Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Cisco® CUCM™ & AT&T IP Flexible Reach SIP Trunk using Mediant E-SBC

November 2014

Document # LTRT-38140

Table of Contents

Notice

This document describes how to connect the Cisco Unified Communications Manager (CUCM) and AT&T IP Flexible Reach SIP Trunk using AudioCodes Mediant E-SBC product series.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: November-13-2014

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads.

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between AT&T IP Flexible Reach) over MIS, PNT and AT&T Virtual Private Network transport SIP Trunk and Cisco Unified Communications Manager (CUCM) environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and AT&T IP Flexible Reach Partners who are responsible for installing and configuring AT&T IP Flexible Reach SIP Trunk and Cisco CUCM for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The E-SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the E-SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes E-SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC
Software Version	SIP_6.80A.227.005
Protocol	▪ SIP/UDP (to the AT&T IP Flexible Reach SIP Trunk) ▪ SIP/UDP (to the Cisco CUCM Server)
Additional Notes	None

2.2 AT&T IP Flexible Reach SIP Trunking Version

Table 2-2: AT&T IP Flexible Reach Version

Vendor/Service Provider	AT&T IP Flexible Reach
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Cisco Unified Communications Manager Version

Table 2-3: Cisco CUCM Version

Vendor	Cisco
Model	Cisco Unified Communications Manager (CUCM)
Software Version	Release 10.0.1
Protocol	SIP
Additional Notes	None

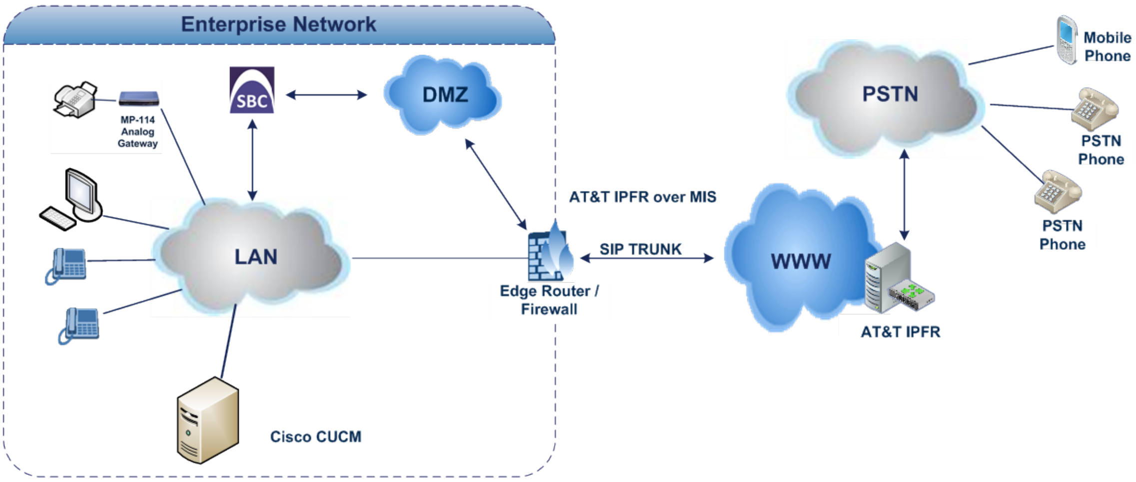
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and AT&T IP Flexible Reach SIP Trunk with Cisco CUCM was done using the following topology setup:

- Enterprise deployed with Cisco CUCM in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees voice capabilities and to connect the Enterprise to the PSTN network using AT&T IP Flexible Reach SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
    - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** IP-to-IP network border between Cisco CUCM network in the Enterprise LAN and AT&T IP Flexible Reach SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Cisco CUCM with AT&T IP Flexible Reach SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Cisco CUCM environment is located on the Enterprise's LAN ▪ AT&T IP Flexible Reach SIP Trunk is located on the WAN
Signaling Transcoding	▪ Cisco CUCM operates with SIP-over-UDP transport type ▪ AT&T IP Flexible Reach SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Cisco CUCM supports G.729 and G.711U-law coders ▪ AT&T IP Flexible Reach SIP Trunk supports G.729 and G.711U-law coders in that preferred order
Media Transcoding	▪ Cisco CUCM operates with RTP media type ▪ AT&T IP Flexible Reach SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Cisco CUCM and AT&T IP Flexible Reach SIP Trunk.

Emergency 911/E911 Services Limitations and Restrictions - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer *Configuration Guide* will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.

While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when that 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.

This page is intentionally left blank.

3 Configuring Cisco CUCM

This chapter describes how to configure Cisco CUCM to operate with AudioCodes E-SBC.

> **Note:** Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

This step describes how to access and configure a SIP Trunk in the Cisco CUCM web site.

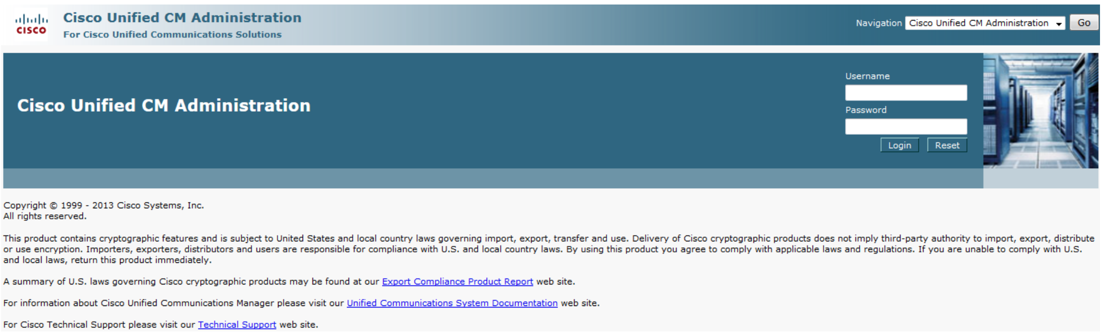
3.1 Access the CUCM

This section describes how to access the CUCM.

➢ **To access the CM:**

1. Open the browser and enter the CUCM URL (example): https://10.15.25.11/ccmadmin/showHome.do

Figure 3-1: Login Page



1. Enter the username and password.
2. Click **Login**.

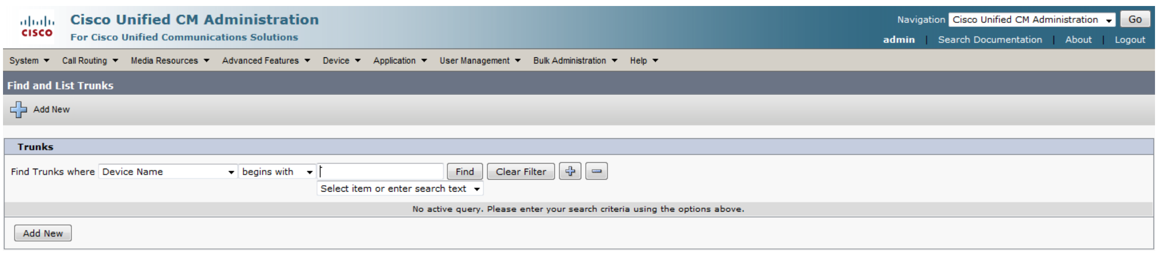
3.2 Create a New Trunk

This section describes how to create a new trunk.

➢ **To create a new trunk:**

1. From the **Device** menu drop-down list, select **Trunk**.
2. Click **Add New**.

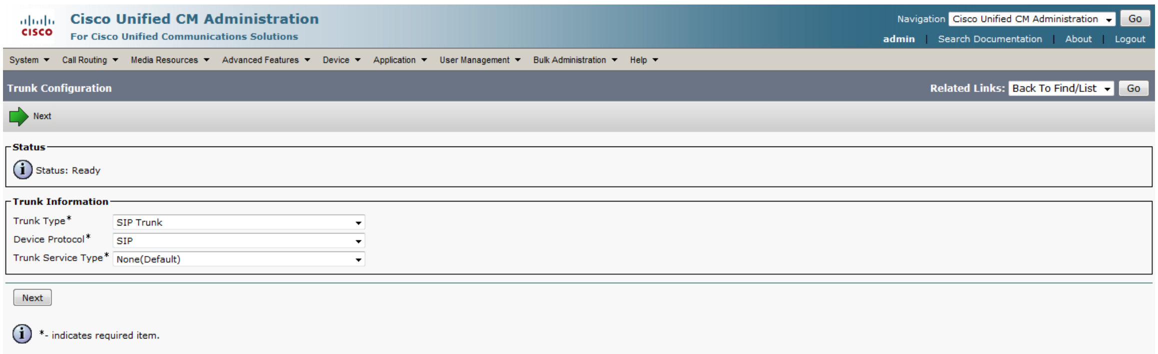
Figure 3-2: Trunk page



3. Select Trunk Type – **SIP Trunk**.

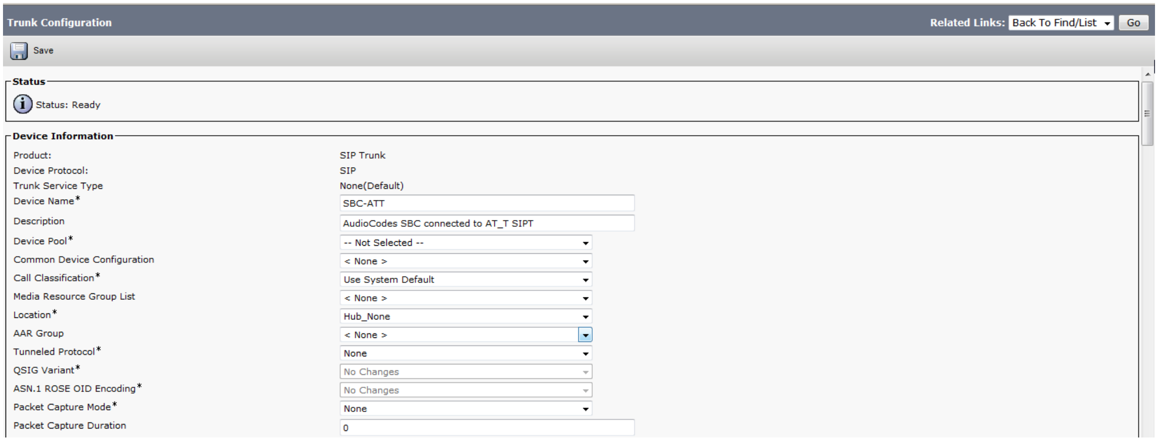
4. Click **Next**.

Figure 3-3: Create Trunk Page



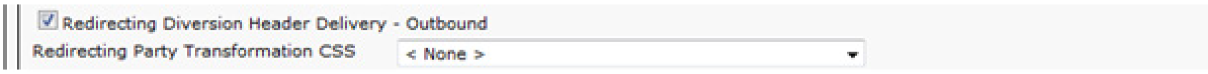
5. In the **Device Name** field, enter a unique SIP Trunk name and optionally provide a description.
6. From the **Device Pool** drop-down list, select a device pool.

Figure 3-4: SIP Trunk Settings Page



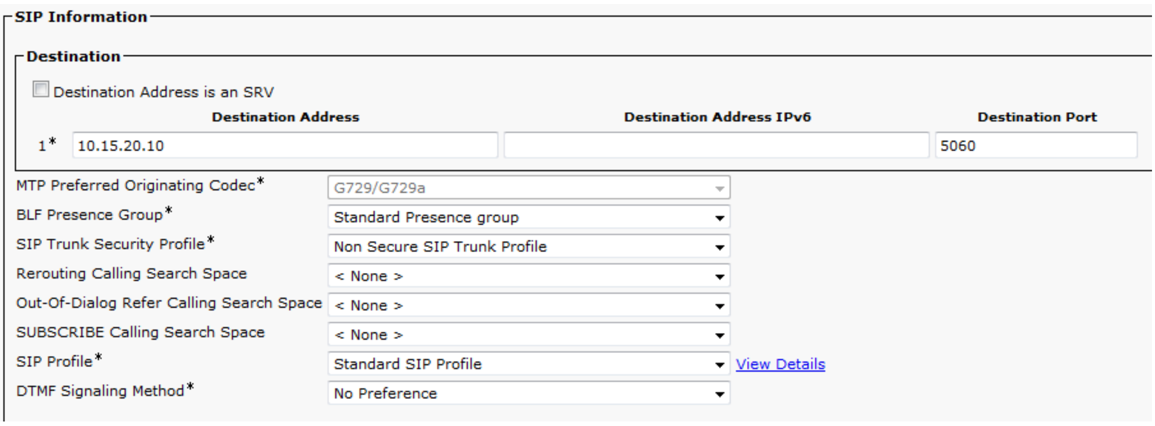
7. Select the 'Redirecting Diversion Header Delivery – Outbound' check box.

Figure 3-5: Redirecting Diversion Header Delivery



8. Enter the Destination Address and Destination Port of the AudioCodes SBC.

Figure 3-6: SIP Information Section



9. From the **SIP Trunk Security** drop-down list, select a profile.

10. From the **SIP Profile** drop-down list, select a profile.
11. Click **Save**.

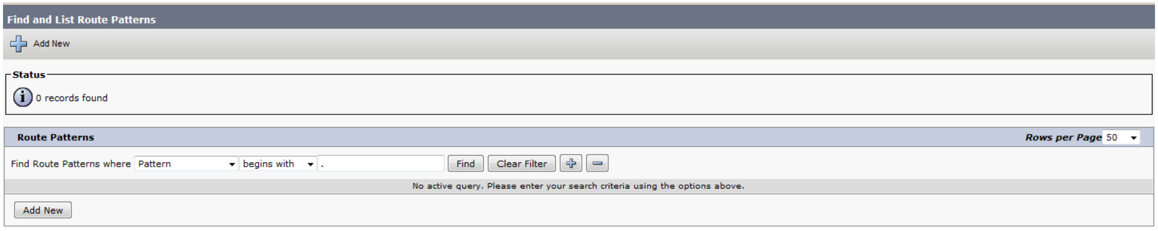
3.3 Create a New Route Pattern

This section describes how to create a new route pattern.

➢ **To create new Route Pattern:**

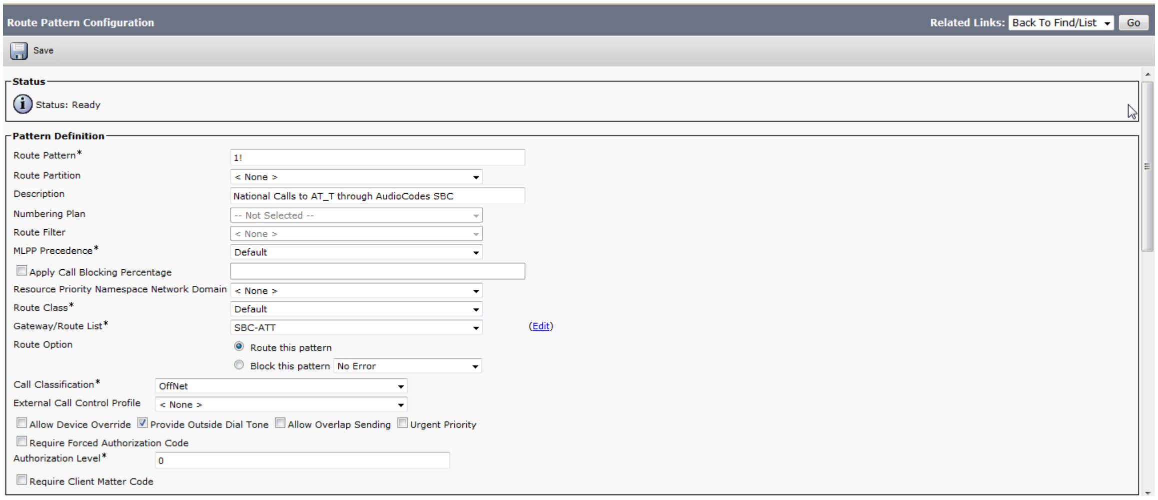
1. From the **Call Routing** menu drop-down list, select **Route Pattern**.
2. Click **Add New**.

Figure 3-7: Route Pattern page



3. Enter a Route Pattern according to schema (optionally provide a description).

Figure 3-8: Create Route Pattern Page



4. From the **Gateway/Route List** drop-down list, select the SIP Trunk device name.
5. Click **Save**.

Figure 3-9: Added Route Pattern

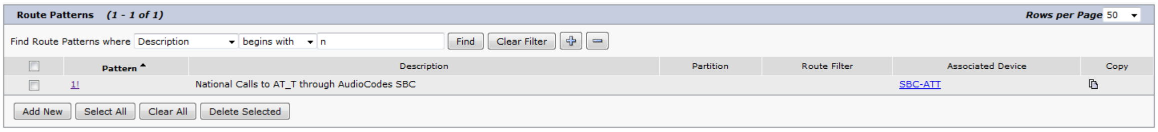
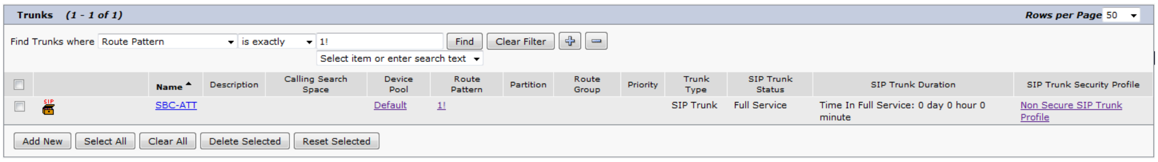


Figure 3-10: Added Trunk



Note: An * indicates a mandatory filed.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Cisco CUCM and the AT&T IP Flexible Reach SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

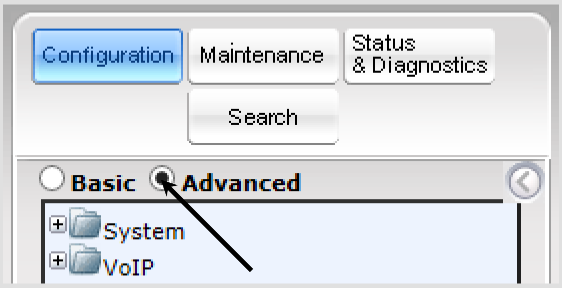
- E-SBC WAN interface - AT&T IP Flexible Reach SIP Trunking environment
- E-SBC LAN interface – Cisco CUCM environment

This configuration is done using the E-SBC's embedded Web server (hereafter, referred to as *Web interface*).

Notes:

- For implementing Cisco CUCM and AT&T IP Flexible Reach SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

  For more information about the Software License Key, contact your AudioCodes sales representative.
- The scope of this document does **not** cover security aspects for connecting the SIP Trunk to the Cisco CUCM environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, refer to the *Recommended Security Guidelines* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Full-menu display mode. To do this, select the **Full** option, as shown below:



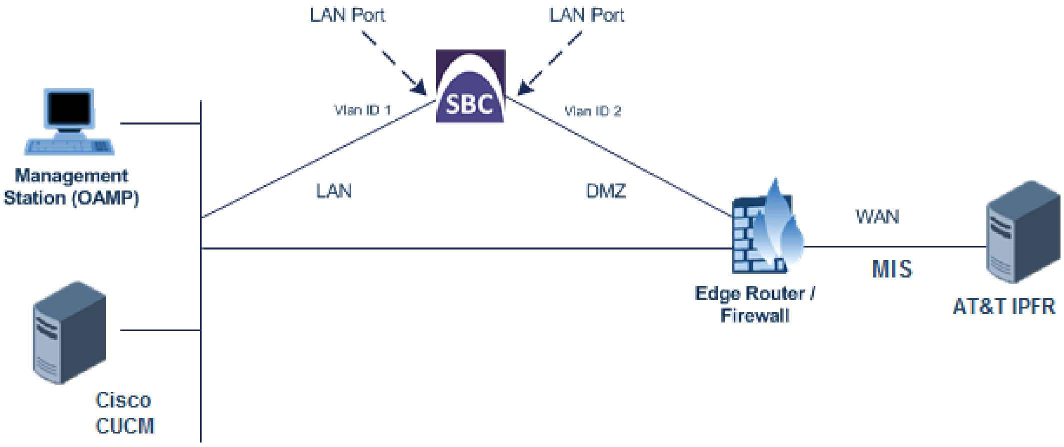
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, this interoperability test topology employs the following deployment method:

- E-SBC interfaces with the following IP entities:
  - Cisco CUCM servers, located on the LAN
  - AT&T IP Flexible Reach SIP Trunk, located on the WAN
- E-SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "Private")
- WAN VoIP (assigned the name "Public")

➢ **To configure the VLANs:**

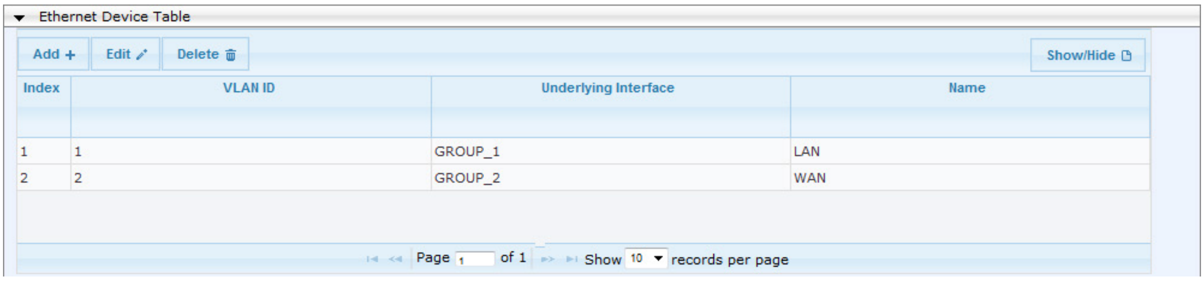
1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).

   There is an existing row for VLAN ID 1 and underlying interface GROUP_1.

2. Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	**1**
VLAN ID	**2**
Underlying Interface	**GROUP_2** (Ethernet port group)
Name	**WAN**

Figure 4-2: Configured VLAN IDs in Ethernet Device Table



4.1.2 Step 1b: Configure Network Interfaces

This step describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP (assigned the name "Private")
- WAN VoIP (assigned the name "Public")

➢ **To configure the IP network interfaces:**

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface as follows:

Parameter	Value
IP Address	**10.15.20.10** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Private** (arbitrary descriptive name)
Underlying Device	**LAN**

3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**12.210.214.226** (WAN IP address)
Prefix Length	**29** (for 255.255.255.248)
Gateway	**12.210.214.225** (router's IP address)
VLAN ID	**2**
Interface Name	**Public**
Underlying Device	**WAN**

4. Click **Apply**, and then **Done**.

The configured IP network interfaces are shown below:

Figure 4-3: Configured Network Interfaces in IP Interfaces Table

Interface Table

Add +

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media +	IPv4 Manual	10.15.20.10	16	10.15.0.1	Private	0.0.0.0	0.0.0.0	LAN
1	Media + Control	IPv4 Manual	12.210.214.226	29	12.210.214.225	Public	0.0.0.0	0.0.0.0	WAN

Page 1 of 1 Show 10 records per page

4.1.3 Step 1c: Configure the Native VLAN ID

This step describes how to configure the Native VLAN ID for the LAN and WAN interfaces.

➢ **To configure the Native VLAN ID for the IP network interfaces:**

1. Open the Physical Ports Settings page (**Configuration** tab> **VoIP** menu > **Network** > **Physical Ports Table**).
2. For the **GROUP_1** member ports, set the 'Native Vlan' field to **1**. This VLAN was assigned to network interface "Private".
3. For the **GROUP_2** member ports, set the 'Native Vlan' field to **2**. This VLAN was assigned to network interface "Public".

Figure 4-4: Configured Port Native VLAN

Physical Ports Settings

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

Page 1 of 2 Show 10 records per page

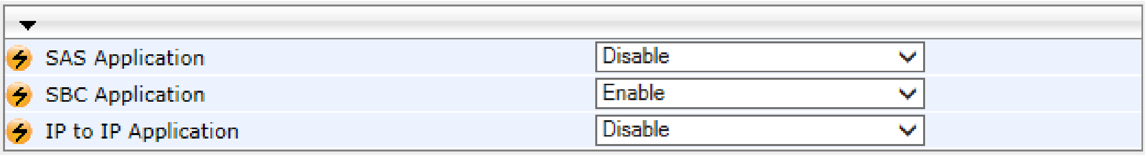
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).

Figure 4-5: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.11 on page 49).

4.3 Step 3: Signaling Routing Domains Configuration

This step describes how to configure Signaling Routing Domains (SRD). The SRD represents a logical VoIP network. Each logical or physical connection requires an SRD, for example, if the E-SBC interfaces with both the LAN and WAN, a different SRD would be required for each one.

The SRD is composed of the following:

- Media Realm: defines a UDP port range for RTP/SRTP (media) traffic on a specific logical IP network interface of the E-SBC.
- SIP Interface: defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface of the E-SBC.

4.3.1 Step 3a: Configure Media Realms

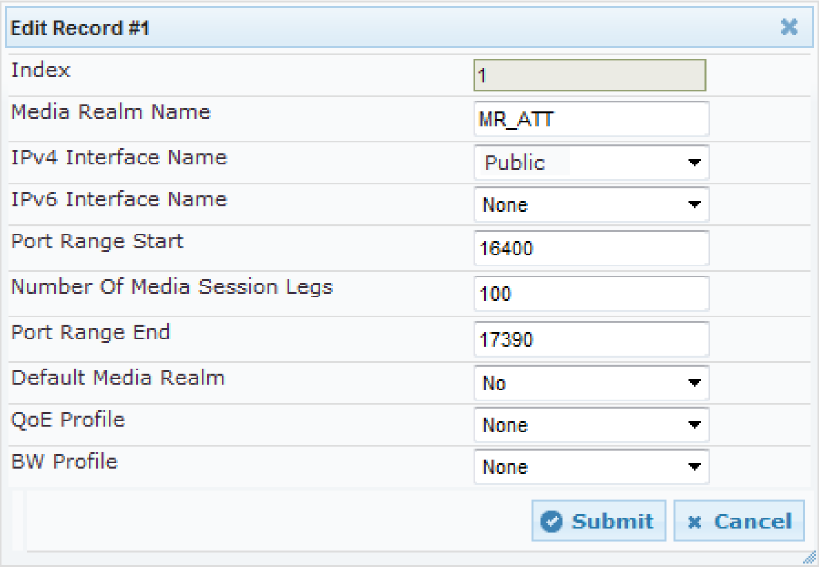
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Modify the existing Media Realm for WAN traffic:

Parameter	Value
Index	**1**
Media Realm Name	**MR_ATT** (descriptive name)
IPv4 Interface Name	**Public**
Port Range Start	**16400** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

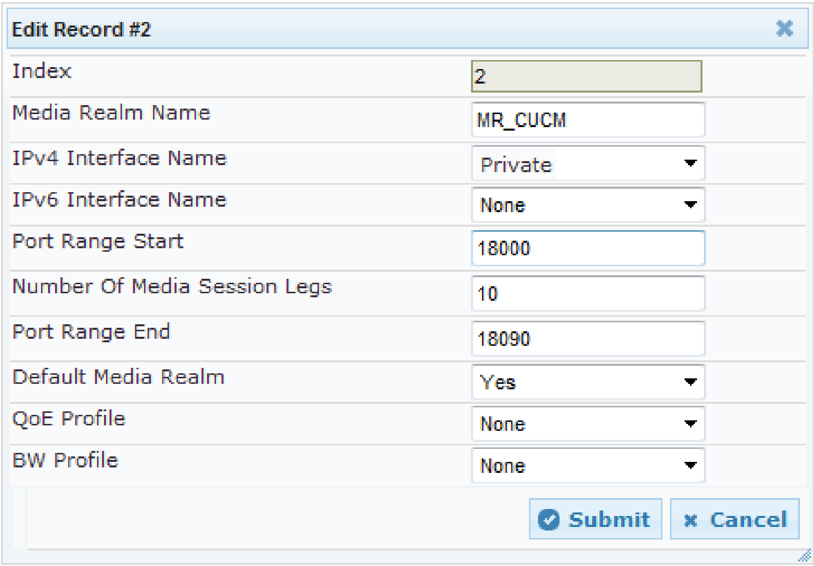
Figure 4-6: Configuring Media Realm for Public facing WAN



3. Configure a Media Realm for LAN traffic:

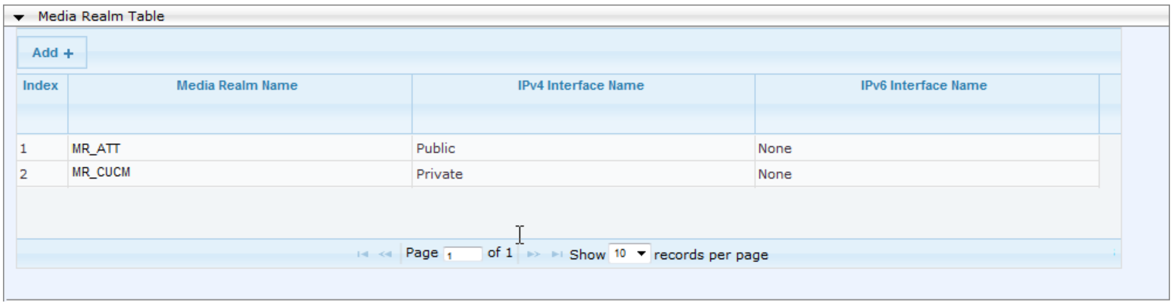
Parameter	Value
Index	**2**
Media Realm Name	**MR_CUCM** (arbitrary name)
IPv4 Interface Name	**Private**
Port Range Start	**18000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

Figure 4-7: Configuring Media Realm for Private facing LAN



The configured Media Realms are shown in the figure below:

Figure 4-8: Configured Media Realms in Media Realm Table



4.3.2 Step 3b: Configure SRDs

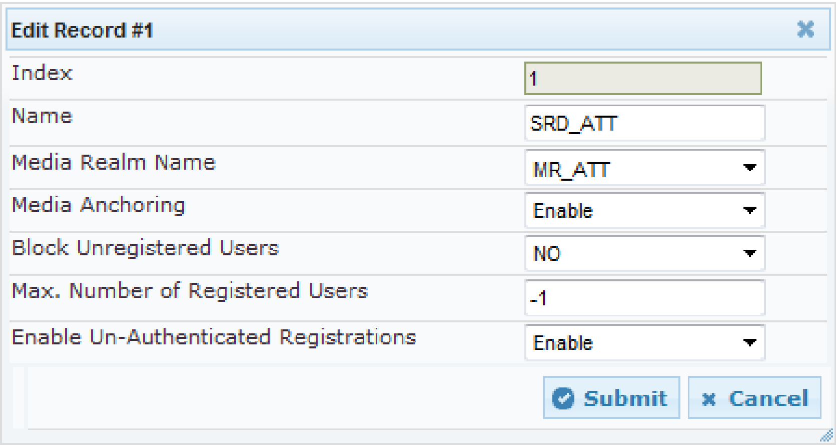
This step describes how to configure the SRDs.

➢ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Configure an SRD for the E-SBC's internal interface (toward AT&T IP Flexible Reach SIP Trunk):

Parameter	Value
SRD Index	**1**
SRD Name	**SRD_ATT** (descriptive name for SRD)
Media Realm	**MR_ATT** (associates SRD with Media Realm)

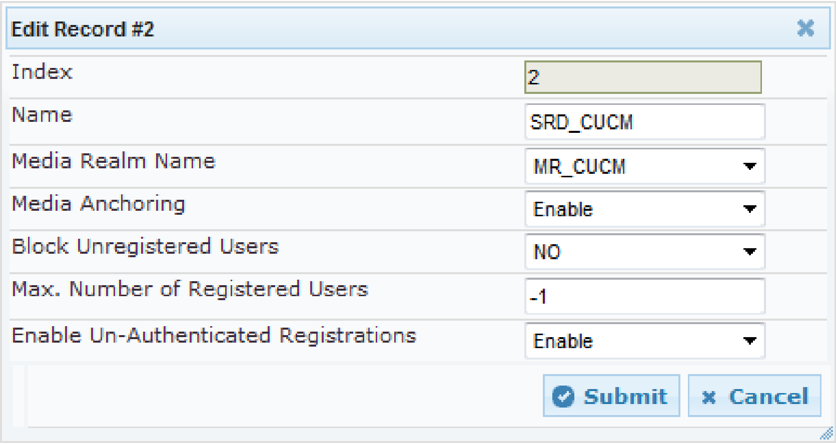
Figure 4-9: Configuring LAN SRD



3. Configure an SRD for the E-SBC's external interface (toward the Cisco CUCM):

Parameter	Value
SRD Index	**2**
SRD Name	**SRD_CUCM**
Media Realm	**MR_CUCM**

Figure 4-10: Configuring WAN SRD



4.3.3 Step 3c: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the E-SBC.

➢ **To configure SIP Interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Configure a SIP interface for the WAN:

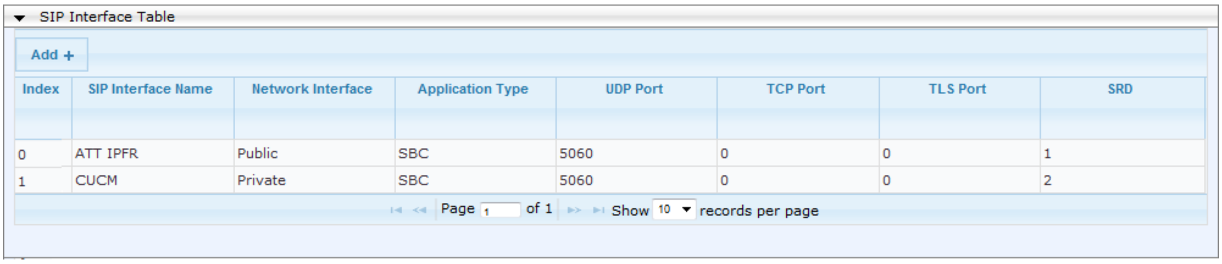
Parameter	Value
Index	**0**
Interface Name	**ATT_IPFR** (arbitrary descriptive name)
Network Interface	**Public**
Application Type	**SBC**
UDP Port	**5060**
TCP and UDP	**0**
SRD	**1**

3. Configure a SIP interface for the LAN:

Parameter	Value
Index	**1**
Interface Name	**CUCM**
Network Interface	**Private**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0**
SRD	**2**

The configured SIP Interfaces are shown in the figure below:

Figure 4-11: Configured SIP Interfaces in SIP Interface Table



SIP Interface Table

Add +

Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
0	ATT IPFR	Public	SBC	5060	0	0	1
1	CUCM	Private	SBC	5060	0	0	2

Page 1 of 1 Show 10 records per page

4.4 Step 4: Configure Proxy Sets

This step describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Cisco CUCM
- AT&T IP Flexible Reach SIP Trunk

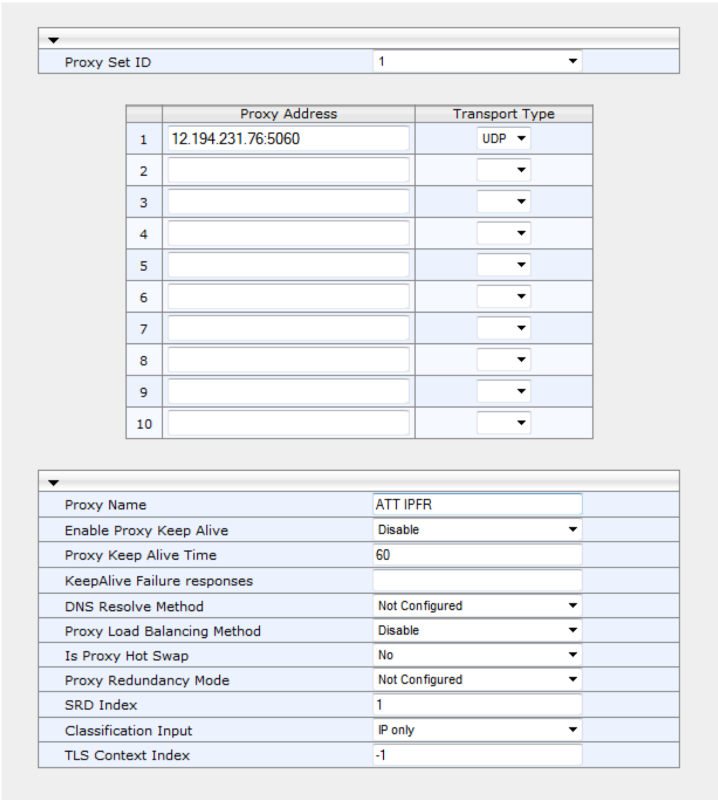
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for AT&T IP Flexible Reach SIP Trunk:

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**12.194.231.76:5060** (ATT IP Flexible Reach IP address / FQDN and destination port)
Transport Type	**UDP**
Proxy Name	**ATT IPFR** (arbitrary descriptive name)
SRD Index	**1**

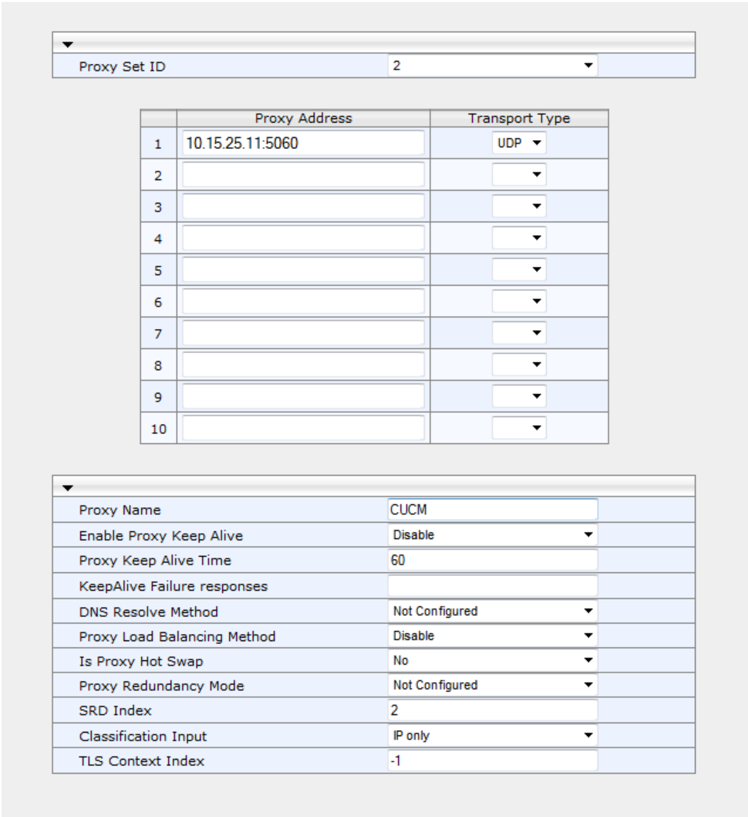
Figure 4-12: Configuring Proxy Set for AT&T IP Flexible Reach



3. Configure a Proxy Set for the Cisco CUCM:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**10.15.25.11:5060** (<CUCM> IP address / FQDN and destination port)
Transport Type	**UDP**
Proxy Name	**CUCM** (arbitrary descriptive name)
SRD Index	**2** (enables classification by Proxy Set for SRD of IP Group belonging to CUCM)

Figure 4-13: Configuring Proxy Set for Cisco CUCM



4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.11 on page 49).

4.5 Step 5: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. A typical deployment consists of multiple IP Groups associated with the same SRD. For example, you can have two LAN IP PBXs sharing the same SRD, and two ITSPs / SIP Trunks sharing the same SRD. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- Cisco CUCM (Server) located on LAN
- AT&T IP Flexible Reach SIP Trunk located on WAN

To configure IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Configure an IP Group for the ATT IP Flexible Reach SIP Trunk:

Parameter	Value
Index	**1**
Type	**Server**
Description	**ATT IPFR** (arbitrary descriptive name)
Proxy Set ID	**1**
SRD	**1**
Media Realm Name	**MR_ATT**
IP Profile ID	**1**

3. Configure an IP Group for the Cisco CUCM:

Parameter	Value
Index	**2**
Type	**Server**
Description	**CUCM** (arbitrary descriptive name)
Proxy Set ID	**2**
SRD	**2**
Media Realm Name	**MR_CUCM**
IP Profile ID	**2**

The configured IP Groups are shown in the figure below:

Figure 4-14: Configured IP Groups in IP Group Table

IP Group Table

Add +

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	ATT IPFR	1				No	1
2	Server	CUCM	2				No	2

Page 1 of 1 Show 10 records per page

4.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

- ATT IP Flexible Reach SIP trunk - to operate in non-secure mode using RTP and UDP
- Cisco CUCM - to operate in non-secure mode using RTP and UDP

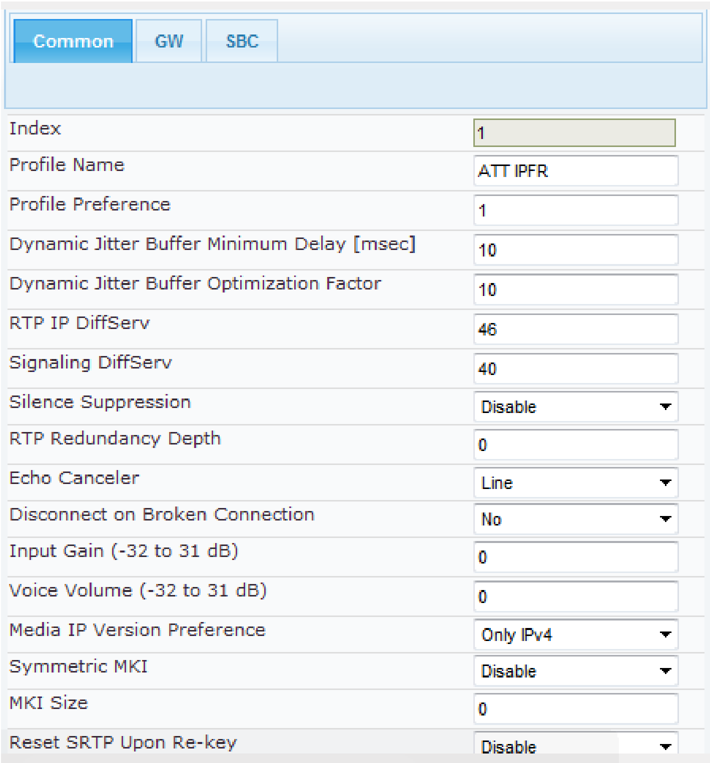
Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 30).

➢ **To configure IP Profiles:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Profile Name	**ATT IPFR** (arbitrary descriptive name)
Disconnect on Broken Connection	**No**

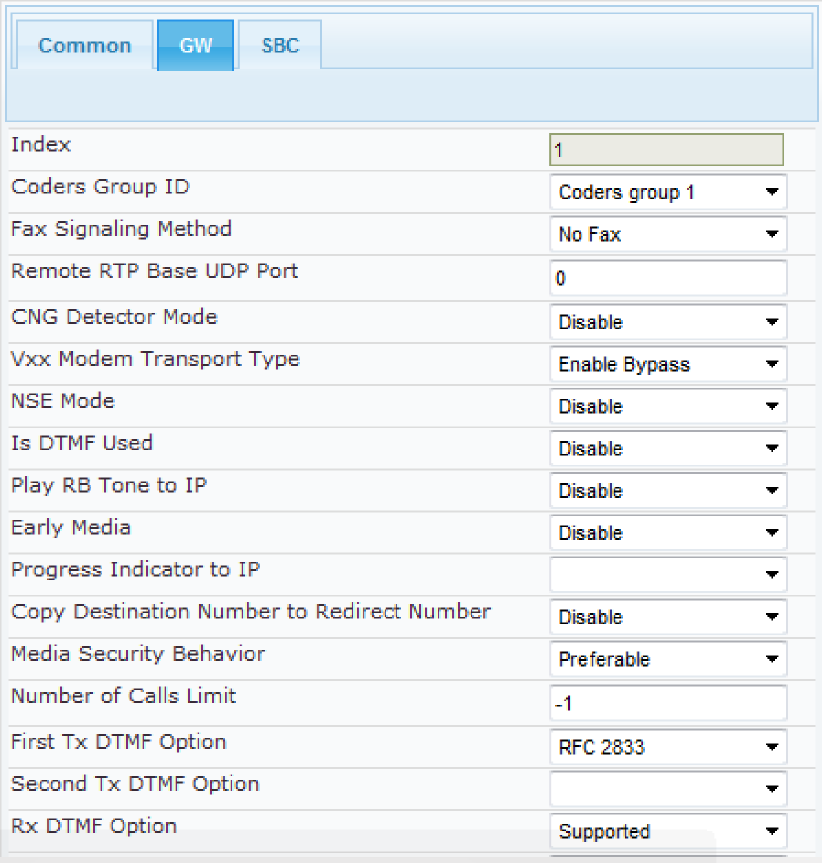
Figure 4-15: Configuring IP Profile for ATT IP Flexible Reach – Common Tab



4. Click the **GW** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Coders Group ID	**Coders Group 1**

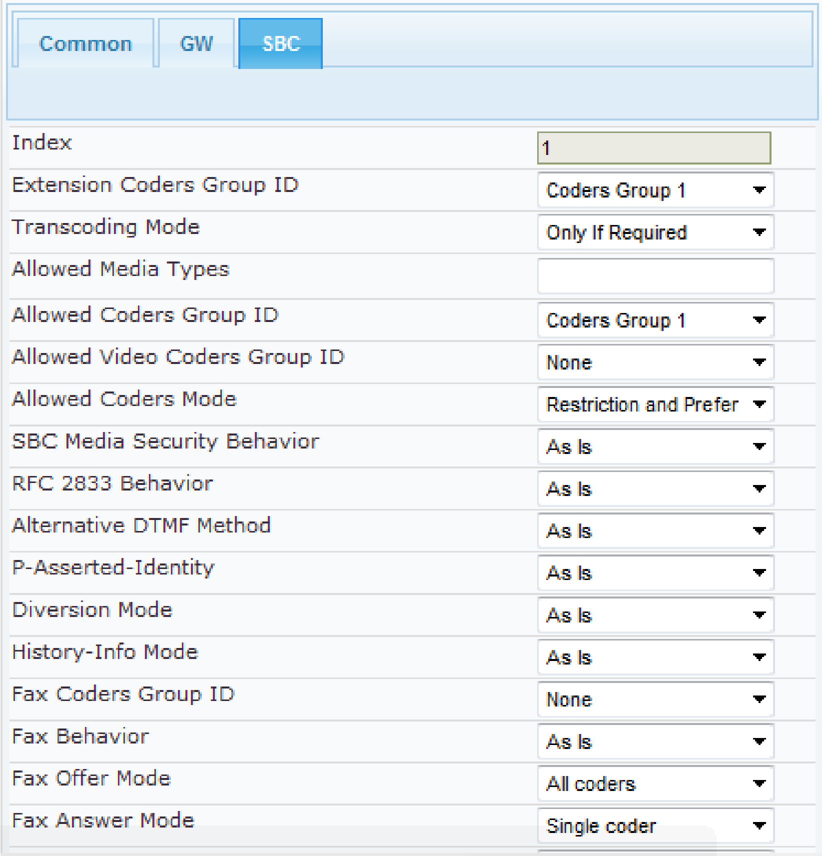
Figure 4-16: Configuring IP Profile for ATT IP Flexible Reach – GW Tab



5. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
SBC Extension Coders Group ID	**Coders Group 1**
SBC Allowed Coders Group ID	**Coders Group 1**
SBC Allowed Coders Mode	**Restriction and Preference**

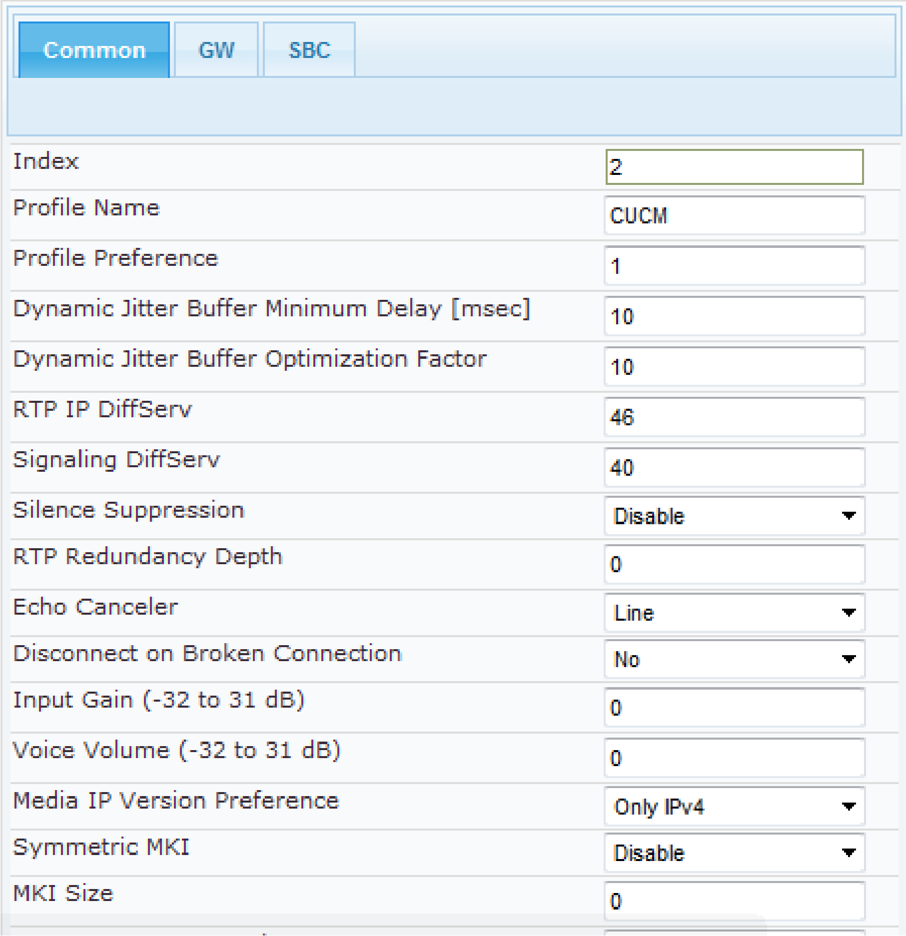
Figure 4-17: Configuring IP Profile for ATT IP Flexible Reach – SBC Tab



6. Configure an IP Profile for the Cisco CUCM:
7. Click **Add**.
8. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Profile Name	**CUCM** (arbitrary descriptive name)
Disconnect on Broken Connection	**No**

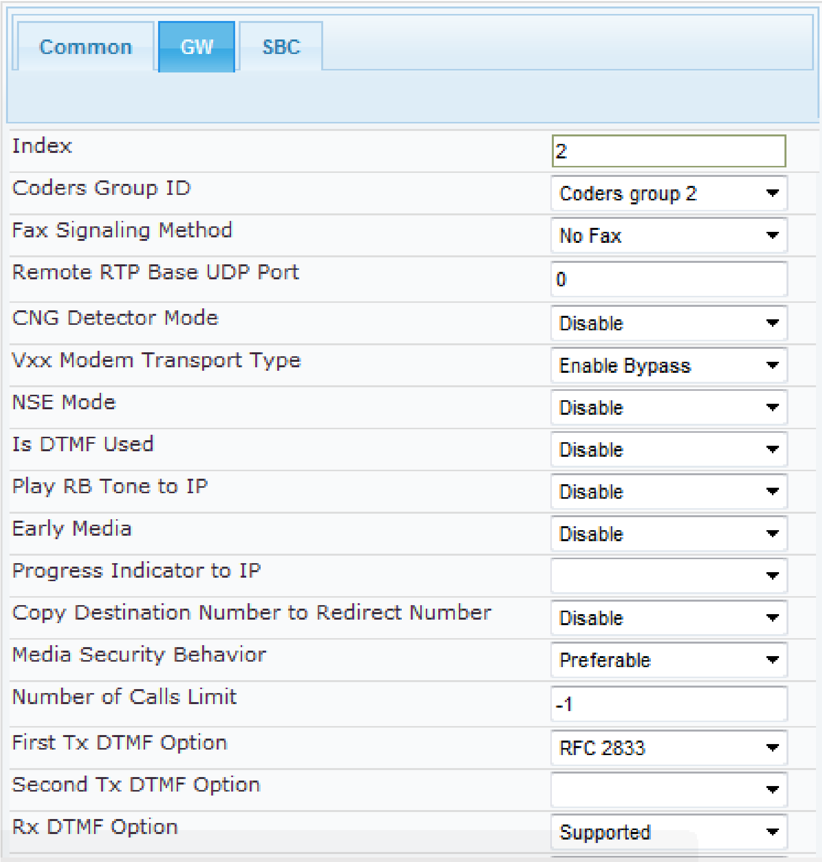
Figure 4-18: Configuring IP Profile for Cisco CUCM – Common Tab



9. Click the **GW** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Coders Group ID	**Coders Group 2**

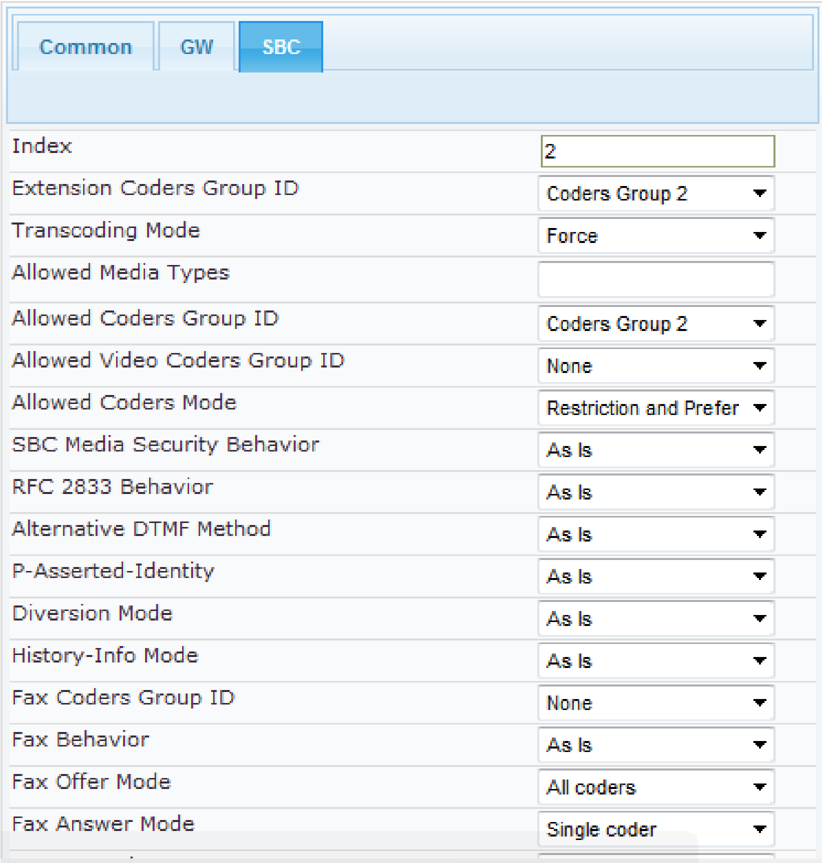
Figure 4-19: Configuring IP Profile for Cisco CUCM – GW Tab



10. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
SBC Extension Coders Group ID	**Coders Group 2**
Transcoding Mode	**Force**
SBC Allowed Coders Group ID	**Coders Group 2**
SBC Allowed Coders Mode	**Restriction and Preference**

Figure 4-20: Configuring IP Profile for Cisco CUCM – SBC Tab



4.7 Step 7: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Cisco CUCM supports the G.729 and G.711 coders while the network connection to AT&T IP Flexible Reach SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the AT&T IP Flexible Reach SIP Trunk.

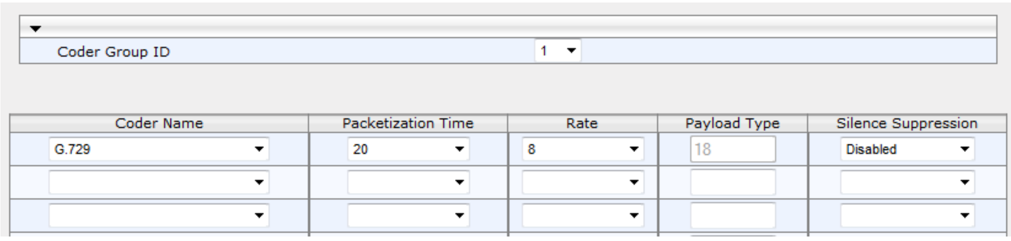
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 32).

➢ **To configure coders:**

1. Open the Coder Group Settings (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**).
2. Configure a Coder Group for AT&T IP Flexible Reach SIP Trunk.

Parameter	Value
Coder Group ID	**1**
Coder Name	**G.729**

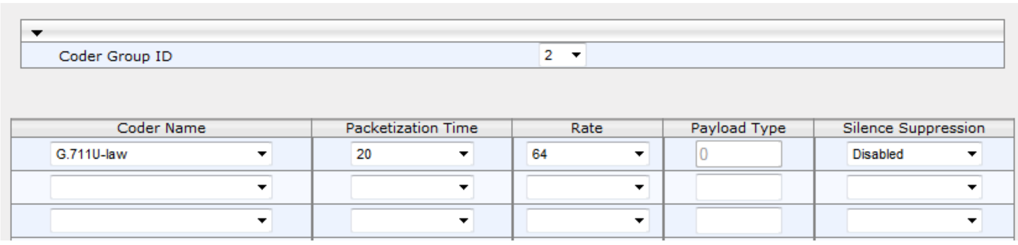
Figure 4-21: Configuring Coder Group for AT&T IP Flexible Reach SIP Trunk



3. Configure a Coder Group for Cisco CUCM:

Parameter	Value
Coder Group ID	**2**
Coder Name	**G.711U-law**

Figure 4-22: Configuring Coder Group for Cisco CUCM



4.7.1 Step 7-1: Configure Allowed Coders Group

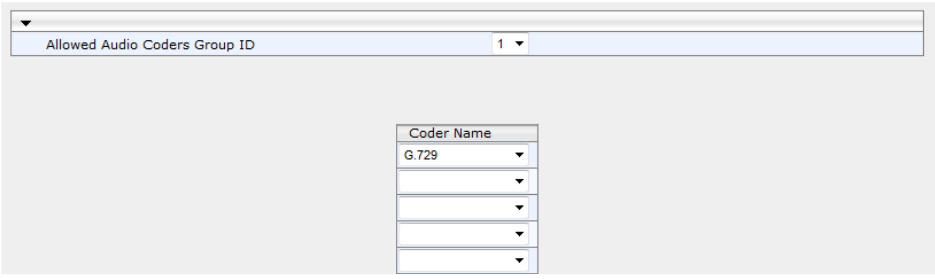
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the AT&T IP Flexible Reach SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the AT&T IP Flexible Reach SIP Trunk in the previous step (see Section 4.6 on page 32).

➢ **To set a preferred coder for the AT&T IP Flexible Reach SIP Trunk:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).
2. Configure an Allowed Coder group for ATT IP Flexible Reach as follows:

Parameter	Value
Allowed Coders Group ID	**1**
Coder Name	**G.729**

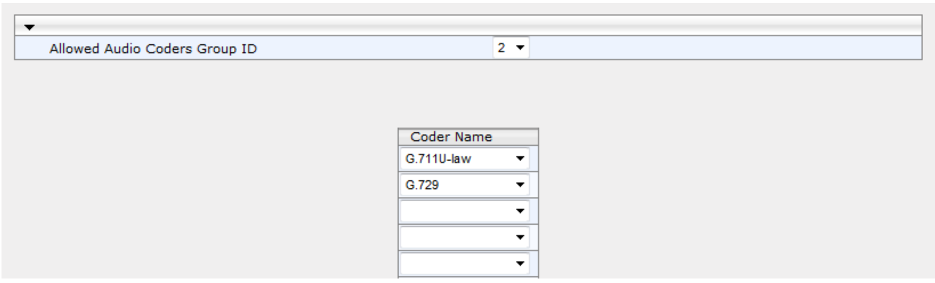
Figure 4-23: Configuring Allowed Coders Group for AT&T IP Flexible Reach SIP Trunk



3. Configure an Allowed Coder group for Cisco CUCM as follows:

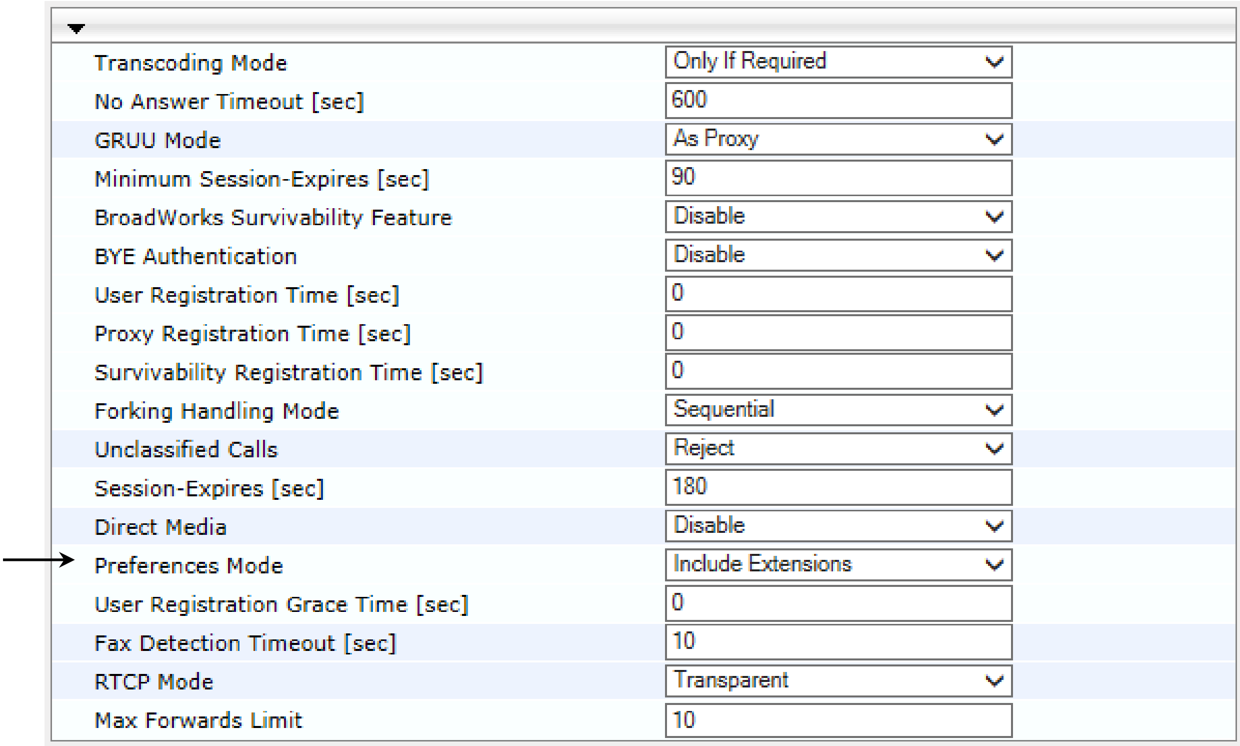
Parameter	Value
Allowed Coders Group ID	**2**
Coder Name	**G.711U-law** **G.729**

Figure 4-24: Configuring Allowed Coders Group for AT&T IP Flexible Reach SIP Trunk



4. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).

Figure 4-25: SBC Preferences Mode



5. From the '**Preferences Mode**' drop-down list, select **Include Extensions**.
6. Click **Submit**.

4.8 Step 8: Configure Maximum IP Media Channels

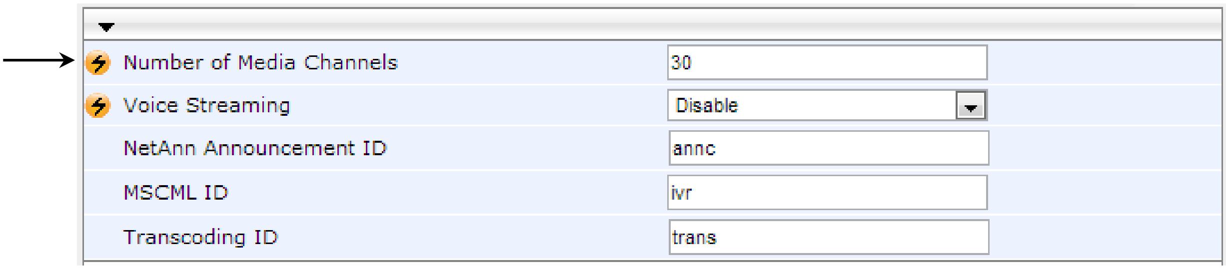
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

> **Note:** This step is required **only** if transcoding is required.

➢ **To configure the maximum number of IP media channels:**

1. Open the IP Media Settings page (**Configuration** tab > **VoIP** menu > **IP Media** > **IP Media Settings**).

Figure 4-26: Configuring Number of IP Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.11 on page 49).

4.9 Step 9: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 30, IP Group 1 represents AT&T IP Flexible Reach SIP Trunk, and IP Group 2 represents Cisco CUCM.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Cisco CUCM (LAN) and AT&T IP Flexible Reach SIP Trunk (WAN):

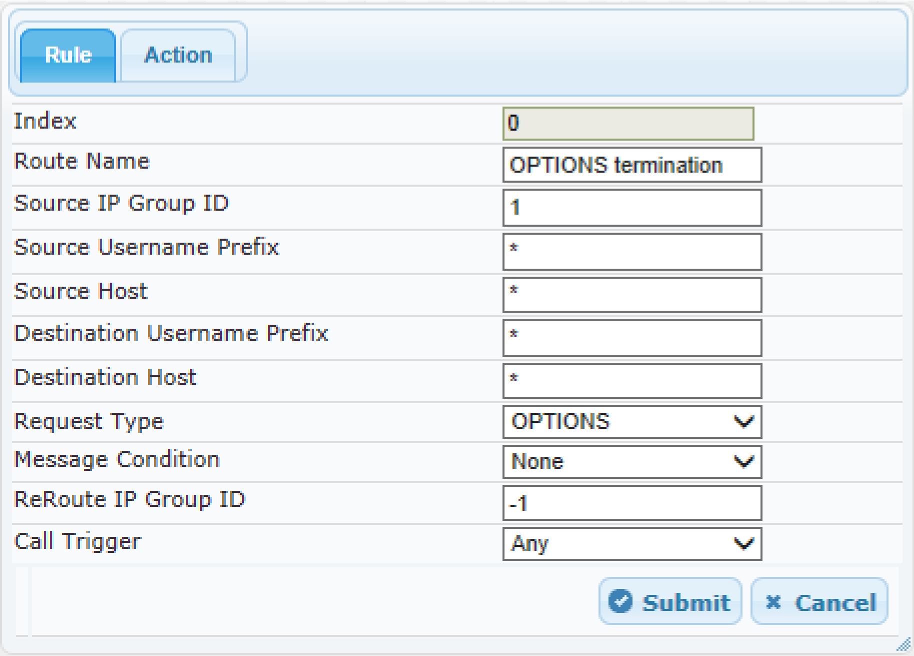
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from AT&T IP Flexible Reach SIP Trunk to Cisco CUCM
- Calls from Cisco CUCM to AT&T IP Flexible Reach SIP Trunk

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
3. Click **Add**.
4. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Route Name	**OPTIONS termination** (arbitrary descriptive name)
Source IP Group ID	**1**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

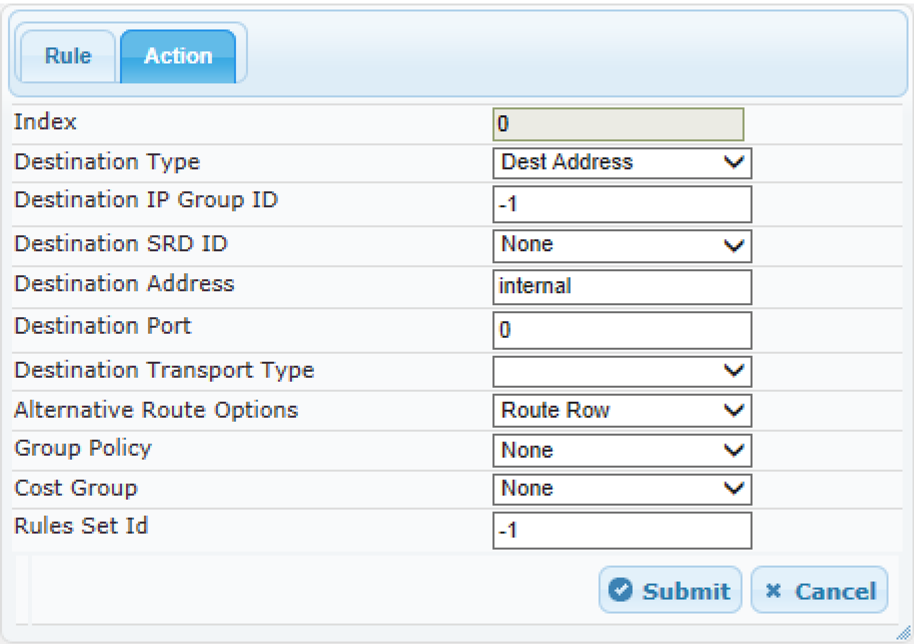
Figure 4-27: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



5. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**Dest Address**
Destination Address	**internal**

Figure 4-28: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

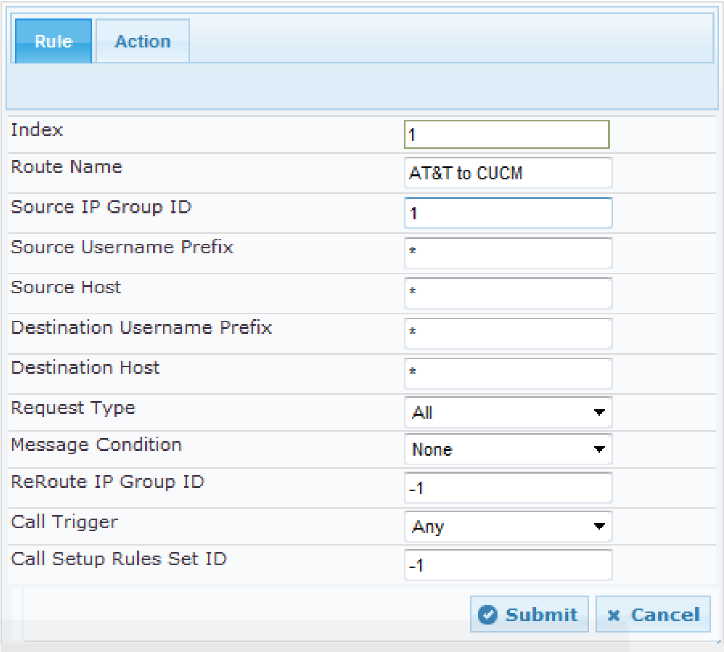


6. Configure a rule to route calls from AT&T IP Flexible Reach SIP Trunk to the Cisco CUCM:
7. Click **Add**.

8. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Route Name	**AT&T to CUCM** (arbitrary descriptive name)
Source IP Group ID	**1**

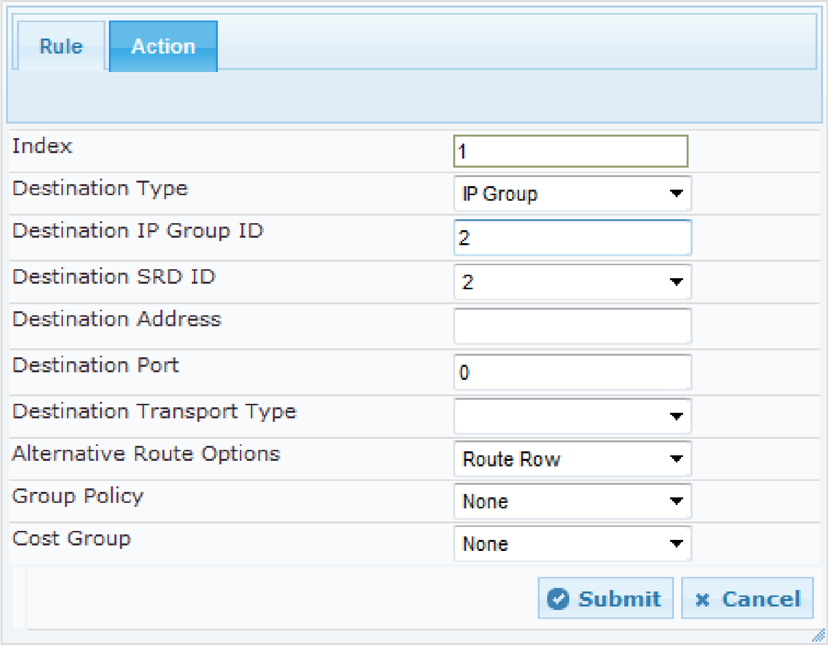
Figure 4-29: Configuring IP-to-IP Routing Rule for AT&T IP Flexible Reach to Cisco CUCM – Rule tab



9. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**2**
Destination SRD ID	**2**

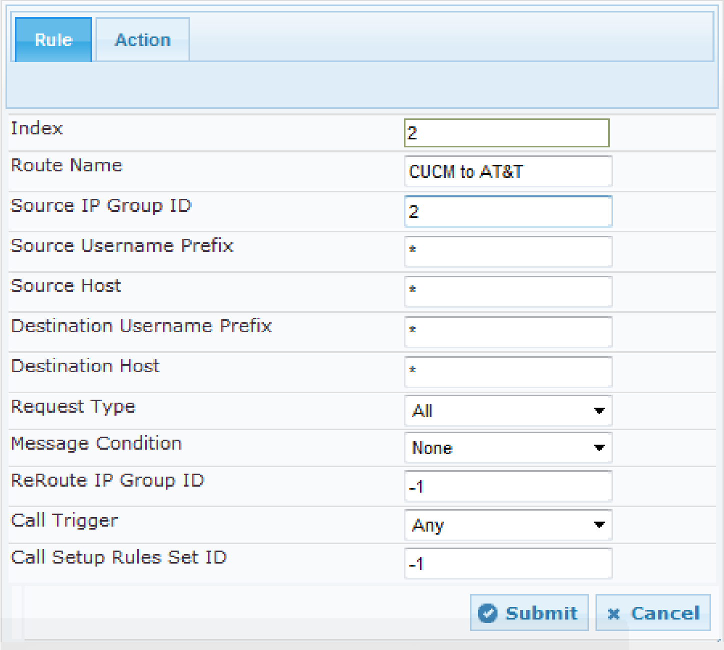
Figure 4-30: Configuring IP-to-IP Routing Rule for AT&T IP Flexible Reach to Cisco CUCM – Action tab



10. Configure a rule to route calls from Cisco CUCM to AT&T IP Flexible Reach SIP Trunk:
11. Click **Add**.
12. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Route Name	**CUCM to AT&T** (arbitrary descriptive name)
Source IP Group ID	**2**

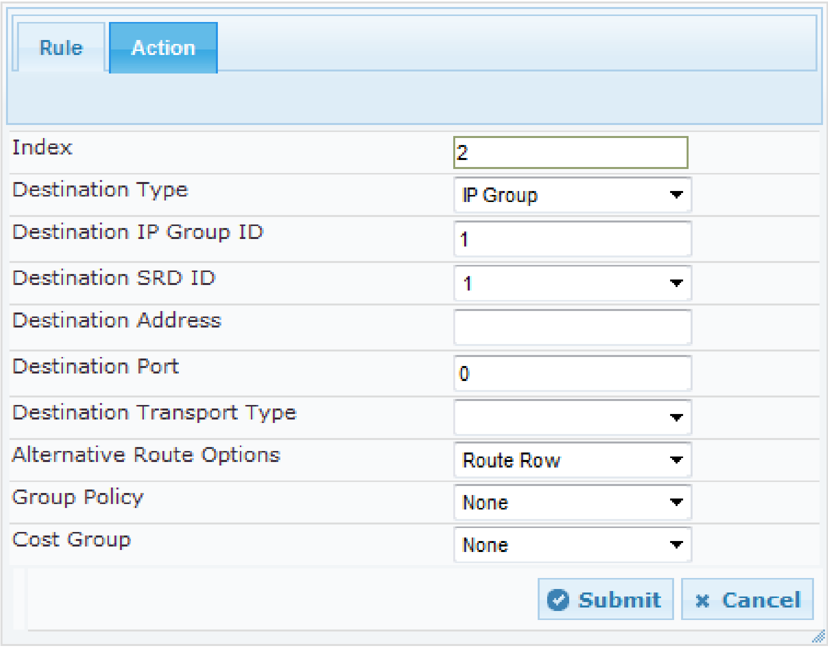
Figure 4-31: Configuring IP-to-IP Routing Rule for CUCM to ATT IP Flexible Reach – Rule tab



13. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 4-32: Configuring IP-to-IP Routing Rule for CUCM to ATT IPFR– Action tab



The configured routing rules are shown in the figure below:

Figure 4-33: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table

Add + Insert +

Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination SRD ID
0	OPTIONS	*	*	*	None	-1	Any	-1	Dest Address	None
1	AT&T to CUCM	*	*	*	None	-1	Any	-1	IP Group	2
2	CUCM to AT&T	*	*	*	None	-1	Any	-1	IP Group	1

Page 1 of 1 Show 10 records per page

Note: The routing configuration may change according to your specific deployment topology.

4.10 Step 10: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

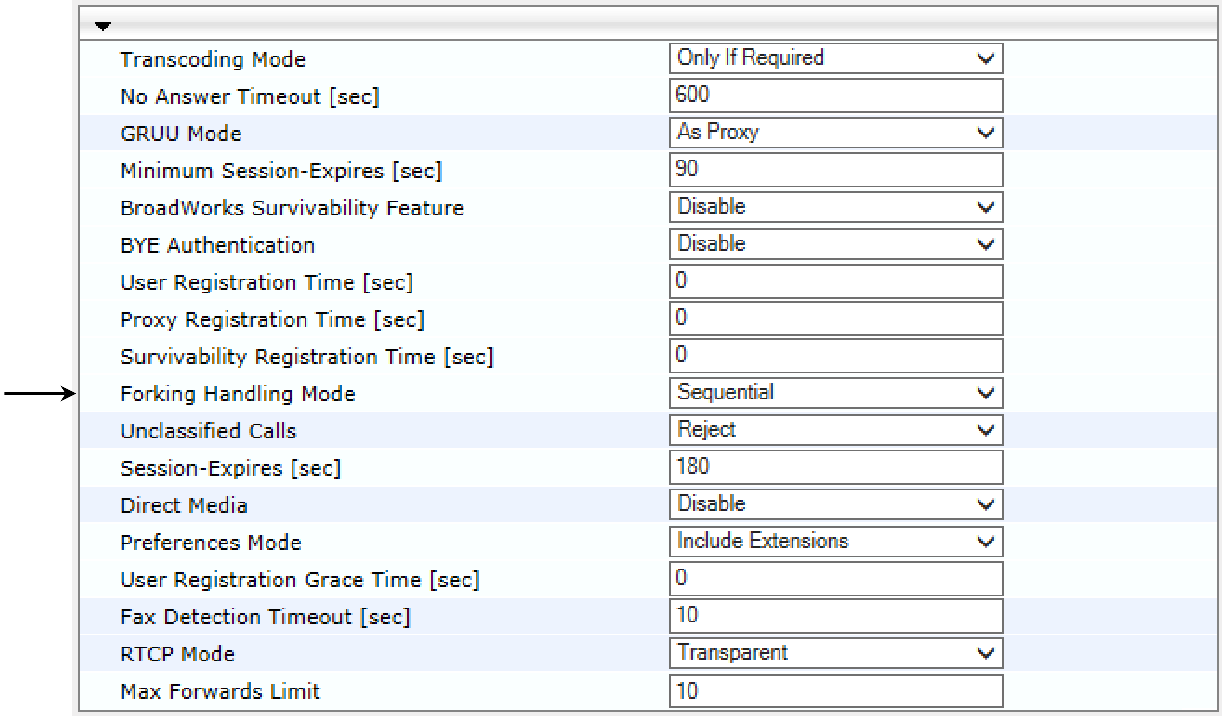
4.10.1 Step 10a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if 18x with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if 180 response without SDP is received.

➢ **To configure call forking:**

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-34: Configuring Forking Mode



3. Click **Submit**.

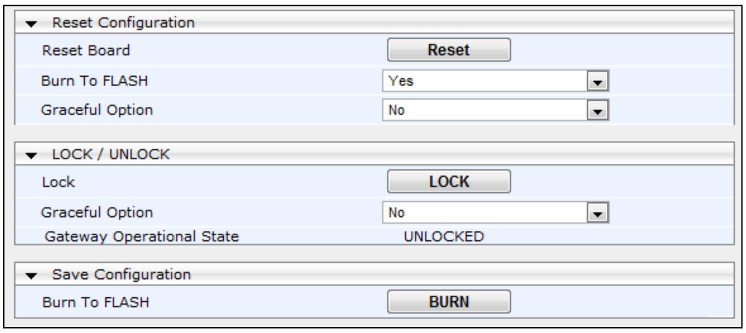
4.11 Step 11: Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

➢ **To save the configuration to flash memory:**

1. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

Figure 4-35: Resetting the E-SBC



2. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
3. Click the **Reset** button.

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Chapter 4 on page 17 is shown below:

Note: To load and save an ini file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

```
;**************
;** Ini File **
;**************

;Board: Mediant 800
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 2542001
;Slot Number: 1
;Software Version: 6.80A.227.005
;DSP Software Version: 5014AE3_R => 680.22
;Board IP Address: 10.15.20.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M   Flash size: 64M   Core speed: 300Mhz
;Num of DSP Cores: 1  Num DSP Channels: 50
;Num of physical LAN ports: 12
;Profile: NONE
;Key features:;Board Type: Mediant 800 ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;Channel Type: RTP DspCh=50
IPMediaDspCh=50 ;DSP Voice features: IpmDetector RTCP-XR
AMRPolicyManagement ;E1Trunks=1 ;T1Trunks=1 ;IP Media: Conf
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;Coders: G723 G729 G728
NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711
MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Control
Protocols: MGCP MEGACO H323 SIP TPNCP SASurvivability SBC=30 MSFT CLI
TRANSCODING=30 FEU=100 TestCall=100 ;Default features:;Coders: G711 G726;

;------ Mediant 800 HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
;      1 : Empty
;      2 : Empty
;      3 : Empty
;----------------------------------------------


[SYSTEM Params]

SSHServerEnable = 1
NTPServerIP = '0.0.0.0'

[BSP Params]

PCMLawSelect = 3
```

```
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

FarEndDisconnectType = 7

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

WebLogoText = 'CUCM2ATT-SBC'
UseWeblogo = 1
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

MEDIACHANNELS = 30
RADDEBLEVEL = 2
RADLOGOUTPUT = 1
GWDEBUGLEVEL = 5
T38USERTPPORT = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SCTP Params]


[IPsec Params]
```

```
[Audio Staging Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 1, 4, "User Port #11", "GROUP_6",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 2, "FE_5_1", "FE_5_2";
EtherGroupTable 3 = "GROUP_4", 2, "FE_5_3", "FE_5_4";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";
```

```
[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName;
DeviceTable 1 = 1, "GROUP_1", "LAN";
DeviceTable 2 = 2, "GROUP_2", "WAN";

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.20.10, 16, 10.15.0.1, 1, "Private",
0.0.0.0, 0.0.0.0, "LAN";
InterfaceTable 1 = 5, 10, 12.210.214.226, 29, 12.210.214.225, 2,
"Public", 0.0.0.0, 0.0.0.0, "WAN";


[ \InterfaceTable ]


[ ACCESSLIST ]

FORMAT ACCESSLIST_Index = ACCESSLIST_Source_IP, ACCESSLIST_Source_Port,
ACCESSLIST_PrefixLen, ACCESSLIST_Start_Port, ACCESSLIST_End_Port,
ACCESSLIST_Protocol, ACCESSLIST_Use_Specific_Interface,
ACCESSLIST_Interface_ID, ACCESSLIST_Packet_Size, ACCESSLIST_Byte_Rate,
ACCESSLIST_Byte_Burst, ACCESSLIST_Allow_Type;
ACCESSLIST 0 = "0.0.0.0", 0, 0, 0, 65535, "Any", 0, "", 0, 0, 0, "Allow";

[ \ACCESSLIST ]


[ DspTemplates ]

;
;  *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
```

```
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 1 = "MR_ATT", "Public", "", 6000, 100, 6990, 0, "", "";
CpMediaRealm 2 = "MR_CUCM", "Private", "", 8000, 10, 8090, 1, "", "";

[ \CpMediaRealm ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SRD_ATT", "MR_ATT", 0, 0, -1, 1;
SRD 2 = "SRD_CUCM", "MR_CUCM", 0, 0, -1, 1;

[ \SRD ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "12.194.231.76:5060", 0, 1;
ProxyIp 2 = "10.15.25.11:5060", 0, 2;

[ \ProxyIp ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
```

```
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;
IpProfile 1 = "ATT", 1, 1, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "", 1, -1, 2, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300;
IpProfile 2 = "CUCM", 1, 2, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0, 1, "", 2, -1, 2, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300;

[ \IpProfile ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, "-1", -1, -1, "";
ProxySet 1 = "ATT IPFR", 0, 60, 0, 0, 1, 0, "-1", -1, -1, "";
ProxySet 2 = "CUCM", 0, 60, 0, 0, 2, 0, "-1", -1, -1, "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "ATT IPFR", 1, "", "", 0, -1, -1, 0, -1, 1, "MR_ATT", 1,
1, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0,
"", "";
```

```
IPGroup 2 = 0, "CUCM", 2, "", "", 0, -1, -1, 0, -1, 2, "MR_CUCM", 1, 2, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "";

[ \IPGroup ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName, IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType, IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions, IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS", -1, "*", "*", "*", "*", 6, "", -1, 0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "AT&T to CUCM", 1, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "CUCM to AT&T", 2, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 1, "1", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion, TLSContexts_ServerCipherString, TLSContexts_ClientCipherString, TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0, 2560, 0;

[ \TLSContexts ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName, SIPInterface_NetworkInterface, SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable, SIPInterface_ClassificationFailureResponseType, SIPInterface_PreClassificationManSet;
SIPInterface 0 = "ATT IPFR", "Public", 2, 5060, 0, 0, 1, "", "", -1, 0, 500, -1;
SIPInterface 1 = "CUCM", "Private", 2, 5060, 0, 0, 2, "", "", -1, 0, 500, -1;

[ \SIPInterface ]



[ CodersGroup0 ]
```

```
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0;

[ \CodersGroup0 ]


[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = "g729", 20, 0, -1, 0;

[ \CodersGroup1 ]


[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0;

[ \CodersGroup2 ]




[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g729";

[ \AllowedCodersGroup1 ]


[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g711Ulaw64k";
AllowedCodersGroup2 1 = "g729";

[ \AllowedCodersGroup2 ]


[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]
```

```
FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]
```

This page is intentionally left blank.

B Configuring Analog Devices (ATA's) for FAX Support

This section describes how to configure the analog device entity to route its calls to the AudioCodes Media Gateway for supporting faxes. The analog device entity must be configured to send all calls to the Cisco Unified Communication Manager.

Note: The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series.

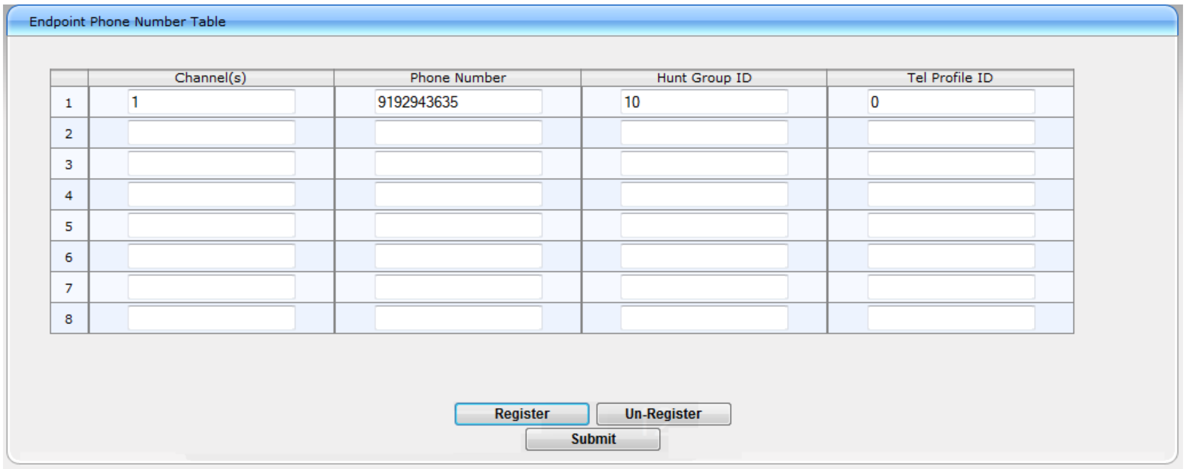
B.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number ''9192943635'' (IP address 10.15.45.20) with all routing directed to the Cisco CUCM device (10.15.25.11).

➢ **To configure the Endpoint Phone Number table:**

- Open the Endpoint Phone Number Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Hunt Group** sub-menu > **Endpoint Phone Number**).

Figure B-1: Endpoint Phone Number Table Page



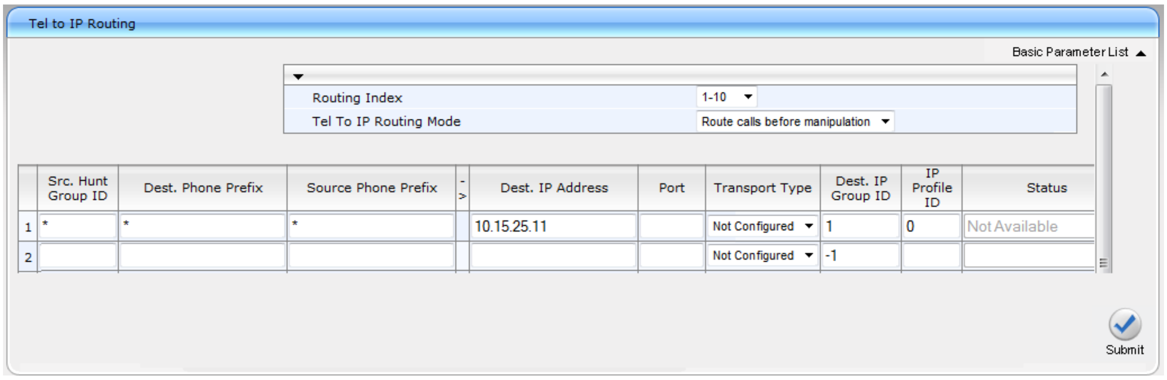
B.2 Step 2: Configure Tel to IP Routing Table

This step describes how to configure the Tel-to-IP routing rules to ensure that the MP-11x device sends all calls to the AudioCodes central E-SBC device.

➢ **To configure the Tel to IP Routing table:**

- Open the Tel to IP Routing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** sub-menu > **Tel to IP Routing**).

Figure B-2: Tel to IP Routing Page



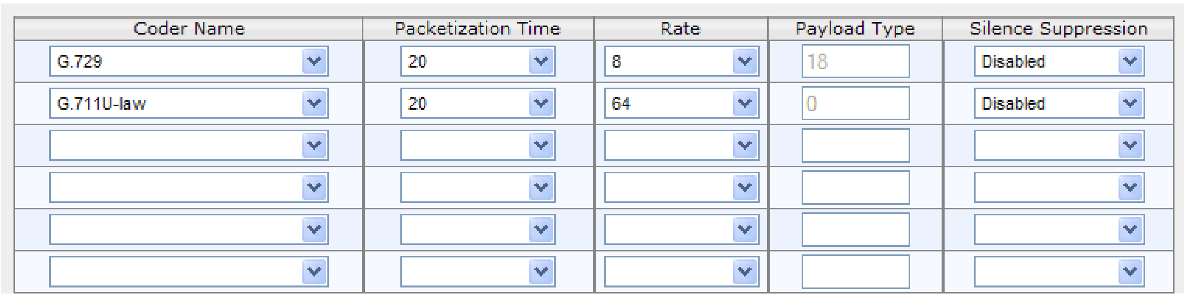
B.3 Step 3: Configure Coders Table

This step describes how to configure the coders for the MP-11x device.

➢ **To configure MP-11x coders:**

- Open the Coders page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** sub-menu > **Coders**).

Figure B-3: Coders Table Page



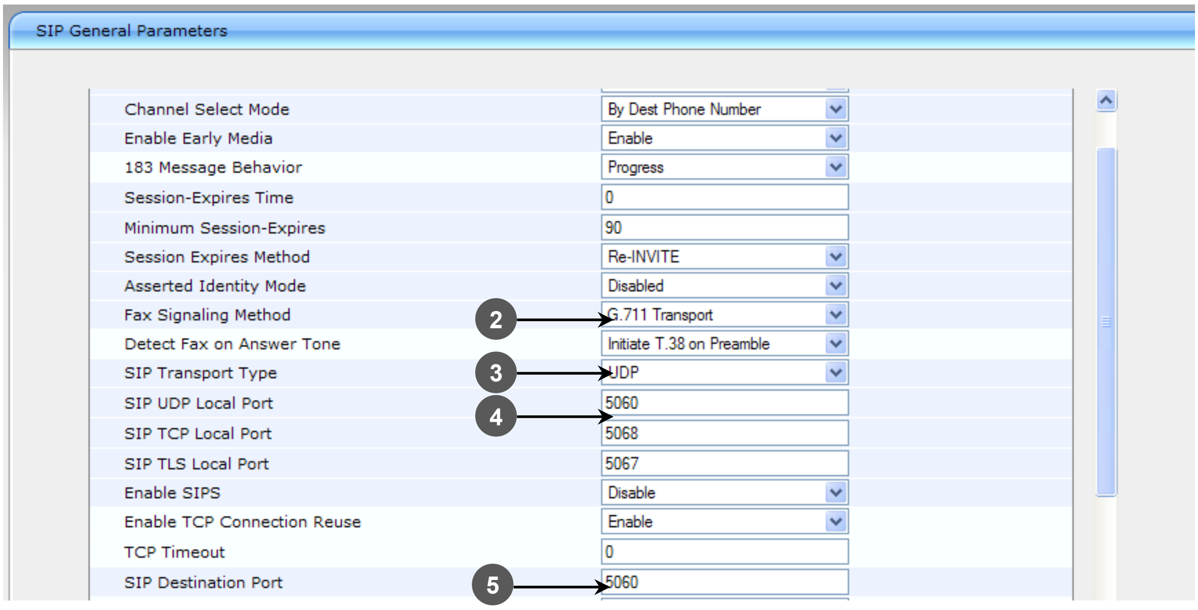
B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

This step describes how to configure the fax signaling method for the MP-11x device.

➢ **To configure the fax signaling method:**

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).

Figure B-4: SIP General Parameters Page



2. From the 'FAX Signaling Method' drop-down list, select **G.711 Transport** for G.711 fax support and select **T.38 Relay** for T.38 fax support**.**
3. From the 'SIP Transport Type' drop-down list, select **UDP**.
4. In the 'SIP UDP Local Port' field, enter **5060** (corresponding to the Central Gateway UDP transmitting port configuration).
5. In the 'SIP Destination Port', enter **5060** (corresponding to the Central Gateway UDP listening port configuration).

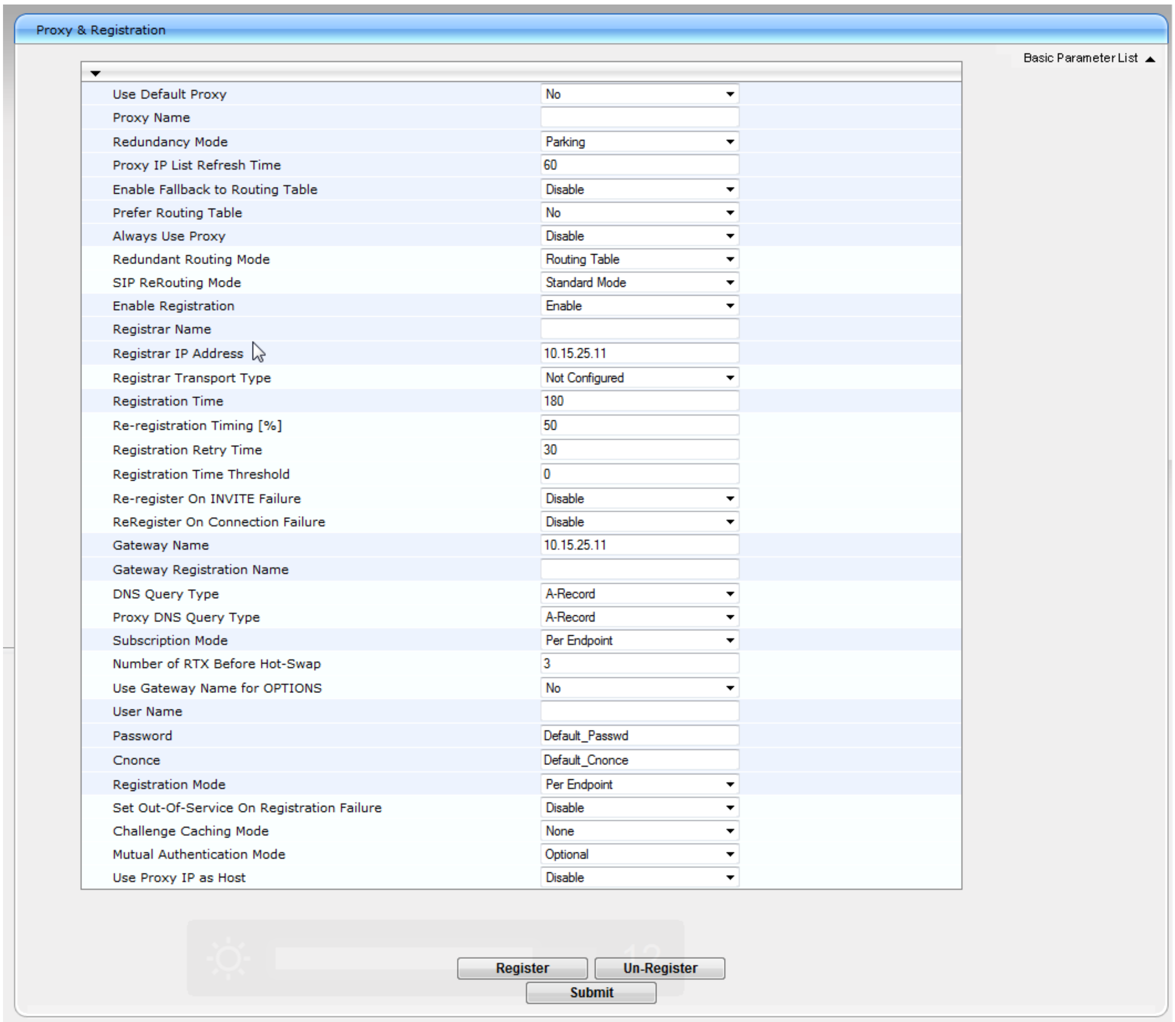
B.5 Step 5: Configure Registration

This step describes how to configure SIP registration toward the Cisco CUCM. This is required so that the analog end point within the MP11x can register with the Cisco CUCM on behalf of the fax machine. The Cisco CUCM requires registration to provide service.

➢ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy and Registration**).

Figure B-5: Configuring SIP Registration Account



2. Configure the following parameters according to the provided information for a Cisco CUCM end-point, for example:

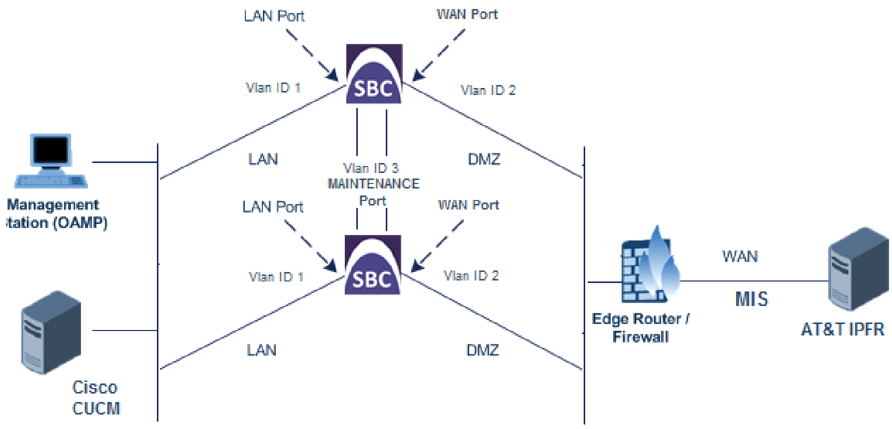
Parameter	Value
Enable Registration	**Enable**
Registrar IP Address	**10.15.25.11**
Gateway Name	10.15.25.11
Registration Mode	Per Endpoint

3. Click **Submit**.

C Configuring AudioCodes E-SBC for High Availability

The figure below shows the configuration of the AudioCodes E-SBC devices for High Availability.

Figure C-1: AudioCodes E-SBC with High Availability



C.1 Configure the HA Devices

This section describes how to initially configure the two devices comprising the HA system. This configuration is done in the following order:

1. Configure the first device for HA – see Section C.1.1 on page 66.
2. Configure the second device for HA - see Section C.1.2 on page 68.
3. Activate HA on the devices - see Section C.1.3 on page 69.

Notes:

- The HA feature is available only if both devices are installed with a Software License Key that includes this feature.
- The physical connections of the first and second devices to the network (i.e., Maintenance interface and OAMP, Control and Media interfaces) **must be identical**. This also means that the two devices must also use the same Ethernet Port Groups and the port numbers belonging to these Ethernet Port Groups. For example, if the first device uses Ethernet Port Group 1 (with ports 1 and 2), the second device must also use Ethernet Port Group 1 (with ports 1 and 2).
- Before configuring HA, determine the required network topology.
- The Maintenance network should be able to perform a fast switchover in case of link failure and thus, Spanning Tree Protocol (STP) should not be used in this network; the Ethernet connectivity of the Maintenance interface between the two devices should be constantly reliable without any disturbances.

C.1.1 Step 1: Configure the First Device

The first stage is to configure the first device for HA, as described in the procedure below:

> **Note:** During this stage, ensure that the second device is powered off or disconnected from the network.

➢ **To configure the first device for HA:**

1. Configure the network interfaces, including the default OAMP interface:
   a. Connect your PC to the device using a local, direct physical cable connection and then access the Web interface using the default OAMP network address
   b. Open the Interface table (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
   c. Change the default OAMP network settings to suite your networking scheme.
   d. Configure the Control and Media network interfaces, as required as was noted in Step 1 in Section 4.1 on page 18.
   e. Add the HA Maintenance interface (i.e., the **MAINTENANCE** Application Type).

> **Note:** Make sure that the MAINTENANCE interface uses an Ethernet Port Group that is not used by any other network interface. The Ethernet Port Group is associated with the Ethernet Device assigned to the interface in the 'Underlying Interface' field.

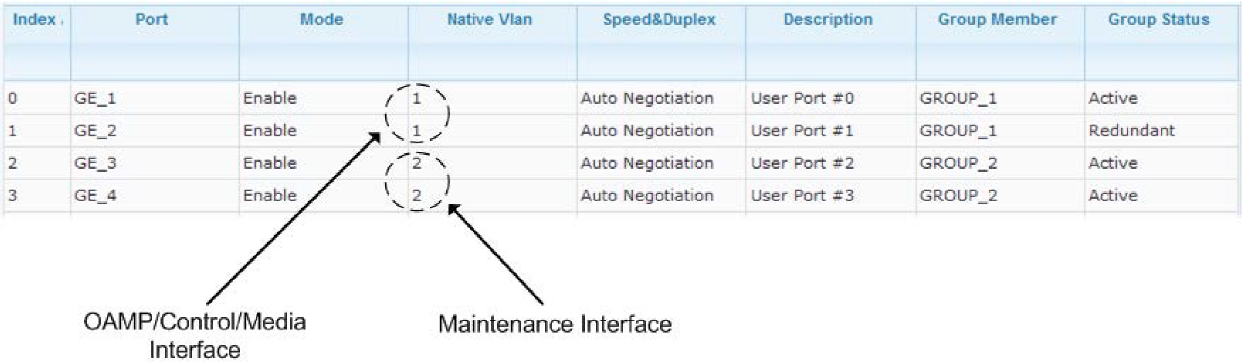
The Interface table below shows an example where the Maintenance interface is assigned to Ethernet Device "vlan 2" (which is associated with Ethernet Port Group "GROUP_2") in the 'Underlying Device' field, while the other interface is assigned to "vlan 1" (associated with "GROUP_1"):

Figure C-2: Interface Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media	IPv4 Manual	10.8.40.47	16	10.8.0.1	Voice			vlan 1
1	MAINTENANCE	IPv4 Manual	10.3.0.11	16	10.3.0.1	Unknown	0.0.0.0	0.0.0.0	vlan 2

2. If the connection is through a switch, the packets of both interfaces should generally be untagged. In such a scenario, set the Native VLAN ID of each Ethernet Port Group so that it is the same as the VLAN ID set for each interface assigned to that Ethernet Port Group. The Native VLAN ID is configured in the Physical Ports Settings page (see "Configuring Physical Ethernet Ports". The figure below shows an example whereby the Native VLAN IDs of the Ethernet Port Groups are set to the same VLAN IDs of the interfaces using these Ethernet Port Groups:

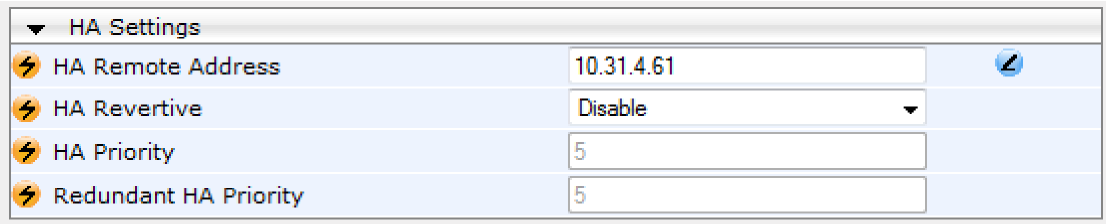
Figure C-3: Ethernet Port Groups



Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Active

3. Set the Ethernet port Tx / Rx mode of the Ethernet Port Group used by the Maintenance interface. This is configured in the Ethernet Group Settings page. The port mode depends on the type of Maintenance connection between the devices, as described in "Network Topology Types and Rx/Tx Ethernet Port Group Settings" on page 367.
4. Configure the HA parameters in the HA Settings page (**Configuration** tab > **System** menu > **HA Settings**):

Figure C-4: HA Settings



   a. In the 'HA Remote Address' field, enter the Maintenance IP address of the **second** device.
   b. (Optional) Enable the Revertive mode by setting the 'HA Revertive' parameter to **Enable** and then setting the priority level of this device in the 'HA Priority' field.
5. Burn the configuration to flash **without** a reset.
6. Power down the device.
7. Proceed to Section C.1.2 on page 68.

C.1.2 Step 2: Configure the Second Device

Once you have configured the first device for HA, you can configure the second device for HA. As the configuration of the second device is similar to the first device, the procedure below briefly describes each procedural step.

> **Note:** During this stage, ensure that the first device is powered off or disconnected from the network..

➤ **To configure the second device for HA:**

1. Connect to the device in the same way as you did with the first device.
2. Open the Interface table (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
3. Configure the **same** OAMP, Media, and Control interfaces as you configured for the first device.
4. Configure a Maintenance interface for this device. The IP address must be different to that configured for the Maintenance interface of the first device. However, the Maintenance interfaces of the devices must be in the same subnet.
5. Configure the **same** Native VLAN IDs of the Ethernet Port Groups and VLAN IDs of the network interfaces as you configured for the first device.
6. Configure the **same** Ethernet port Tx / Rx mode of the Ethernet Port Group used by the Maintenance interface as you configured for the first device.
7. Configure the HA parameters in the HA Settings page (**Configuration** tab > **System** menu > **HA Settings**):
   a. In the 'HA Remote Address' field, enter the Maintenance IP address of the **first** device.
   b. (Optional) Enable the Revertive mode by setting the 'HA Revertive' field to **Enable** and then setting the priority level of this second device in the 'HA Priority' field.
8. Burn the configuration to flash **without** a reset.
9. Power down the device.
10. Proceed to C.1.3 on page 69.for completing the HA configuration.

C.1.3 Step 3: Initialize HA on the Devices

Once you have configured both devices for HA as described in the previous sections, follow the procedure below to complete and initialize HA so that the devices become operational in HA. This last stage applies to both devices.

➢ **To initialize the devices for HA:**

1. Cable the devices to the network.

> **Note:** You must connect both ports (two) in the Ethernet Port Group of the Maintenance interface to the network (i.e., two network cables are used). This provides 1+1 Maintenance port redundancy.

2. Power up the devices; the redundant device synchronizes with the active device and updates its configuration according to the active device. The synchronization status is indicated as follows:
   - Active device: The Web interface's Home page displays the HA status as "Synchronizing".
   - Redundant device: The LED is lit yellow on the E-SBC module.

   When synchronization completes successfully, the redundant device resets to apply the received configuration and software.

   When both devices become operational in HA, the HA status is indicated as follows:
   - Both devices: The Web interface's Home page displays the HA status as "Operational".
   - Active device: The LED is lit green
   - Redundant device: The LED flashes yellow
3. Access the active device with its OAMP IP address and configure the device as required.

C.2 Configuration While HA is Operational

When the devices are operating in HA state, the subsequent configuration is as follows:

- All configuration, including HA is done on the active device only.
- Non-HA configuration on the active device is automatically updated on the redundant device (through the Maintenance interface).
- HA-related configuration on the active device is automatically updated on the redundant device:
  - Maintenance interface:
    - Modified Maintenance interface address of the active device: this address is set as the new 'HA Remote Address' value on the redundant device.
    - Modified 'HA Remote Address' value on the active device: this address is set as the new Maintenance interface address on the redundant device. This requires a device reset.
    - Modifications on all other Maintenance interface parameters (e.g., Default Gateway and VLAN ID): updated to the Maintenance interface on the redundant device:
      - ✓ 'HA Revertive' mode (this requires a device reset).
      - ✓ 'HA Priority' parameter is set for the active device.
      - ✓ Modified 'Redundant HA Priority' value is set for the redundant device. This requires a device reset.

Note: If the HA system is already in Revertive mode and you want to change the priority of the device, to ensure that system service is maintained and traffic is not disrupted, it is recommended to set the higher priority to the redundant device and then reset it. After it synchronizes with the active device, it initiates a switchover and becomes the new active device (the former active device resets and becomes the new redundant device).

This page is intentionally left blank.

Configuration Note