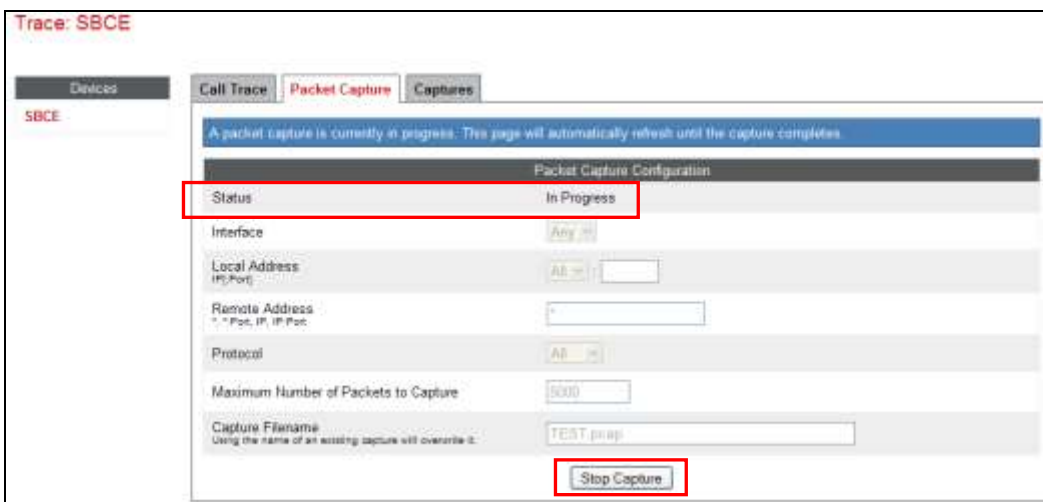
Step 2 - Select the **Packet Capture** tab and select the following:

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

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



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



Step 3 – Run the test.

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

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

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



10 Conclusion

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

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

11 References

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

Avaya Session Border Controller for Enterprise

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

AT&T IP Flexible Reach - Enhanced Features Service:

12. AT&T IP Flexible Reach - Enhanced Features Service description - <http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>

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

The IPFR-EF 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 **10.10.10.11** and **10.10.10.12**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to 10.10.10.12.

12.1 Configure the Secondary Border Element Server Configuration

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

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

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

The screenshot shows the 'Server Configuration: ATT_Secondary_SC' dialog box with the 'General' tab selected. The 'Server Type' is 'Trunk Server'. The 'IP Address / FQDN' field contains '10.10.10.12'. The 'Port' field contains '5060' and the 'Transport' field contains 'UDP'. There are 'Add', 'Edit', 'Rename', 'Close', and 'Delete' buttons.

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

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

The screenshot shows the 'Heartbeat' tab of the 'Server Configuration: ATT_Secondary_SC' dialog box. The 'Enable Heartbeat' checkbox is checked. The 'Method' is 'OPTIONS', 'Frequency' is '60 seconds', 'From URI' is 'secondary@customer.com', and 'To URI' is 'secondary@customer.com'.

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

The screenshot shows the 'Advanced' tab of the 'Server Configuration: ATT_Secondary_SC' dialog box. The 'Enable DoS Protection' and 'Enable Grooming' checkboxes are unchecked. The 'Interworking Profile' is 'ATT_Trunk_SI', the 'Signaling Manipulation Script' is 'CS1K_maxptime_Remote_Address', and the 'Connection Type' is 'SUBID'.

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

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

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

12.2 Add Secondary Border Element IP Address to Routing

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

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

12.3 Configure Secondary AT&T Border Element End Point Flow

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

Subscriber Flows
Server Flows

Server Configuration: ATT_Primary_SC

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

Server Configuration: ATT_Secondary_SC

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

Server Configuration: SM_Trunk_SC

Update

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

©2015 Avaya Inc. All Rights Reserved.

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

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