AudioCodes Mediant™ Series

Enterprise Session Border Controllers (E-SBC)

Interoperability Laboratory

Configuration Note

Connecting Microsoft® Lync™ Server 2010/2013 with AT&T IP Flexible Reach (Enhanced Features) using AudioCodes E-SBC

March 2013

Document #: LTRT-38101

Table of Contents

1 Introduction 11

1.1 Intended Audience 11
1.2 About AudioCodes E-SBC Product Series 11

2 Component Information 13

2.1 AudioCodes E-SBC Version 13
2.2 AT&T IP Flexible Reach – EF Service Version 13
2.3 Microsoft Lync Server 2013 Version 13
2.4 AudioCodes Fax Supporting ATA Version 14
2.5 Deploying the E-SBC - Typical Topology 15
2.6 Environment Setup 16
2.7 Known Limitations 17
2.8 AT&T Enhanced Service Offering 18

3 Configuring Lync Server 2013 19

3.1 Configure the E-SBC as an IP / PSTN Gateway 19
3.2 Configuring the "Route" on Lync Server 2013 27

4 Configuring AudioCodes E-SBC 39

4.1 Step 1: Network Interface Configuration 40
4.1.1 Step 1a: Configure IP Network Interfaces 41
4.1.2 Step 1b: Configure the Native VLAN ID 42
4.2 Step 2: Enable the SBC Application 43
4.3 Step 3: Signaling Routing Domains 44
4.3.1 Step 3a: Configure RTP/RTCP Base Level Media settings 44
4.3.2 Step 3b: Configure Media Realms 45
4.3.3 Step 3c: Configure SRDs 47
4.3.4 Step 3d: Configure SIP Signaling Interfaces 48
4.4 Step 4: Configure Proxy Sets 49
4.5 Step 5: Configure IP Groups 52
4.6 Step 6: Configure IP Profiles 54
4.7 Step 7: Configure Coders 60
4.8 Step 8: SIP TLS Connection Configuration 62
4.8.1 Step 8a: Configure the NTP Server Address 62
4.8.2 Step 8b: Configure a Certificate 63
4.9 Step 9: Configure SRTP 68
4.10 Step 10: Configure Number of Media Channels 69
4.11 Step 11: Configure IP-to-IP Call Routing Rules 70
4.12 Step 12: Configure IP-to-IP Manipulation 78
4.13 Step 13: Configure SIP Message Manipulation Rules 84
4.14 Step 15: Miscellaneous Configuration 99
4.14.1 Step 15a: Configure DNS Query Methods 99
4.14.2 Step 15b: Configure Forking Mode 100
4.14.3 Step 15c: Configure SRTP Behavior upon Rekey Mode 101
4.15 Step 16: Reset the E-SBC 103

A AudioCodes INI File 105

B Configuring Analog Devices (ATA's) 115

B.1 Step 1: Configure IP Address of the MP-11x 115
B.2 Step 2: Configure Endpoint Phone Numbers 116
B.3 Step 3: Configure Tel-to-IP Routing Rules 117
B.4 Step 4: Configure Coders for MP-11x 118
B.5 Step 5: Configure SIP UDP Transport Type and Fax Signaling Method 119
B.6 Step 6: Configure Base Media Fax Settings 120

List of Figures

Figure 2-1: E-SBC Interworking Microsoft Lync and AT&T IP Flexible Reach - EF Service Topology Example 15
Figure 3-1: Starting the Lync Server Topology Builder 19
Figure 3-2: Topology Builder Options 20
Figure 3-3: Saving the Topology 20
Figure 3-4: Displaying Downloaded Topology 21
Figure 3-5: Choosing New IP/PSTN Gateway 21
Figure 3-6: Defining the New IP/PSTN Gateway 22
Figure 3-7: Defining the IP Address 22
Figure 3-8: Defining the Root Trunk 23
Figure 3-9: Adding E-SBC as an IP/PSTN Gateway and Creating a Trunk 24
Figure 3-10: Selecting Publish Topology from the Action Menu 24
Figure 3-11: Publishing Topology 25
Figure 3-12: Publishing the Topology in Progress 25
Figure 3-13: Publishing Topology Successfully Completed 26
Figure 3-14: Opening the Lync Server Control Panel 27
Figure 3-15: Entering Lync Server Credentials 28
Figure 3-16: Displaying Microsoft Lync Server 2013 Control Panel 28
Figure 3-17: Selecting Voice Routing 29
Figure 3-18: Selecting the Route Option 30
Figure 3-19: Adding a New Voice Route 30
Figure 3-20: Adding a New Trunk 31
Figure 3-21: Displaying Deployed Trunks 32
Figure 3-22: Selecting E-SBC Trunk 33
Figure 3-23: Associating PSTN Usage to Route 34
Figure 3-24: Confirming New Voice Route 34
Figure 3-25: Committing Voice Routes 34
Figure 3-26: Un-committing Voice Configuration Settings 35
Figure 3-27: Confirming Successful Voice Routing Configuration 36
Figure 3-28: Displaying Voice Routing Committed Routes 37
Figure 4-1: Configuring Network Interfaces 40
Figure 4-2: Configuring IP Network Interfaces 41
Figure 4-3: Configuring Native VLAN ID 42
Figure 4-4: Enabling SBC Application 43
Figure 4-5: Configuring RTP/RTCP Base Port Settings 44
Figure 4-6: Configuring LAN Media Realm 45
Figure 4-7: Configuring WAN Media Realm 46
Figure 4-8: Displaying Configured Media Realm 46
Figure 4-9: Configuring LAN SRDs 47
Figure 4-10: Configuring WAN SRDs 47
Figure 4-11: Displaying Configured SIP Interfaces 48
Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013 49
Figure 4-13: Configuring Proxy Set for AT&T IP Flexible Reach - EF Service 50
Figure 4-14: Configuring Proxy Set for Fax Supporting ATA 51
Figure 4-15: Configuring IP Groups 53
Figure 4-16: Configuring IP Profile for Lync Server 2013 55
Figure 4-17: Configuring IP Profile for AT&T IP Flexible Reach - EF Service 57
Figure 4-18: Configuring IP Profile for Fax Supporting ATA 59
Figure 4-19: Configuring Coders for Lync Server 2013 60
Figure 4-20: Configuring Coders for AT&T IP Flexible Reach - EF Service 60
Figure 4-21: Setting Preferred Coder for AT&T IP Flexible Reach - EF Service 61
Figure 4-22: Setting Preferred Coder for Lync Server 2013 61
Figure 4-23: Configuring NTP Server Address 62
Figure 4-24: Configuring Certificates 63
Figure 4-25: Navigating to Microsoft Certificate Services Web Site 64
Figure 4-26: Requesting a Certificate 64
Figure 4-27: Selecting Advanced Certificate Request 65

Figure 4-28: Submitting a Certificate Request 65
Figure 4-29: Displaying Certificate Issued....66
Figure 4-30: Downloading a CA Certificate 66
Figure 4-31: Uploading Certificate....67
Figure 4-32: Configuring Media Security....68
Figure 4-33: Configuring the Number of Media Channels....69
Figure 4-34: Configuring IP-to-IP Routing Rules....71
Figure 4-35: Adding Rule to Terminate SIP Options from LAN....72
Figure 4-36: Adding Rule to Terminate SIP Options from ATA....73
Figure 4-37: Configuring IP-to-IP Routing Rule for LAN to WAN....74
Figure 4-38: Configuring IP-to-IP Routing Rule for WAN to LAN Fax ATA....75
Figure 4-39: Configuring IP-to-IP Routing Rule for WAN to LAN....76
Figure 4-40: Configuring IP-to-IP Routing Rule for WAN to LAN....77
Figure 4-41: Displaying Configured IP-to-IP Routing Rules....77
Figure 4-42: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab....78
Figure 4-43: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab....79
Figure 4-44: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab....79
Figure 4-45: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab....80
Figure 4-46: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab....80
Figure 4-47: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab....81
Figure 4-48: Configuring IP to IP Inbound Manipulation Rules....81
Figure 4-49: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab....82
Figure 4-50: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab....83
Figure 4-51: Configuring IP to IP Outbound Manipulation Rules....83
Figure 4-52: Configuring SIP Message Manipulation – Index 1....84
Figure 4-53: Configuring SIP Message Manipulation – Index 6....85
Figure 4-54: Configuring SIP Message Manipulation – Index 7....86
Figure 4-55: Configuring SIP Message Manipulation – Index 8....87
Figure 4-56: Configuring SIP Message Manipulation – Index 9....88
Figure 4-57: Configuring SIP Message Manipulation – Index 10....89
Figure 4-58: Configuring SIP Message Manipulation – Index 11....90
Figure 4-59: Configuring SIP Message Manipulation – Index 12....91
Figure 4-60: Configuring SIP Message Manipulation – Index 13....92
Figure 4-61: Configuring SIP Message Manipulation – Index 14....93
Figure 4-62: Configuring SIP Message Manipulation – Index 15....94
Figure 4-63: Configuring SIP Message Manipulation – Index 16....95
Figure 4-64: Configuring SIP Message Manipulation – Example....96
Figure 4-65: Assigning Manipulation Rule to IP Group 1....97
Figure 4-66: Assigning Manipulation Rule to IP Group 2....98
Figure 4-67: Configuring DNS Query Methods....99
Figure 4-68: Configuring Forking Mode....100
Figure 4-69: Configuring SRTP Behavior upon Rekey Mode....101
Figure 4-70: Resetting the E-SBC....103
Figure 4-71: Configuring IP Address of the MP-11x....115
Figure 4-72: Configuring Endpoint Phone Numbers....116
Figure 4-73: Configuring Tel-to-IP Routing Rules....117
Figure 4-74: Configuring Coders for MP-11x....118
Figure 4-75: Configuring SIP UDP Transport Type and Fax Signaling Method....119
Figure 4-76: Configuring Base Media Fax Settings....120

List of Tables

Table 2-1: AudioCodes E-SBC Version 13
Table 2-2: AT&T IP Flexible Reach - EF Service Version....13
Table 2-3: Microsoft Lync Server 2013 Version 13
Table 2-4: AudioCodes Fax Supporting ATA Version....14
Table 2-5: Environment Setup....16

Reader's Notes

Notice

This document describes how to connect the Microsoft Lync Server 2013 and AT&T IP Flexible Reach – Enhanced Features with MIS, PNT or AVPN transport 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: March-21-2013

Trademarks

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 service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

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.

Note: Throughout this manual, unless otherwise specified, the term *E-SBC* refers to the AudioCodes device.

Reader's Notes

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as E-SBC) for interworking between AT&T IP Flexible Reach – Enhanced Features (EF) service for SIP trunks and Microsoft's Lync Communication platform.

1.1 Intended Audience

The document is intended as an example guide for engineers, or AudioCodes and AT&T IP Flexible Reach – EF service partners who are responsible for installing and configuring AT&T IP Flexible Reach - EF service and Microsoft's Lync Communication platform 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 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.

Reader's Notes

2 Component Information

The section below describes component information for connecting the Microsoft Lync Server 2013 and AT&T IP Flexible Reach - EF service using AudioCodes Mediant E-SBC.

2.1 AudioCodes E-SBC Version

The table below describes the 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 with Network Expansion Module ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.60A.031.014
Protocol	▪ SIP/UDP (to the AT&T IP Flexible Reach - EF service) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 AT&T IP Flexible Reach – EF Service Version

The table below describes the AT&T IP Flexible Reach - EF Service Version.

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

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

2.3 Microsoft Lync Server 2013 Version

The table below describes the Microsoft Lync Server 2013 Version.

Table 2-3: Microsoft Lync Server 2013 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2013
Protocol	SIP
Additional Notes	None

2.4 AudioCodes Fax Supporting ATA Version

The table below describes the AudioCodes Fax Supporting ATA Version (Optional)

Table 2-4: AudioCodes Fax Supporting ATA Version

SBC Vendor	AudioCodes
Models	▪ Media Pack 1xx series Analog Gateways ▪ Mediant 800 Gateway & E-SBC with FXS interfaces ▪ Mediant 1000B Gateway & E-SBC with FXS module
Software Version	SIP_ 6.60A.035.004 (as tested on stand-alone MP 1xx) Would be same base load as E-SBC for the 800/1000B series devices.
Protocol	SIP/UDP (to the AudioCodes E-SBC)
Additional Notes	Support of Fax using T38 (initiating call in the G729 codec and transitioning to T38)

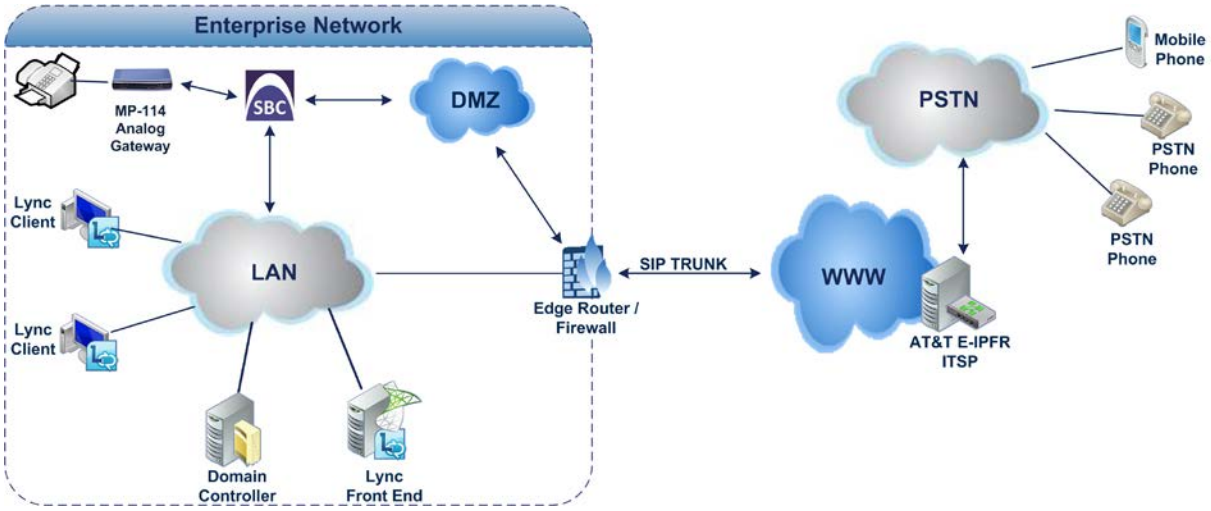
2.5 Deploying the E-SBC - Typical Topology

The procedures in this document describe how to deploy the E-SBC using the following example scenario:

- The Enterprise is deployed with Microsoft Lync Server 2013 in its private network for enhanced communication within the Enterprise.
- The Enterprise wants to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using AT&T IP Flexible Reach – EF SIP Trunking service (Internet Telephony Service Provider / ITSP).
- 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 Lync Server 2013 network in the Enterprise LAN and AT&T IP Flexible Reach – EF Service SIP Trunk located in the public network.

The figure below illustrates E-SBC interworking between Lync Server 2013 and AT&T IP Flexible Reach - EF Service SIP Trunking site.

Figure 2-1: E-SBC Interworking Microsoft Lync and AT&T IP Flexible Reach - EF Service Topology Example



2.6 Environment Setup

The example scenario includes the following environment setup:

Table 2-5: Environment Setup

Area	Setup
Network	▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN ▪ AT&T IP Flexible Reach - EF service is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 functions with SIP-over-TLS transport type ▪ AT&T IP Flexible Reach - EF service operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ AT&T IP Flexible Reach - EF service supports G.729 coder and G.711U-law
Media Transcoding	▪ Microsoft Lync Server 2013 operates with the SRTP media type ▪ AT&T IP Flexible Reach - EF service operates with the RTP media type
Media handling	▪ AT&T IP Flexible Reach - EF Service requires the RTP/RTCP media to be send in the range of 16384-32767

2.7 Known Limitations

The following limitations were observed in the Interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and AT&T IP Flexible Reach - EF Service:

1. **Network call forward non-reachable:** This feature is only supported when either the customer edge router or the AT&T IP Flexible Reach circuit are down. Since Lync returns a 183 message prior to Lync related non-reachable messages, network-based call forwarding non-reachable will not be invoked for these Lync outage scenarios.
2. **Network call forward busy:** For the same reason as above, network call forwarding on busy will not be invoked for a Lync busy condition.
3. **AT&T IP Teleconferencing functionality:** A Lync Server 2013 user must first set up the AT&T IP Teleconference bridge prior to adding a local Lync bridge to the call scenario. If the user first creates a Lync based conference bridge and then attempts to add into the local conference an AT&T IP Teleconferencing bridge, then the conference bridge PIN number will not be transmitted over the SIP trunk. This is by design so that the local users of the Lync conference bridge do not become exposed to audible DTMF.
4. **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.

2.8 AT&T Enhanced Service Offering

Enhanced Feature	Support
Network-Based Simultaneous Ringing Feature	Supported
Network-Based Locate Me (Sequential Ringing Feature)	Supported
Network-Based Blind Call Transfer	Not Supported
Network-Based Call Forward Unconditional (CFA, CFU)	Supported
Network-Based Call Forward Not Reachable (CF-NR)	Supported **Note:** This feature is only supported when either the customer edge router or the AT&T IP Flexible Reach circuit are down. Since Lync returns a SIP 183 response prior to Lync-related non-reachable messages, network-based call forwarding non-reachable will not be invoked for these Lync outage scenarios.
Network-Based Call Forward Busy (CF Busy)	Not Supported **Note:** For the same reason as above, network call forwarding on busy will not be invoked for a Lync busy condition.
Network-Based Call Forward Ring No Answer (CF-RNA)	Supported

3 Configuring Lync Server 2013

This section describes how to configure Microsoft Lync Server 2013 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.

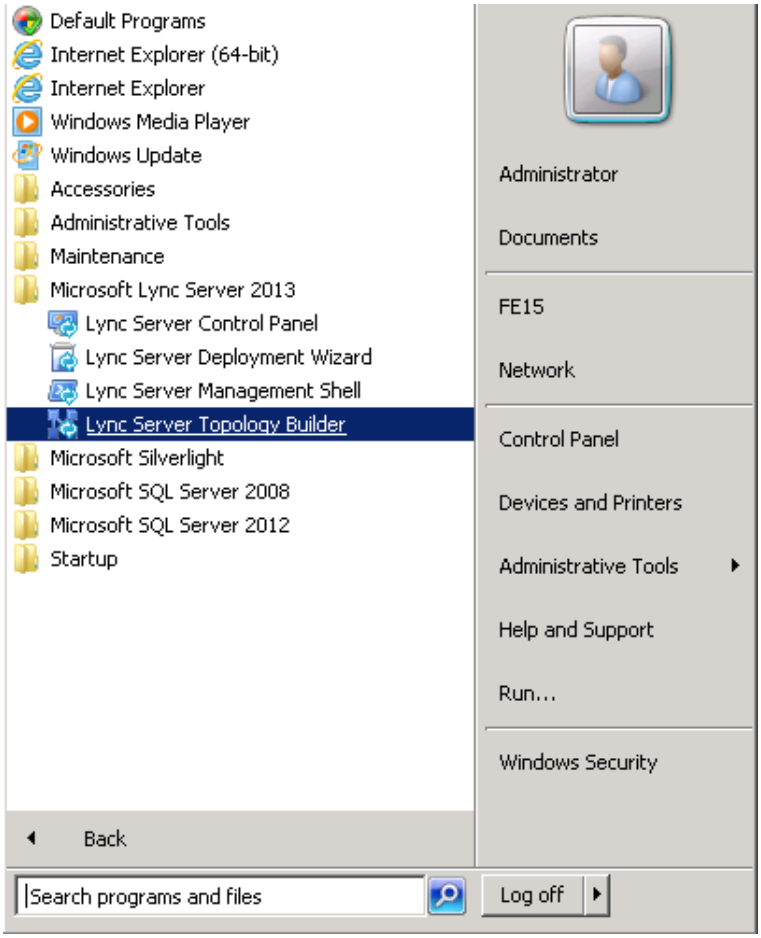
3.1 Configure the E-SBC as an IP / PSTN Gateway

The procedure below describes how to configure the E-SBC as an IP / PSTN Gateway.

➢ **To configure the E-SBC as an IP/PSTN Gateway and Associate it with the Mediation Server:**

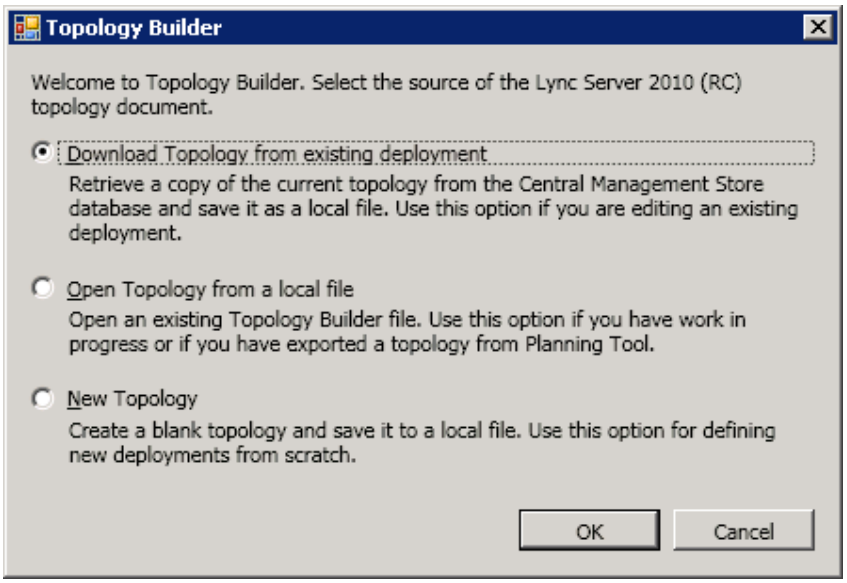
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**).

Figure 3-1: Starting the Lync Server Topology Builder



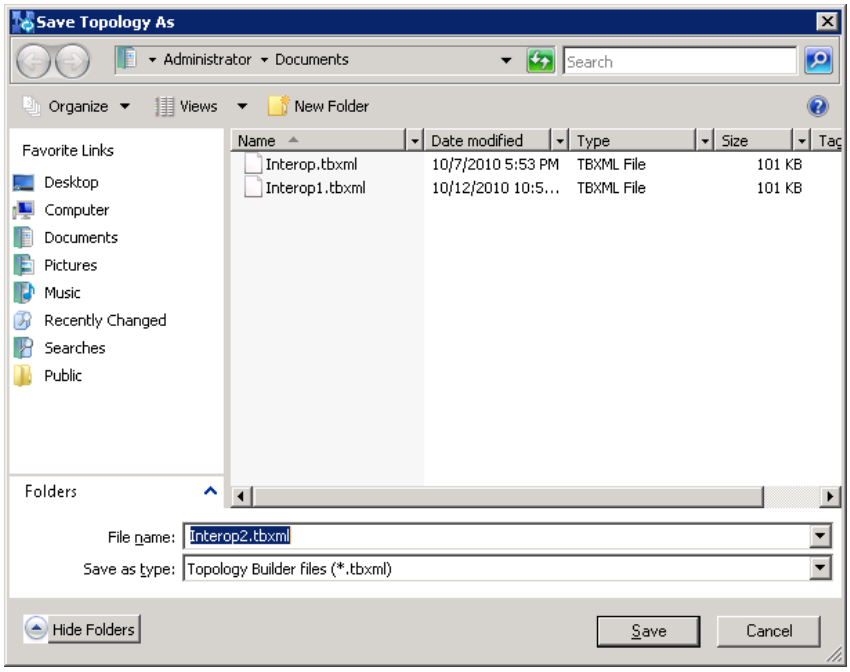
The following screen is displayed:

Figure 3-2: Topology Builder Options



2. Select the **Download Topology from existing deployment** option, and then click **OK**; you are prompted to save the downloaded Topology:

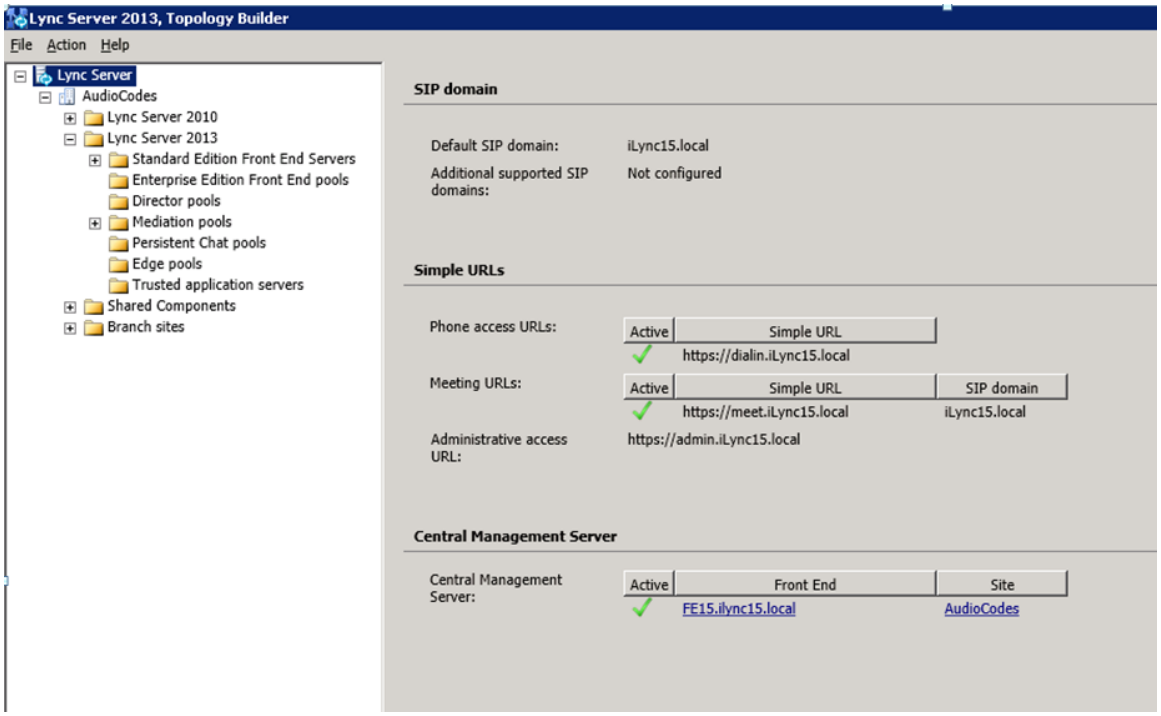
Figure 3-3: Saving the Topology



3. Enter a name for the Topology file, and then click **Save**. This step enables you to roll back from any changes you make during the installation.

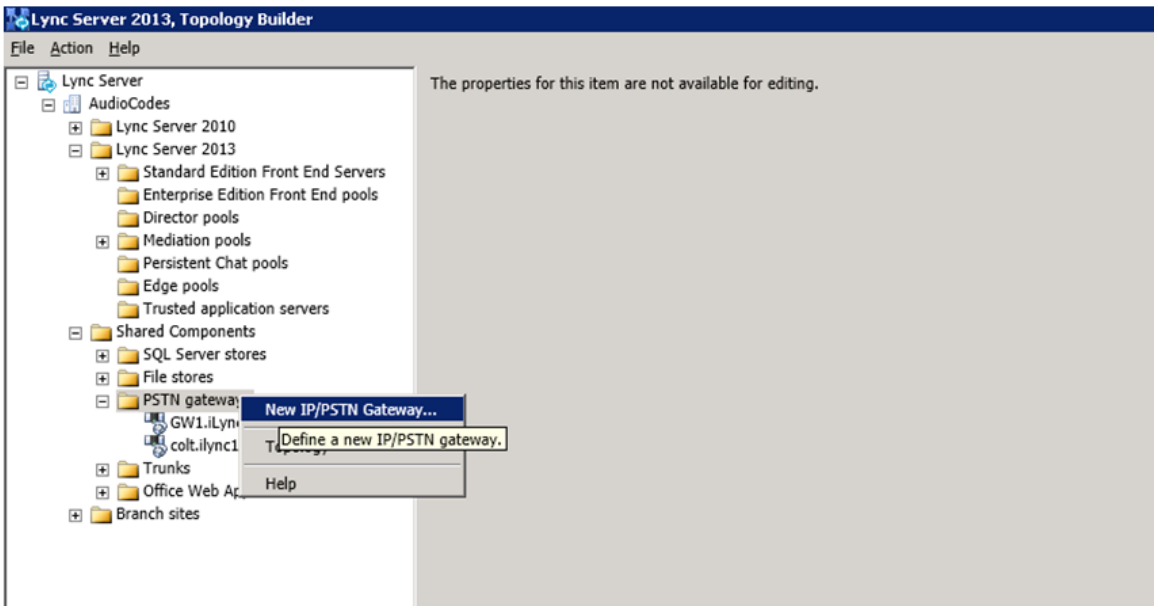
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Displaying Downloaded Topology



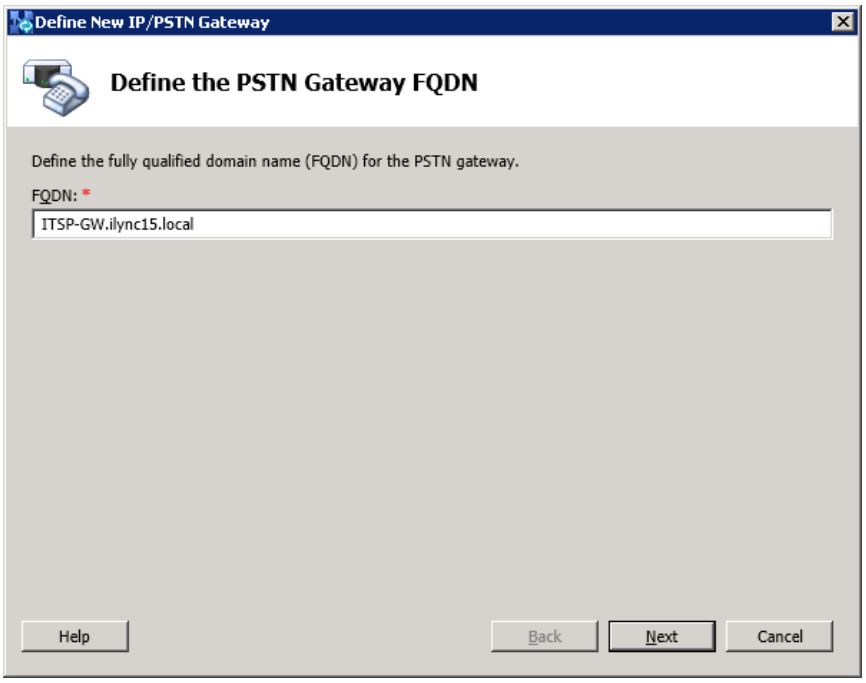
4. Under **Lync Server 2013** > *your site name* > **Shared Components**, right-click the **PSTN Gateways** node, and then click **New PSTN Gateway**.
5. Right-click the **PSTN gateways** folder, and then choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



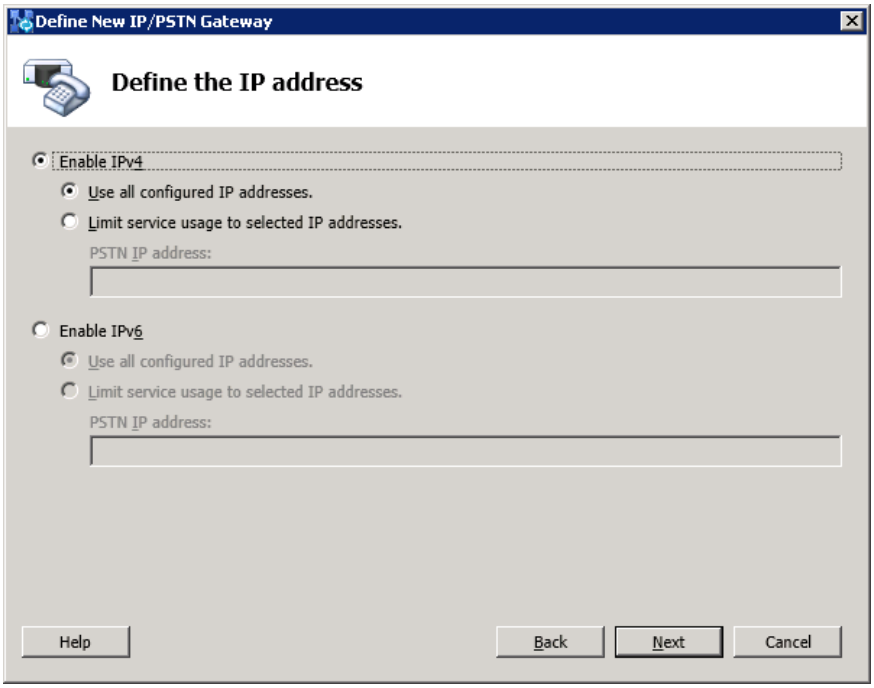
The following screen appears:

Figure 3-6: Defining the New IP/PSTN Gateway



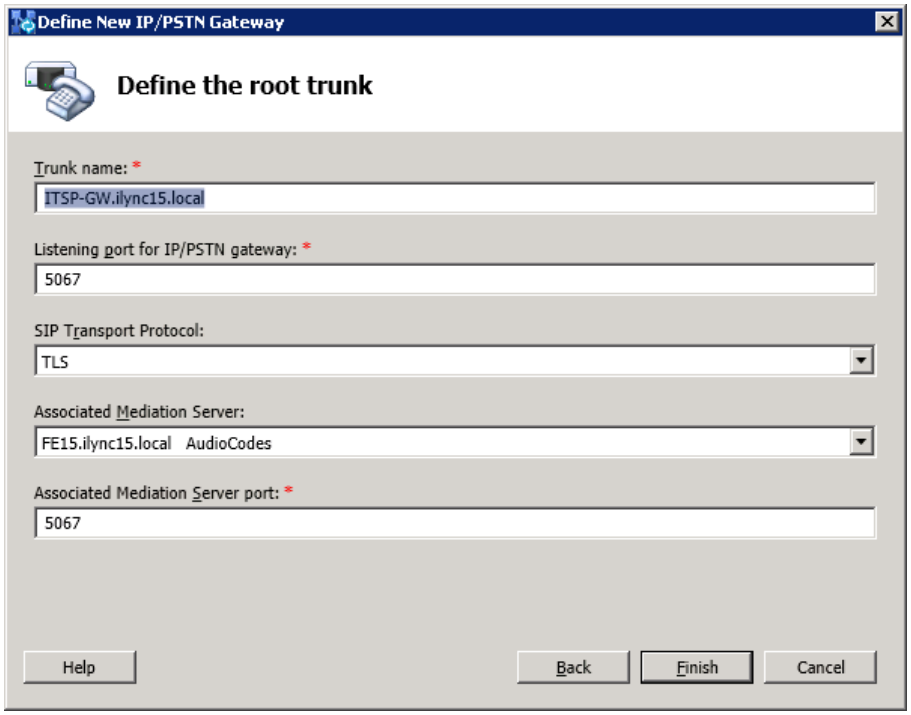
6. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., "ITSP-GW.ilync15.local"); this FQDN should be updated in the relevant DNS record, and then click **Next.**
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

Figure 3-7: Defining the IP Address



8. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between a Mediation Server and a gateway uniquely identified by the combination *{Mediation Server FQDN, Mediation Server listening port (TLS or TCP) : gateway IP and FQDN, gateway listening port}*.
   - When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
   - The root trunk cannot be removed until the associated PSTN gateway is removed.

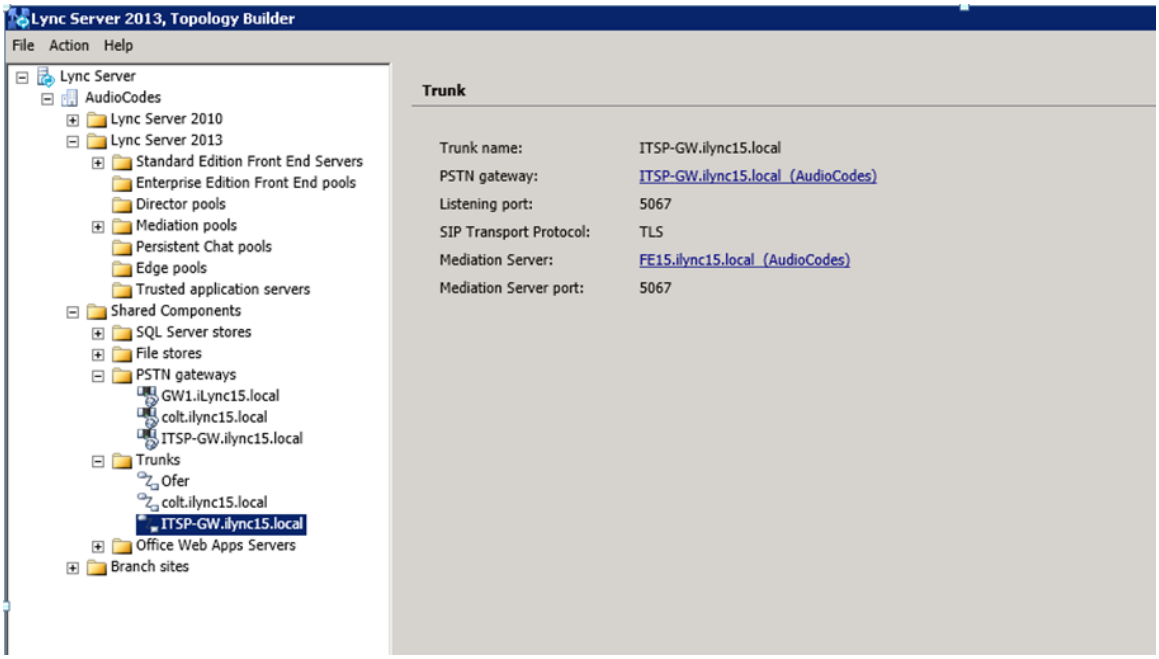
Figure 3-8: Defining the Root Trunk



a. In the 'Listening Port for IP/PSTN Gateway' field, enter "5067". This is the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway
b. From the 'SIP Transport Protocol' drop-down list, select the Transport Type that the trunk uses (i.e., **TLS**).
c. From the Associated Mediation Server drop-down list, select the Mediation Server pool to associate with the root trunk of this PSTN Gateway.
d. In the 'Associated Mediation Server port' field, enter "5067", which is the listening port that the Mediation Server uses for SIP messages from the SBC.
e. Click **Finish**.

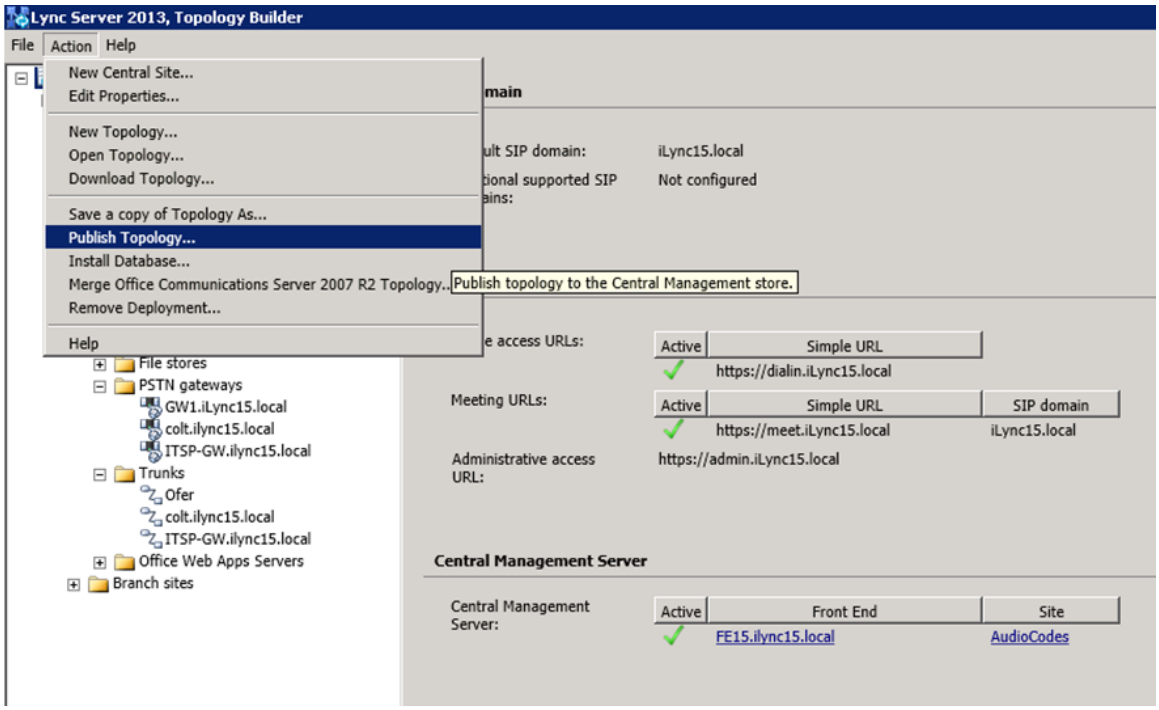
The SBC is added as a PSTN Gateway and a trunk was created as shown below:

Figure 3-9: Adding E-SBC as an IP/PSTN Gateway and Creating a Trunk



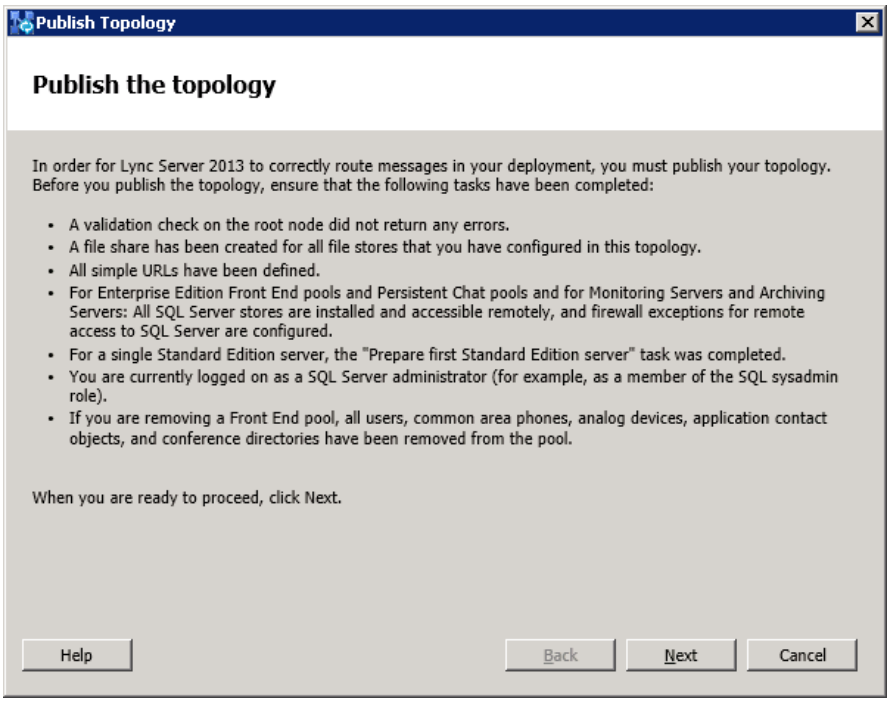
9. Publish the Topology by selecting the root item **Lync Server**, and then from the **Action** menu on the menu bar, choose **Publish Topology**, as shown below:

Figure 3-10: Selecting Publish Topology from the Action Menu



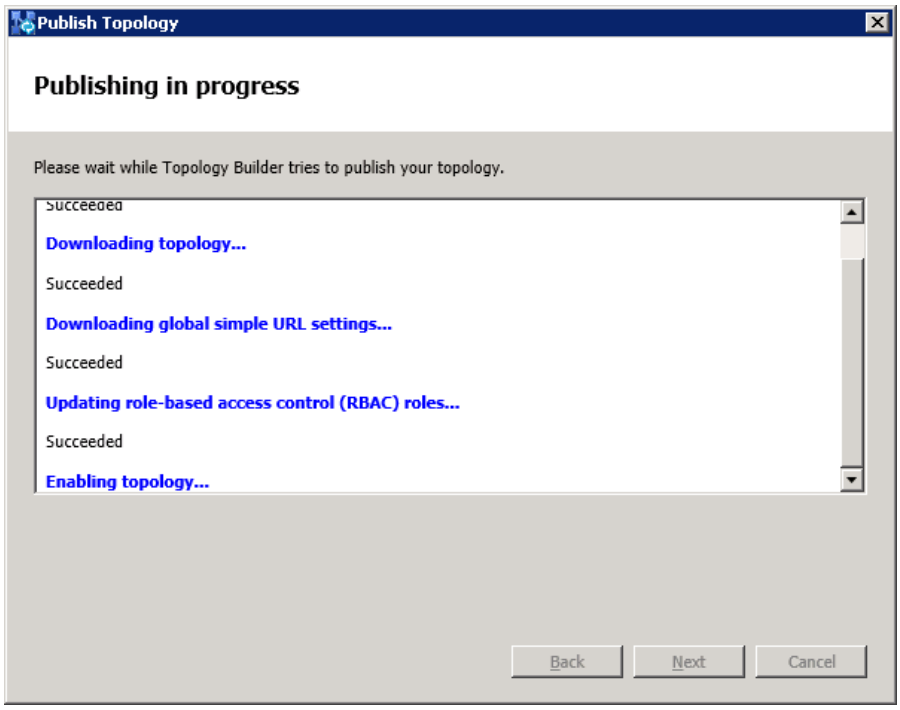
The Publish Topology screen is displayed:

Figure 3-11: Publishing Topology



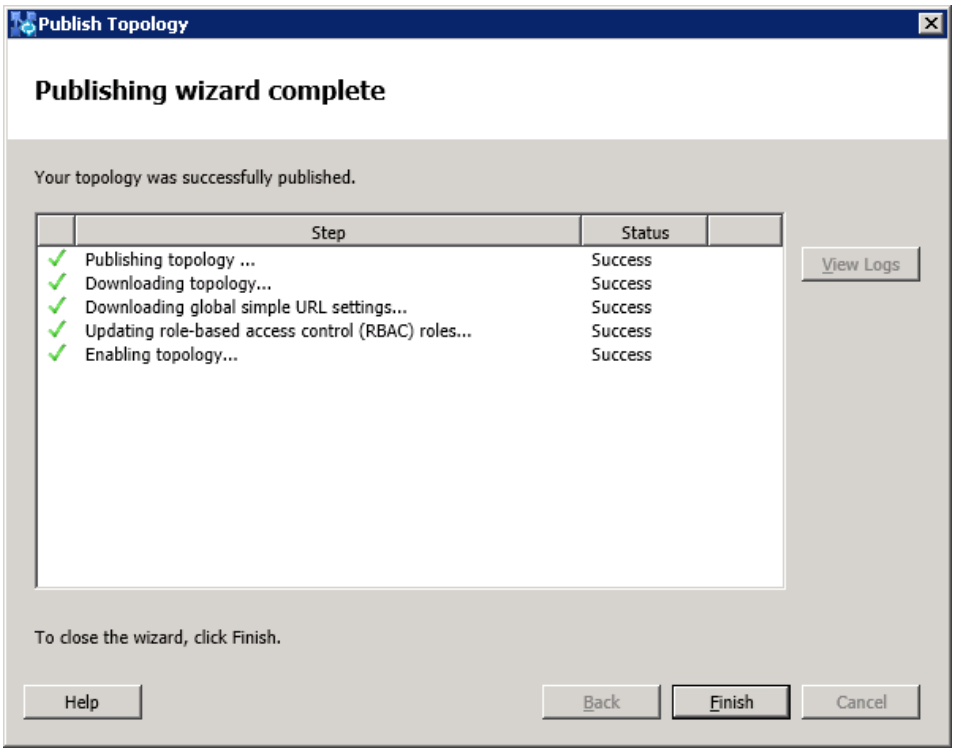
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing the Topology in Progress



11. Wait until the publishing topology process completes successfully, as shown below:

Figure 3-13: Publishing Topology Successfully Completed



12. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

The procedure below describes how to configure a "Route" on the Lync Server 2013 and how to associate it with the E-SBC PSTN gateway.

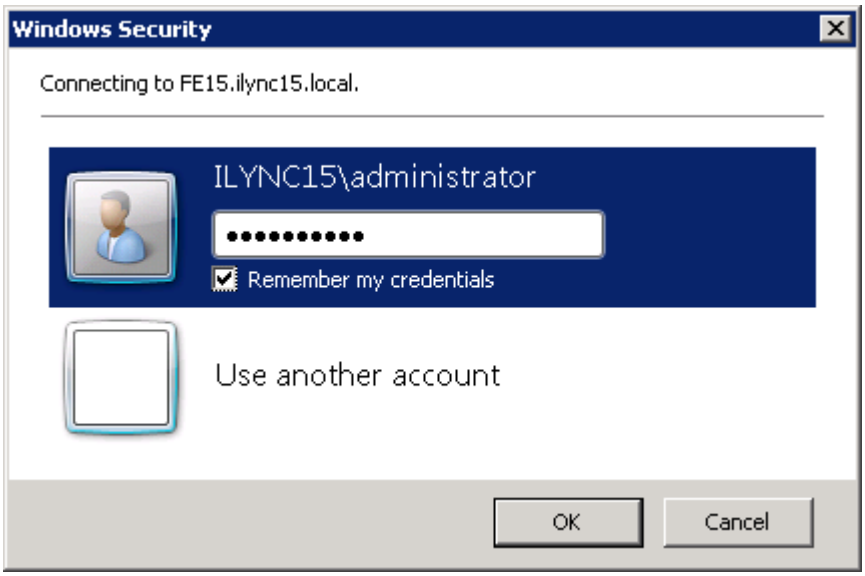
➢ **To configure the "route" on Lync Server 2013:**

1. Start the Microsoft Lync Server 2013 Control Panel (**Start** > **All Programs** > **Microsoft Lync Server 2013** > **Lync Server Control Panel**) as shown below:

Figure 3-14: Opening the Lync Server Control Panel

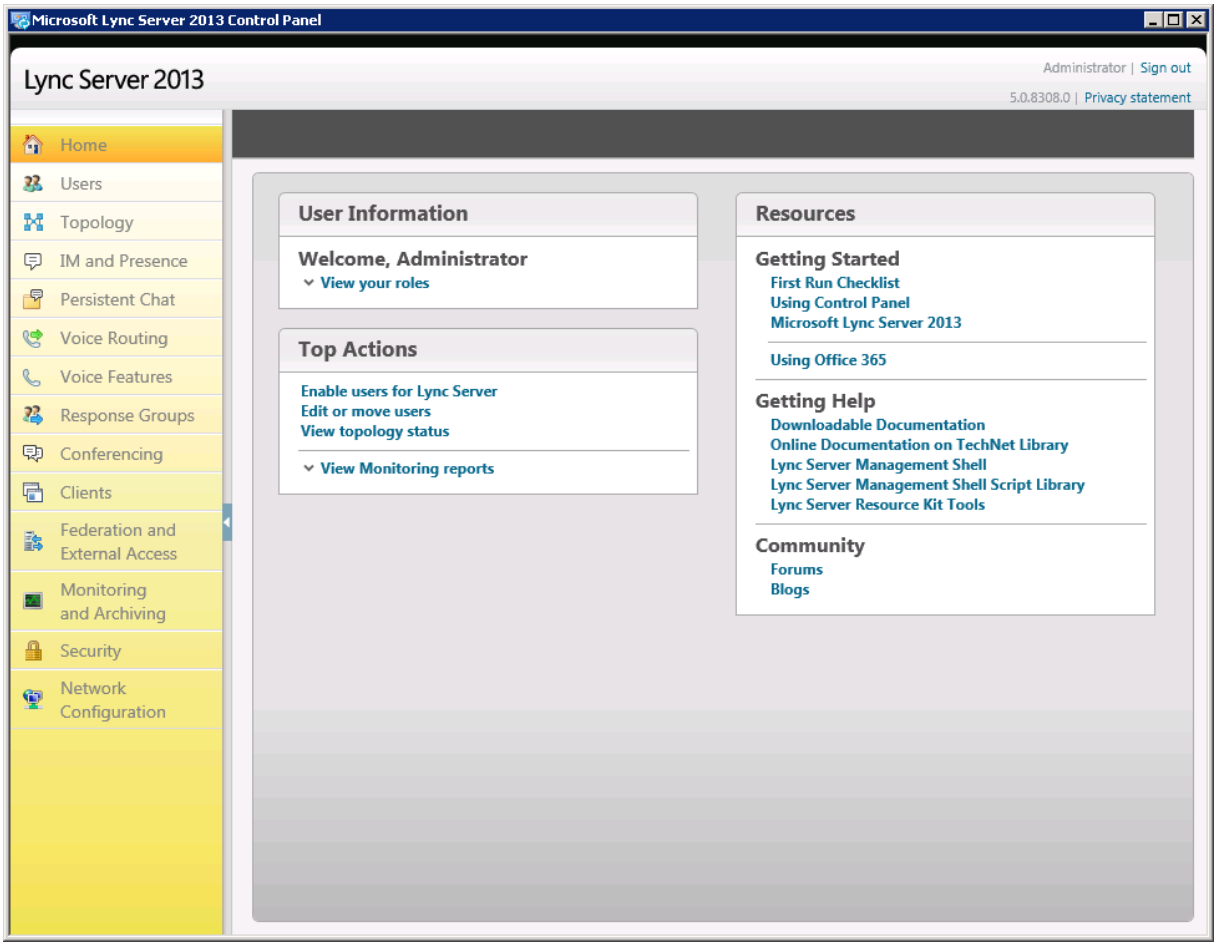
2. You are prompted to enter your login credentials:

Figure 3-15: Entering Lync Server Credentials



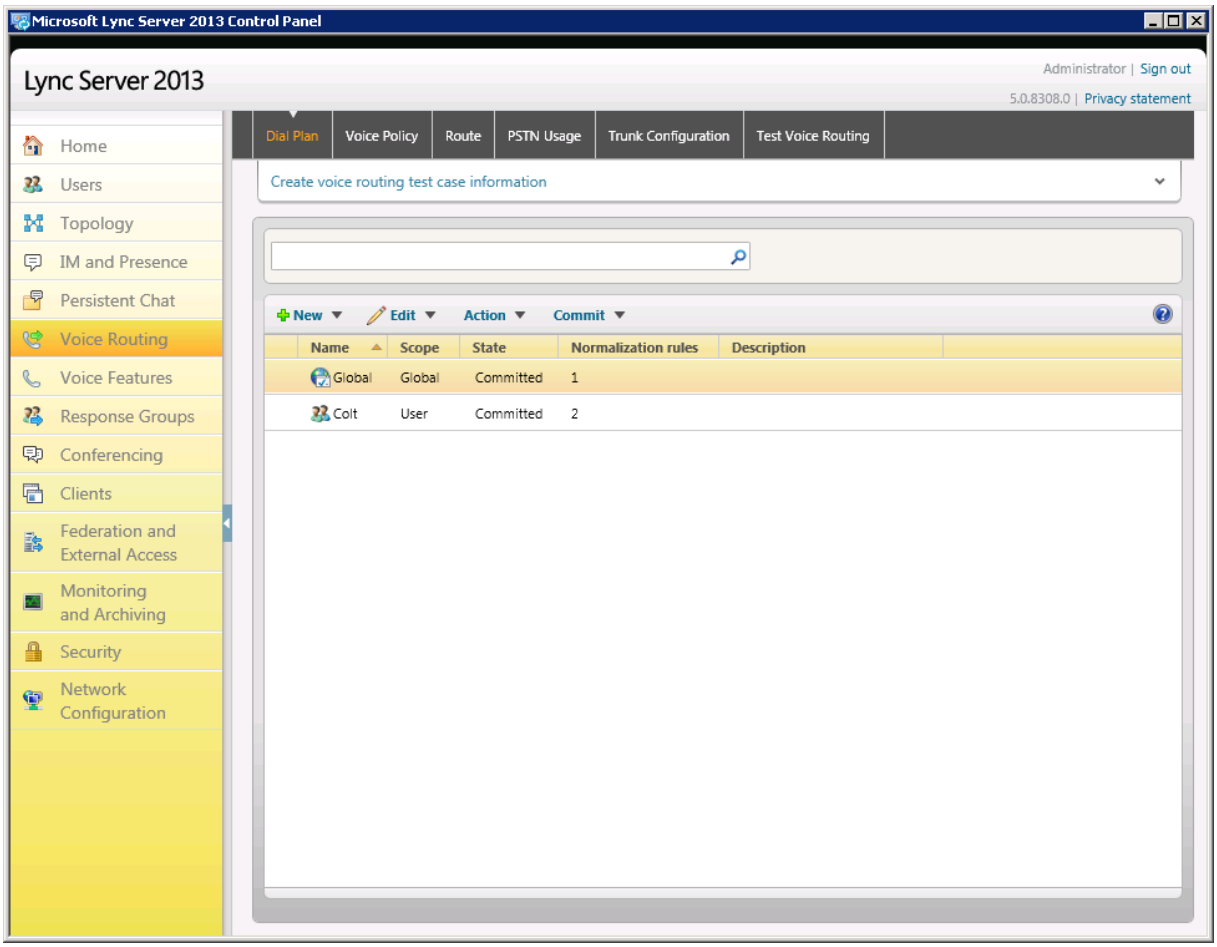
3. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel appears:

Figure 3-16: Displaying Microsoft Lync Server 2013 Control Panel



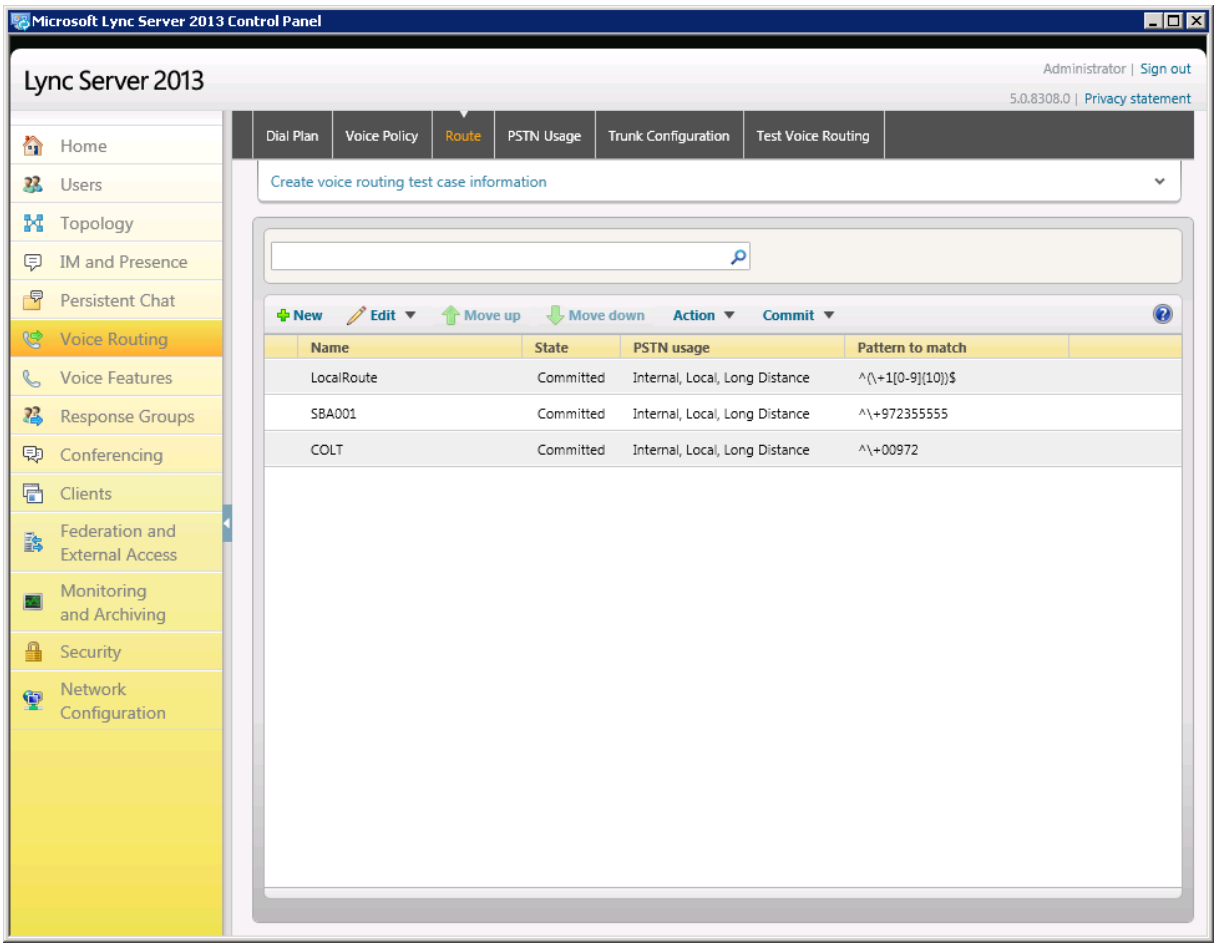
4. In the left navigation pane, select **Voice Routing**; the following screen appears:

Figure 3-17: Selecting Voice Routing



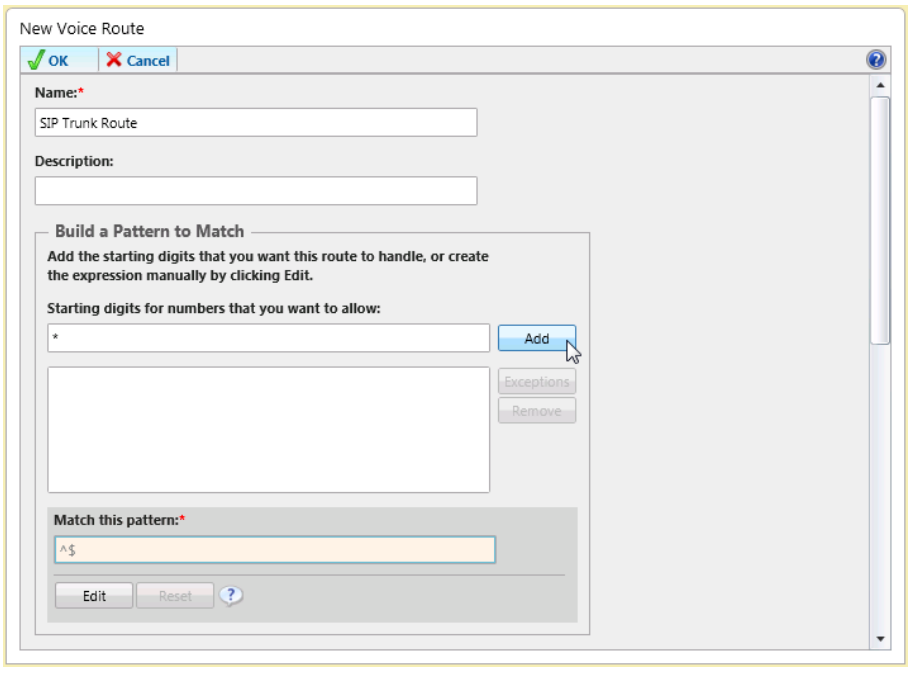
5. In the Voice Routing page, click the **Route** tab.

Figure 3-18: Selecting the Route Option



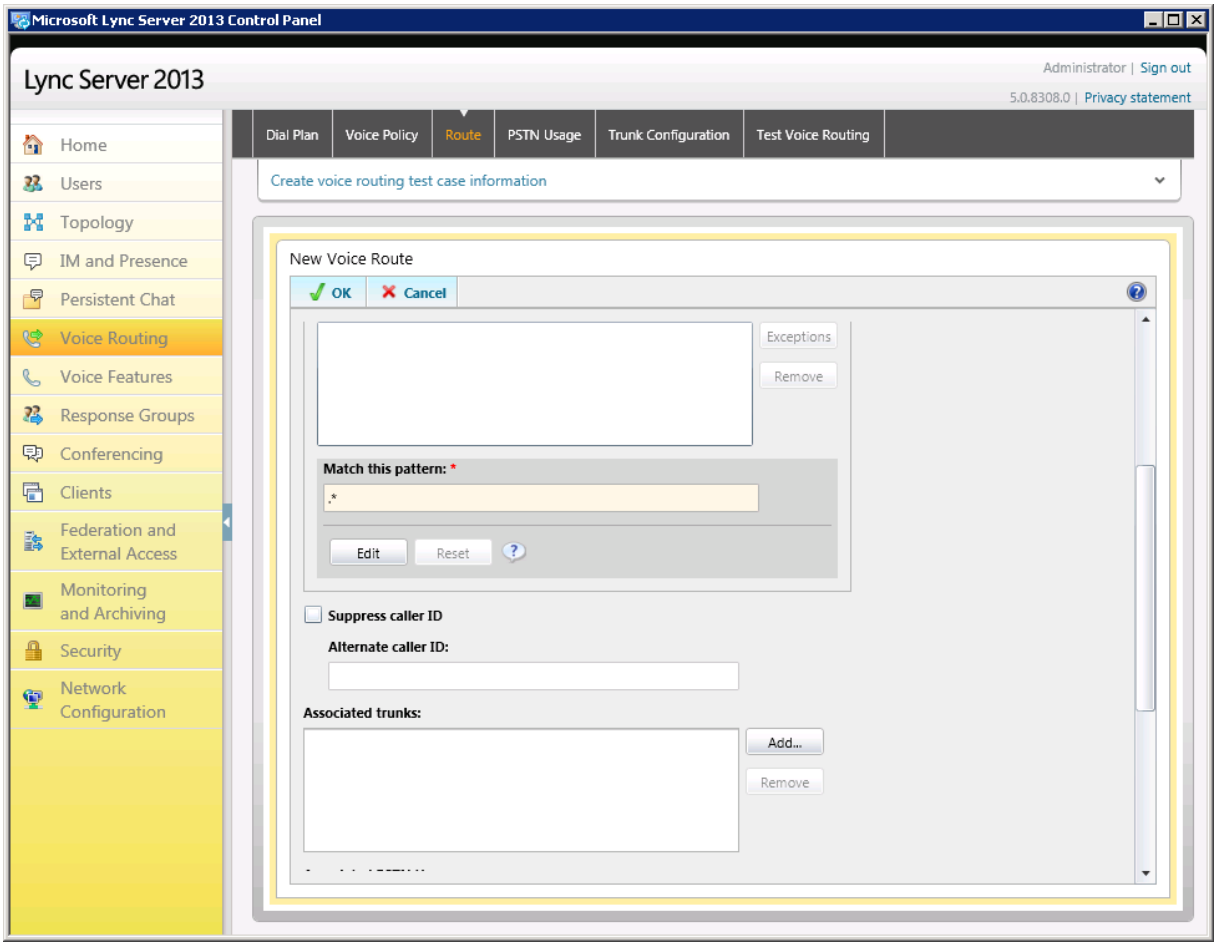
6. Click **New**; the New Voice Route dialog box appears:

Figure 3-19: Adding a New Voice Route



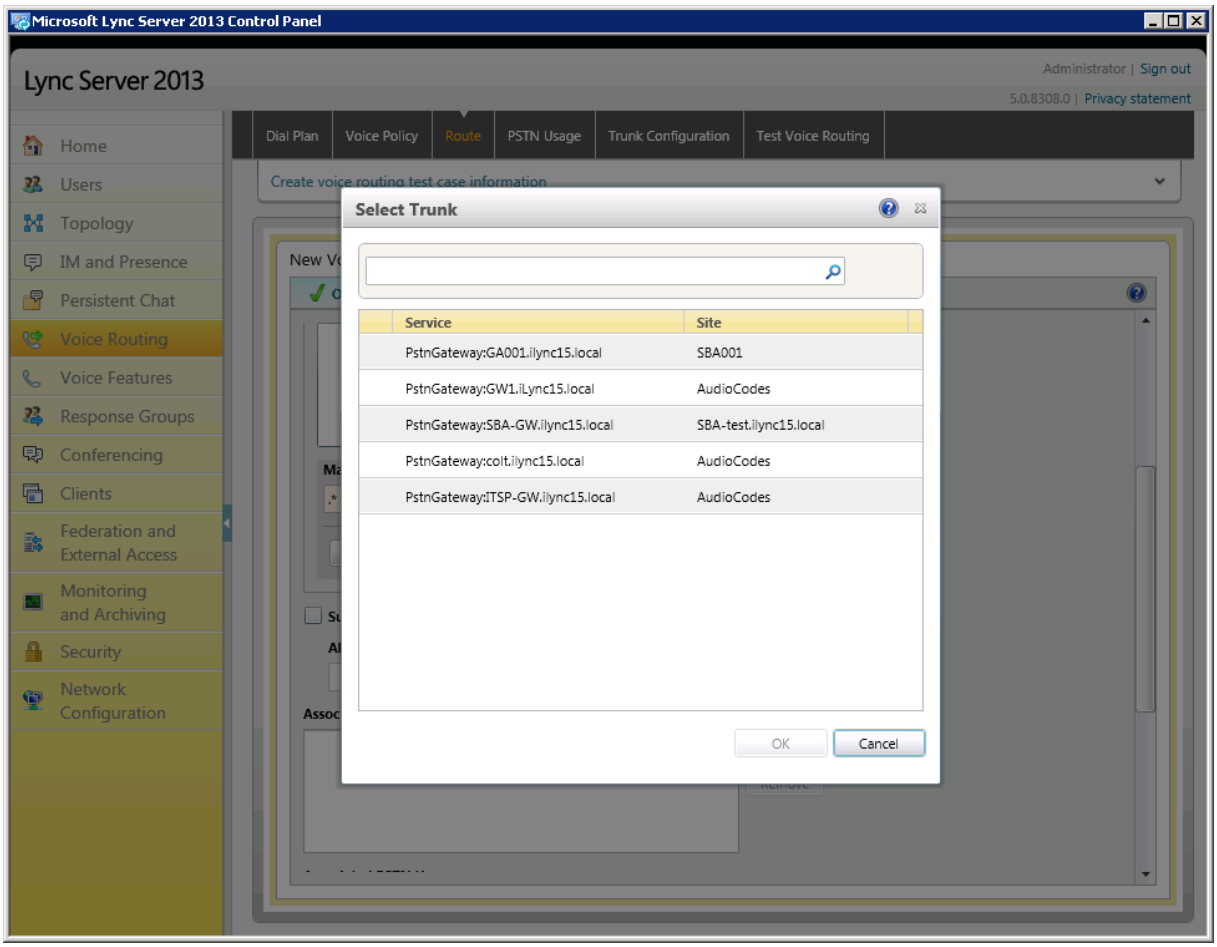
7. In the 'Name' field, enter a name for this route (e.g., "SIP Trunk Route").
8. In the 'Build a Pattern to Match' field, enter the starting digits you want this route to handle (e.g., "*", which means to match all numbers).
9. Click **Add**.

Figure 3-20: Adding a New Trunk



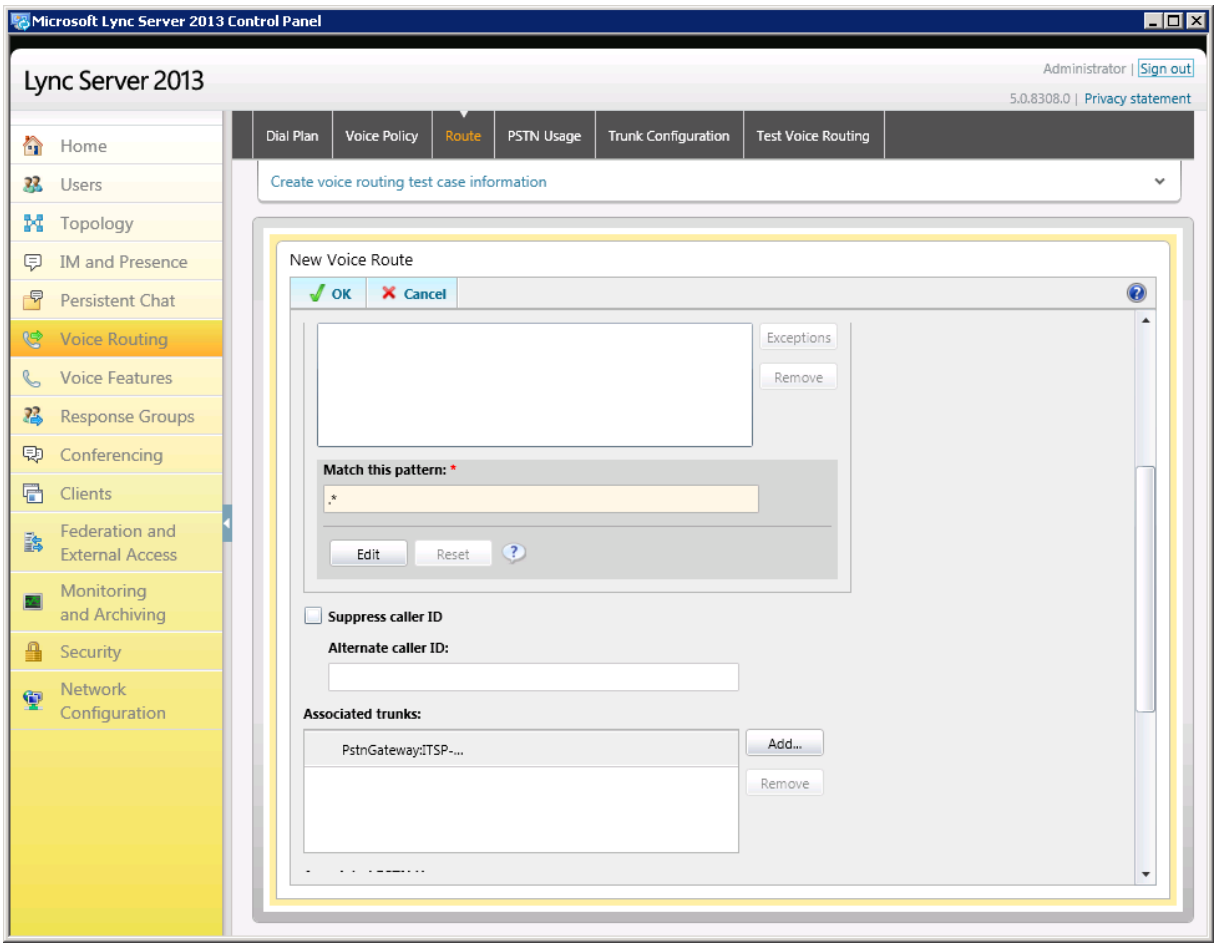
10. Associate the route with the E-SBC Trunk that you created:
    a. In the Associated Trunks pane, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: Displaying Deployed Trunks



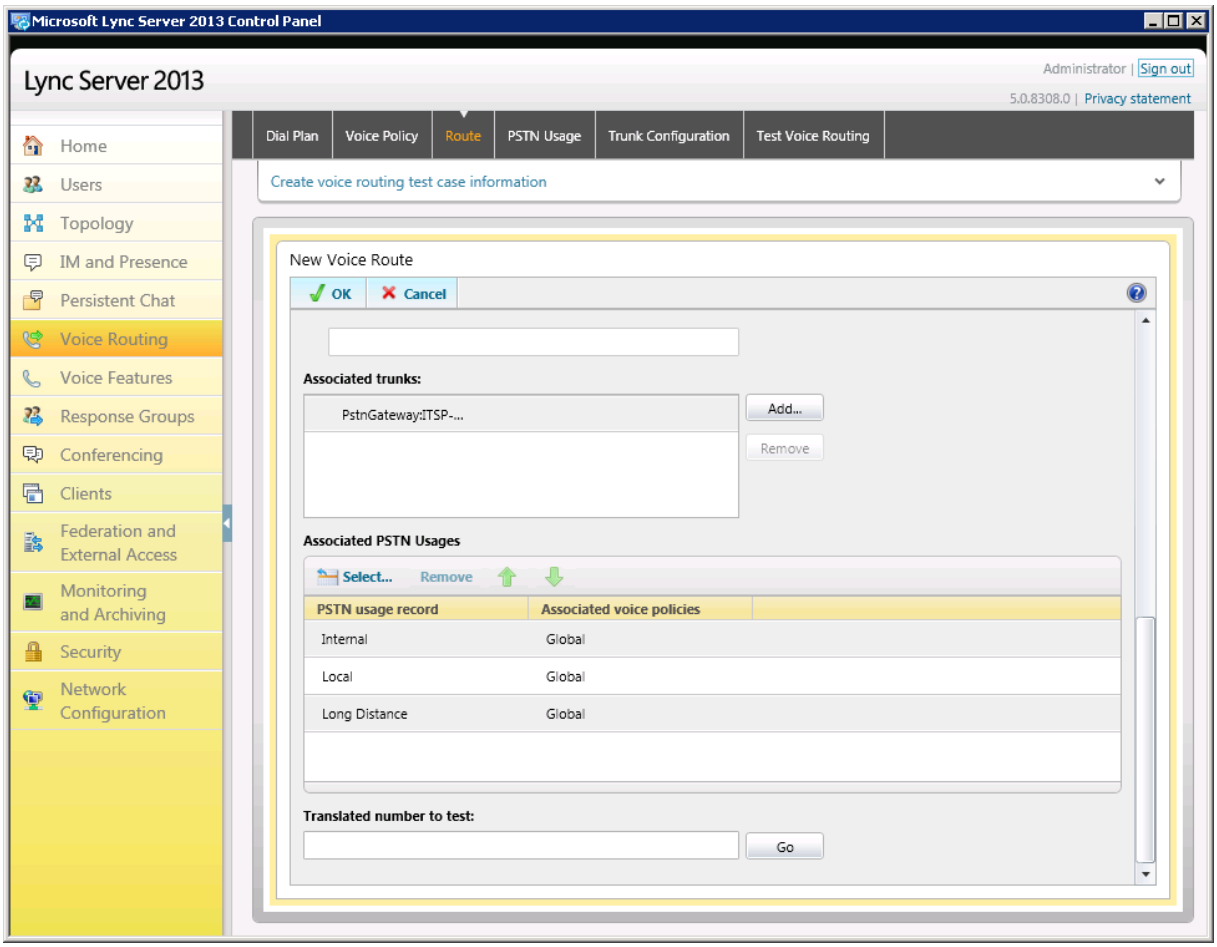
b. Select the E-SBC Trunk you created, and then click **OK**.

Figure 3-22: Selecting E-SBC Trunk



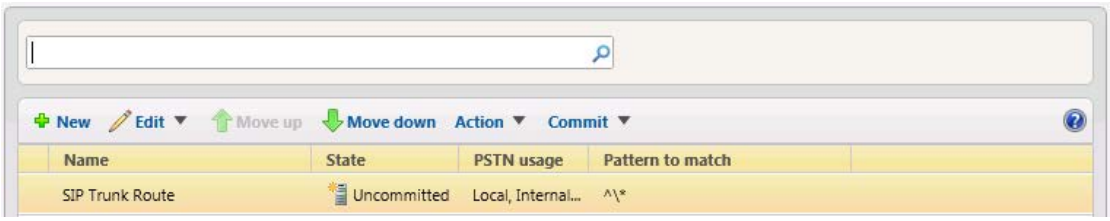
11. Associate a PSTN Usage to this route:
    a. In the Associated PSTN Usages group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



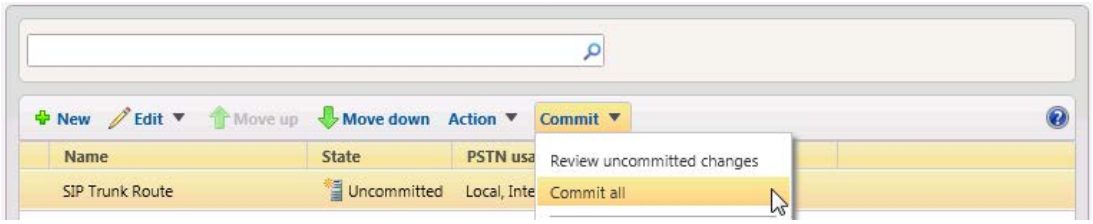
12. Click **OK** (located on the top of the New Voice Route dialog box); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirming New Voice Route



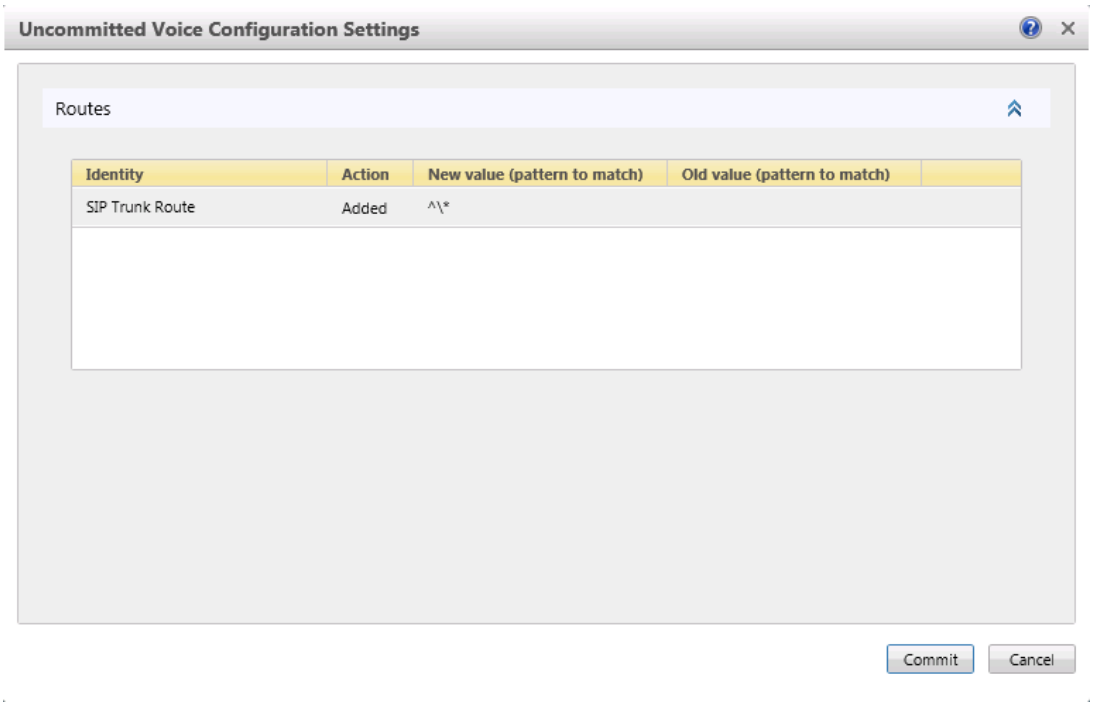
13. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



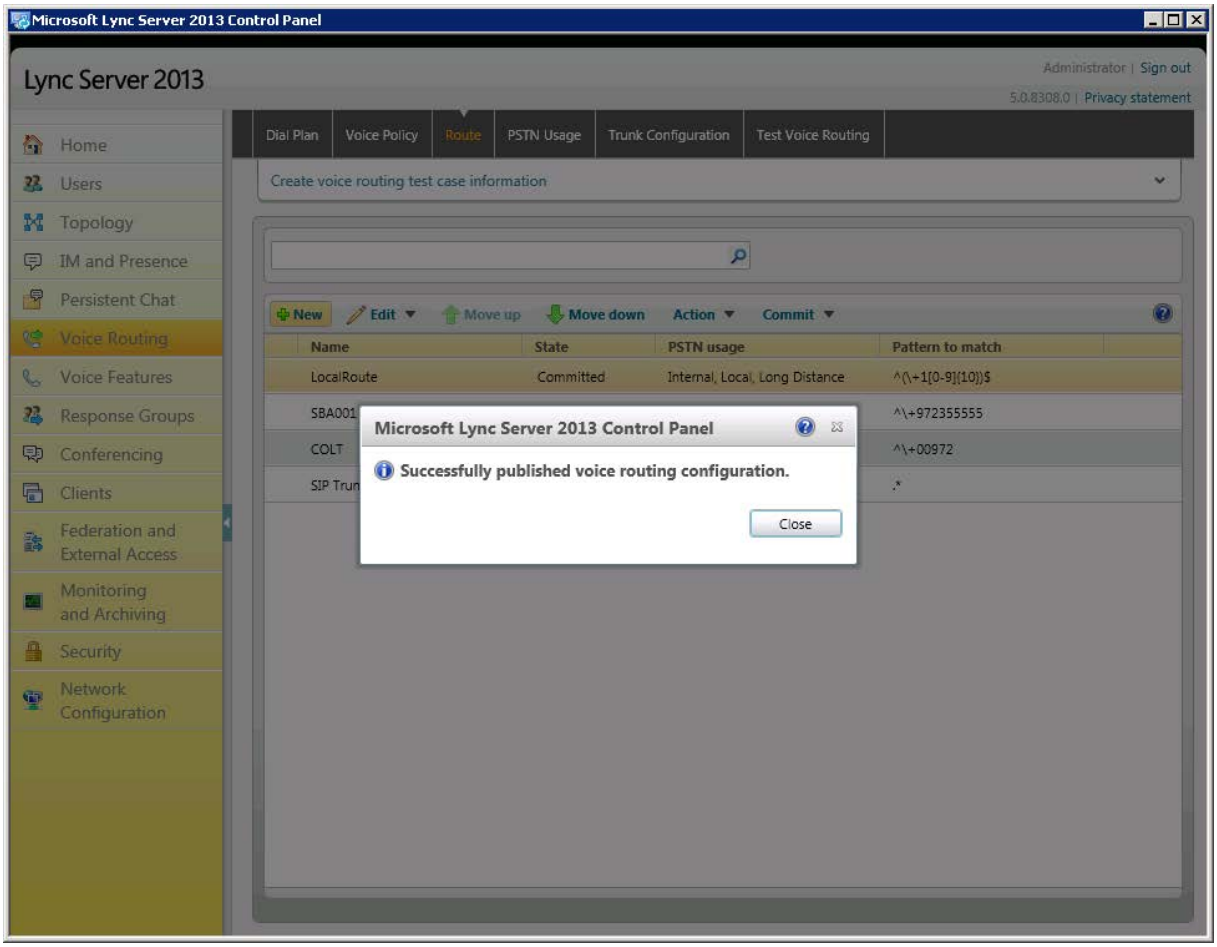
The Uncommitted Voice Configuration Settings dialog box appears:

Figure 3-26: Un-committing Voice Configuration Settings



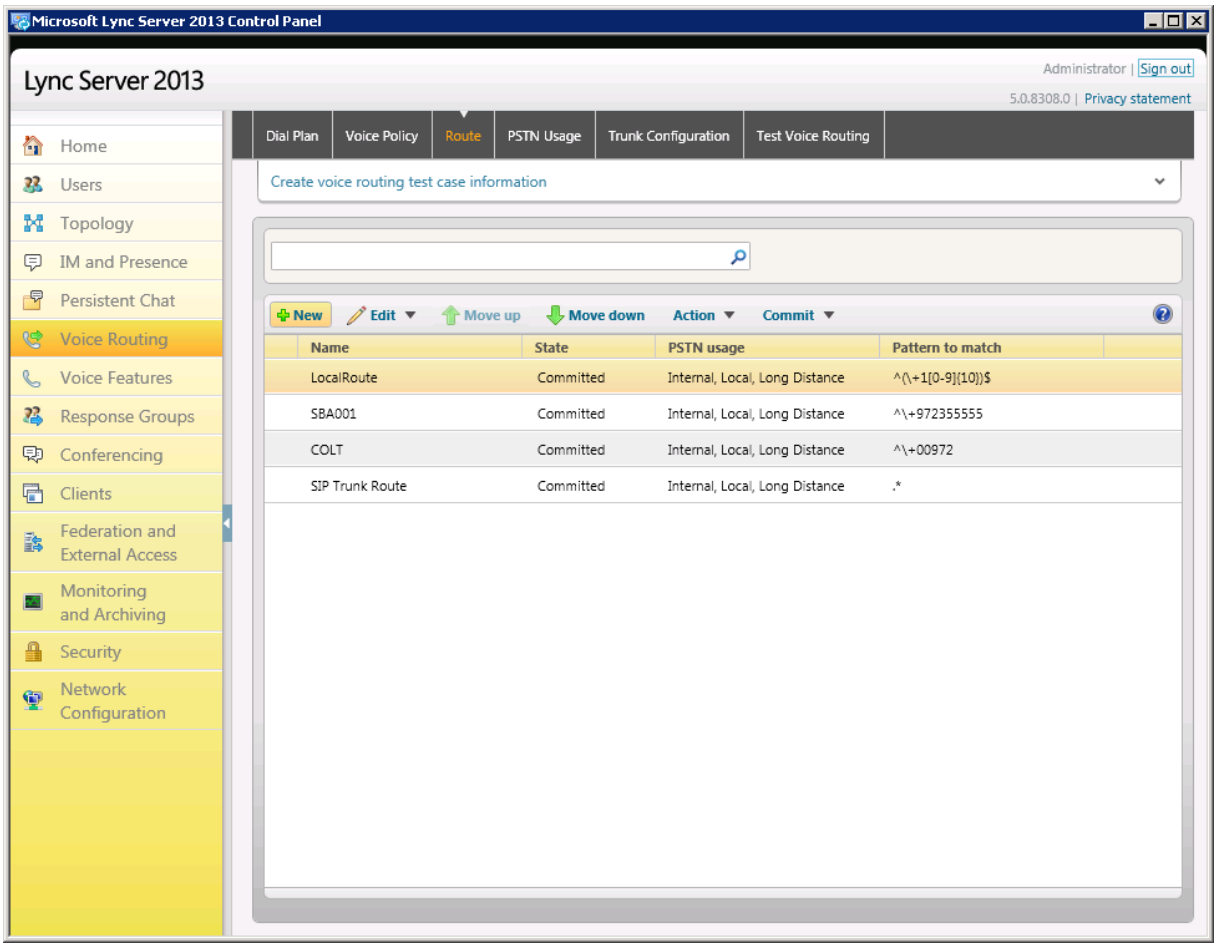
14. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirming Successful Voice Routing Configuration



15. Click **Close**; the new committed Route is displayed in the Voice Routing screen, as shown below:

Figure 3-28: Displaying Voice Routing Committed Routes



Reader's Notes

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and AT&T IP Flexible Reach - EF service:

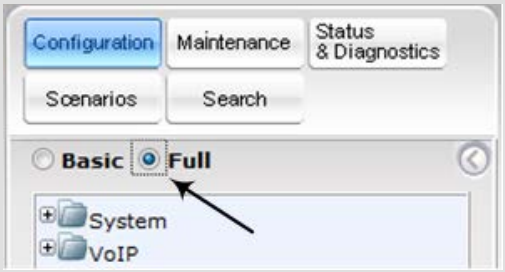
- **E-SBC WAN interface:** AT&T IP Flexible Reach - EF service environment
- **E-SBC LAN interface:** Lync Server 2013 environment

This configuration is done using the E-SBC's Web-based management tool (embedded Web server).

Notes:

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

  For more information about the Software Upgrade Feature Key, please contact your AudioCodes sales representative.
- The scope of this document does **not** cover security aspects for connecting the SIP Trunk to the Microsoft Lync environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, refer to the *Recommended Security Guidelines Technical Note* 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 displayed below:



  When the E-SBC is reset, the Web GUI reverts to Basic-menu display.
- The AudioCodes E-SBC configuration is backward compatible with Microsoft Lync Server 2010.

4.1 Step 1: Network Interface Configuration

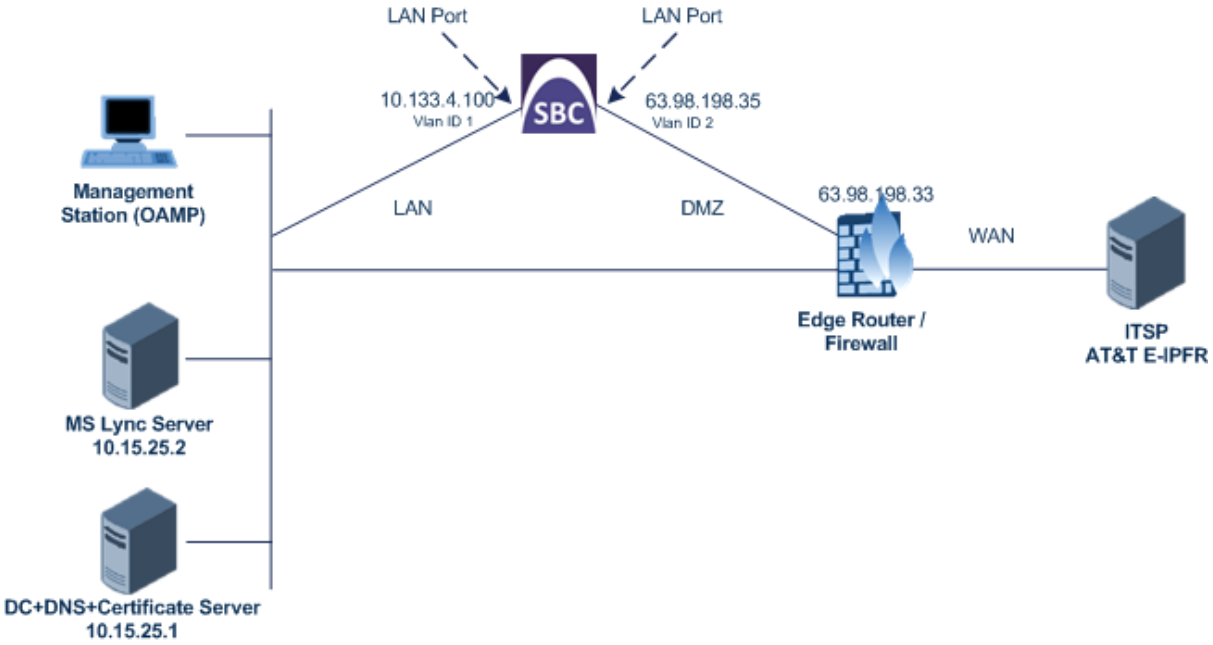
This step describes how to configure the E-SBC's network interfaces. There are several ways to deploy the E-SBC. However, the example scenario in this document uses the following deployment method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the AT&T IP Flexible Reach - EF service located on the WAN.
- The E-SBC connects to the WAN through a DMZ network.

The type of physical LAN connection depends on the method used to connect to the Enterprise's network. In this example, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and network cables).

In addition, the E-SBC uses two logical network interfaces; one to the LAN (VLAN ID 1) and one to the WAN (VLAN ID 2).

Figure 4-1: Configuring Network Interfaces



4.1.1 Step 1a: Configure IP Network Interfaces

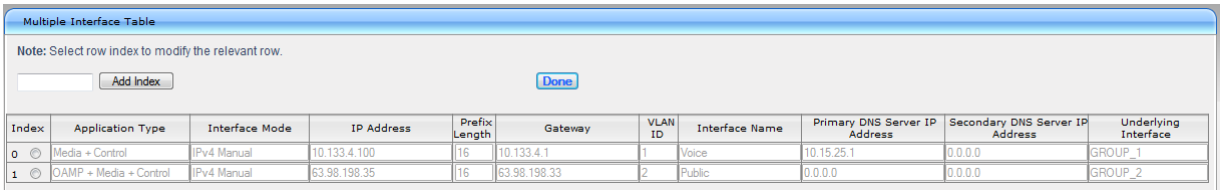
The procedure below describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP ("Voice")
- WAN VoIP ("Public")

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

1. Open the Multiple Interface Table page (**Configuration** tab > **Network Settings** > **IP Settings**).

Figure 4-2: Configuring IP Network Interfaces



2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button corresponding to the Application Type, "OAMP + Media + Control", and then click **Edit**.
   b. Set the interface as follows:

Parameter	Settings
Application Type	**Media + Control**
IP Address	**10.133.4.100** This is the E-SBC IP address.
Prefix Length	**16** This is the subnet mask in bits for 255.255.0.0.
Gateway	**10.133.4.1**
VLAN ID	**1**
Interface Name	**Voice** This is an arbitrary descriptive name.
Primary DNS Server IP Address	**10.15.25.1**
Underlying Interface	**GROUP_1** This is the Ethernet port group.

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

Parameter	Settings
Application Type	**OAMP + Media + Control**
IP Address	**63.98.198.35** This is the WAN IP address.
Prefix Length	**16** This is the subnet mask in bits for 255.255.0.0.

Parameter	Settings
Gateway	**63.98.198.33** This is the default gateway - router's IP address.
VLAN ID	**2**
Interface Name	**Public** This is the arbitrary descriptive name of WAN interface.
Underlying Interface	**GROUP_2** This is the Ethernet port group.

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

OAMP can be assigned to only one of the interfaces. You may place it on either interface depending on how you wish to control the device depending on the deployment.

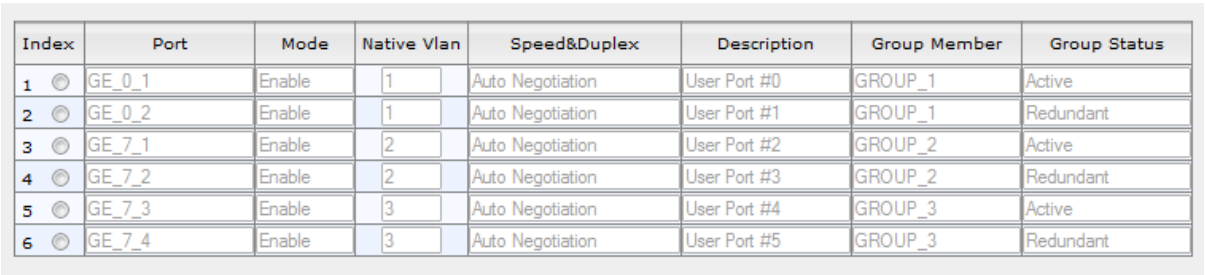
4.1.2 Step 1b: Configure the Native VLAN ID

The procedure below describes how to configure the Native VLAN ID for the two network interfaces (LAN and WAN).

➢ **To configure the Native VLAN ID:**

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

Figure 4-3: Configuring Native VLAN ID



Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_0_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
2	GE_0_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
3	GE_7_1	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
4	GE_7_2	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant
5	GE_7_3	Enable	3	Auto Negotiation	User Port #4	GROUP_3	Active
6	GE_7_4	Enable	3	Auto Negotiation	User Port #5	GROUP_3	Redundant

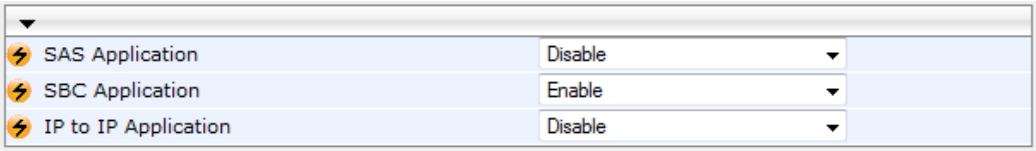
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Reset the E-SBC with a **burn to flash** for this setting to take effect (see Section 4.15 on page 103).

4.3 Step 3: Signaling Routing Domains

This step describes how to configure Signaling Routing Domains (SRD). An SRD is a set of definitions comprising IP interfaces, E-SBC resources, SIP behaviors, and Media Realms.

4.3.1 Step 3a: Configure RTP/RTCP Base Level Media settings

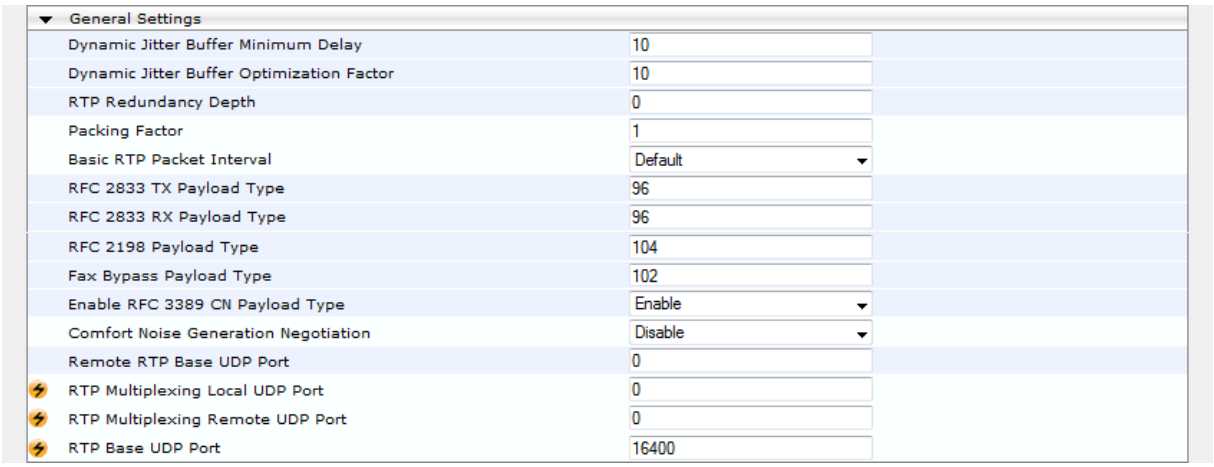
AT&T requires that the RTP/RTCP be passed within the range of 16384 - 32767 for proper network management and COS within the AT&T network. To set the ports, associated with an IP interface, which are used by the E-SBC to transmit or receive media (RTP or SRTP). This must be performed prior to setting the Media Realms are associated with SRDs or IP Groups. Prior to setting these other parameters, the base level Media Settings must first be set and the unit must be reset for the functionality to take effect.

This is described in the procedure below for our example scenario.

➢ **To configure RTP/RTCP base port settings:**

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** > **Media** > **RTP/RTCP Settings**).
2. Set **RTP base UDP port** to 16400:
   a. Click **Submit**.
   b. Click **Burn.**
   c. Reset the device.

Figure 4-5: Configuring RTP/RTCP Base Port Settings



4.3.2 Step 3b: Configure Media Realms

A Media Realm represents a set of ports, associated with an IP interface, which are used by the E-SBC to transmit or receive media (RTP or SRTP). Media Realms are associated with SRDs or IP Groups.

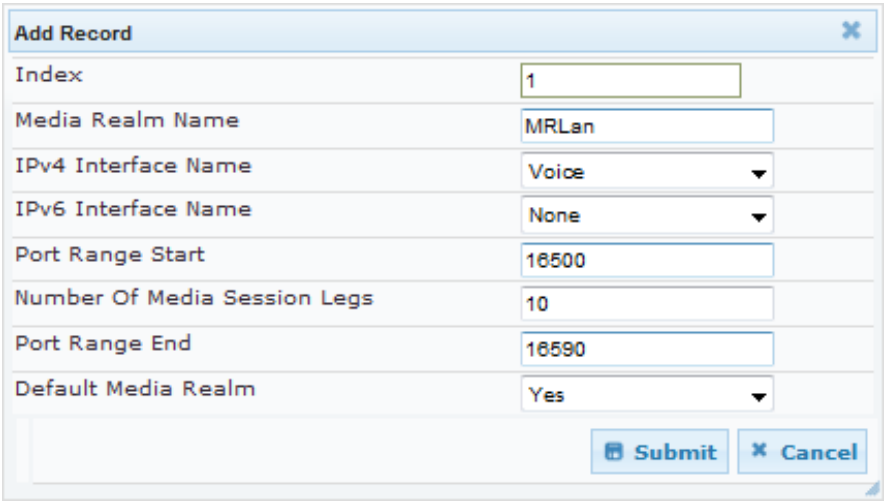
The simplest configuration is to create one Media Realm for internal (LAN) traffic and another for external (WAN) traffic, which is described in the procedure below for our example scenario.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** > **Media** > **Media Realm Configuration**).
2. Add a Media Realm for the LAN traffic:
   a. Click **Add**.
   b. Configure the Media Realm as follows:

Parameter	Settings
Index	**1**
Media Realm Name	**MRLan** This is an arbitrary name.
IPv4 Interface Name	**Voice**
Port Range Start	**16500** This represents the lowest UDP port number that will be used for media on the LAN
Number of Media Session Legs	**10** This is the number of media sessions that are assigned with the port range.

Figure 4-6: Configuring LAN Media Realm

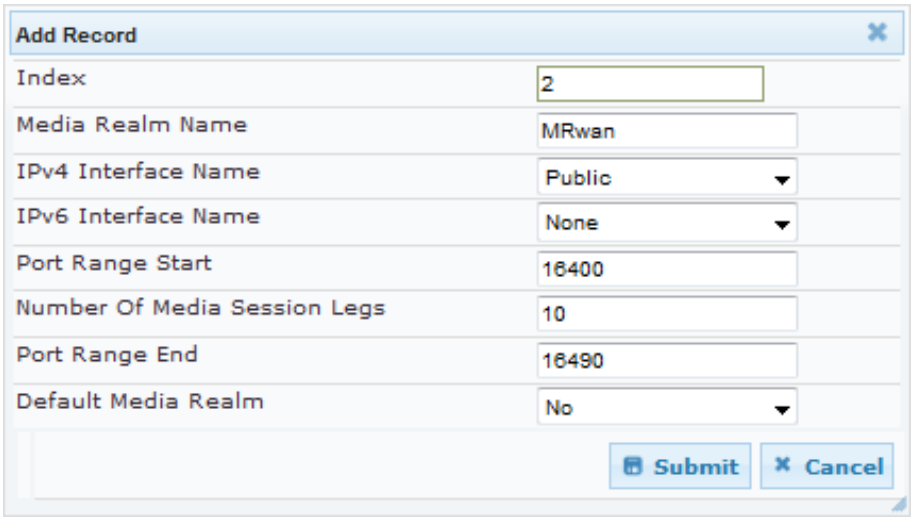


   c. Click **Submit**.

3. Add a Media Realm for the external traffic (WAN):
   a. Click **Add**.
   b. Configure the Media Realm as follows:

Parameter	Settings
Index	**2**
Media Realm Name	**MRwan** This is an arbitrary name.
IPv4 Interface Name	**Public**
Port Range Start	**16400** This is the number that represents the lowest UDP port number that will be used for media on the WAN.
Number of Media Session Legs	**10** This is the number of media sessions that are assigned with the port range.

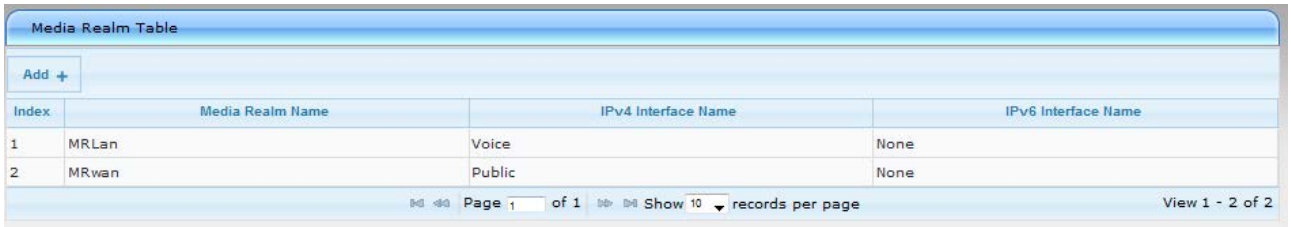
Figure 4-7: Configuring WAN Media Realm



   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-8: Displaying Configured Media Realm



4.3.3 Step 3c: Configure SRDs

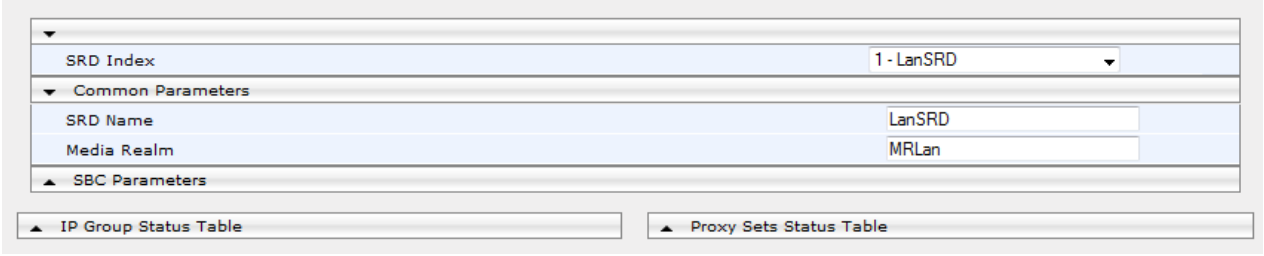
The procedure below describes how to configure the SRDs.

➢ **To configure SRDs:**

1. Open the SRD Table page (**Configuration** tab > **VoIP** > **Control Network** > **SRD Table**).
2. Add an SRD for the E-SBC's internal interface (toward Lync Server 2013):
   a. Configure the following parameters:

Parameter	Settings
SRD Index	**1-LanSRD**
SRD Name	**LanSRD**
Media Realm	**MRLan** This associates the SRD with a Media Realm**.**

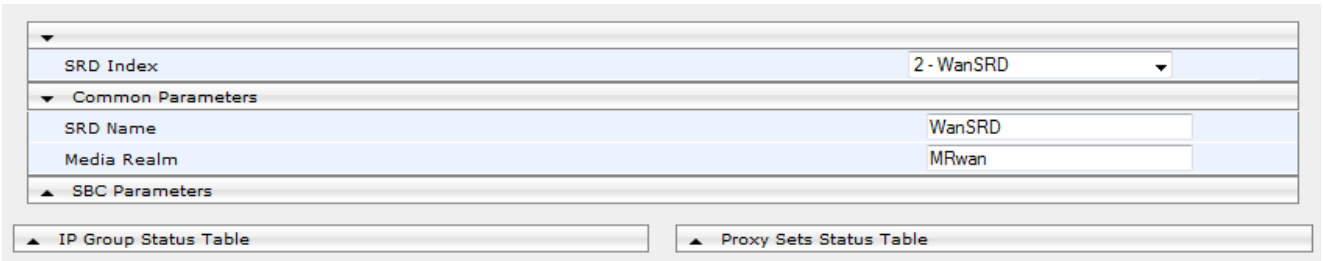
Figure 4-9: Configuring LAN SRDs



   b. Click **Submit**.
3. Add an SRD for the E-SBC's external interface (toward the AT&T IP Flexible Reach - EF service):
   a. Configure the following parameters:

Parameter	Settings
SRD Index	**2-WanSRD**
SRD Name	**WanSRD**
Media Realm	**MRwan** This associates the SRD with a Media Realm.

Figure 4-10: Configuring WAN SRDs



   b. Click **Submit**.

4.3.4 Step 3d: Configure SIP Signaling Interfaces

A SIP Interface consists of a combination of ports (UDP, TCP, and TLS) associated with a specific IP network interface. The SIP Interface is associated with an SRD.

The procedure below describes how to add SIP interfaces. In our example scenario, you need to add an internal and external SIP interface for the E-SBC.

➢ **To add SIP interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** > **Control Network** > **SIP Interface Table**).
2. Add a SIP interface for the LAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Settings
Index	**0**
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP	**5068** This was used to test TCP to MS Lync environment. It is recommended to set to **0** if you are only using TLS.
UDP	**5060** This supports the optional Fax supporting ATA.
SRD	**1**

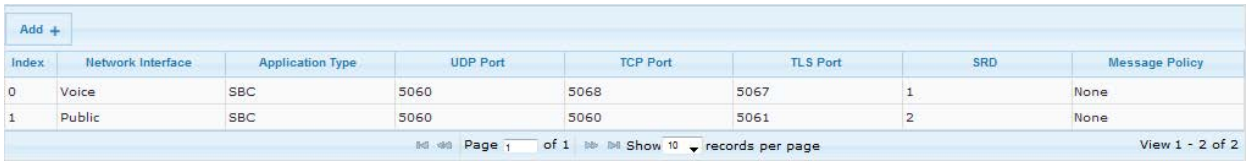
   c. Click **Submit**.
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Settings
Index	**1**
Network Interface	**Public**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	This was not used towards the ITSP but may be set to **0** to close the ports for security purposes.
SRD	**2**

   c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-11: Displaying Configured SIP Interfaces



4.4 Step 4: Configure Proxy Sets

This step describes how to configure the Proxy Sets. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). In the example scenario, you need to configure two Proxy Sets and an optional third (Fax) for the following entities:

- Microsoft Lync Server 2013
- AT&T IP Flexible Reach - EF service
- Fax supporting ATA

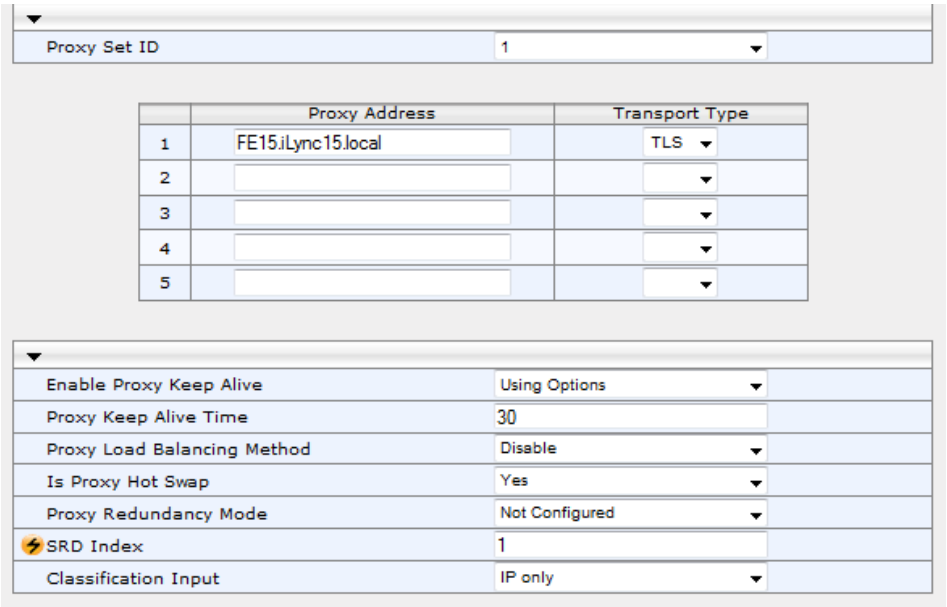
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Add a Proxy Set for Lync Server 2013:
   a. Configure the following parameters:

Parameter	Settings
Proxy Set ID	**1**
Proxy Address	**FE15.ilync15.local** This is the Lync Server 2013 SIP Trunking IP address or FQDN.
Transport Type	**TLS**
Enable Proxy Keep Alive	**Using Options**
SRD Index	**1**

Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013

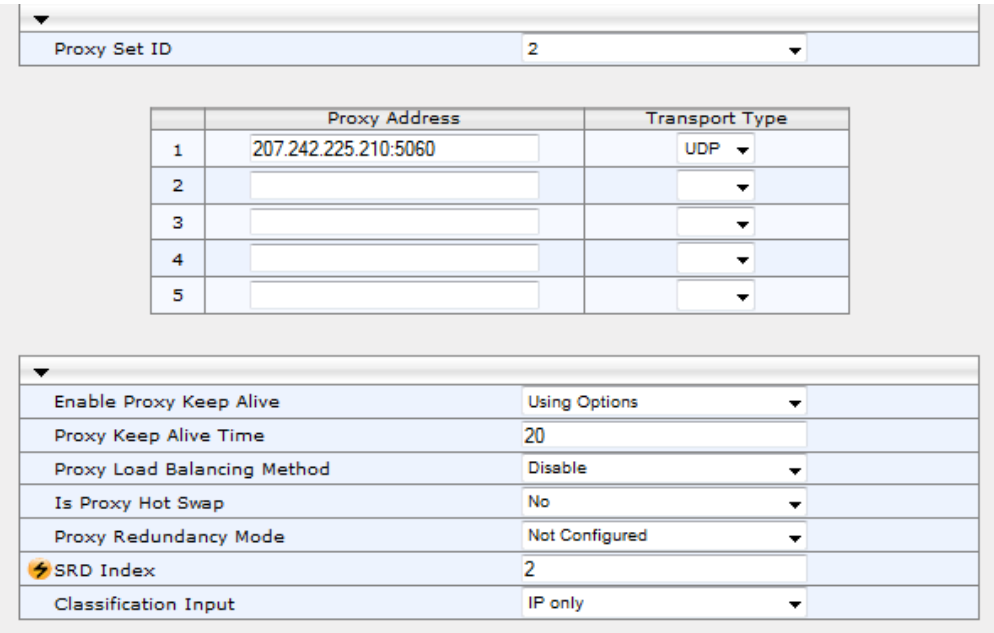


   b. Click **Submit**.

3. Add a Proxy Set for the AT&T IP Flexible Reach - EF service:
   a. Configure the following parameters:

Parameter	Settings
Proxy Set ID	**2**
Proxy Address	**207.242.225.210:5060** AT&T IP Flexible Reach - EF service IP address or FQDN and destination port
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
SRD Index	**2** This enables classification by Proxy Set for this SRD in the IP Group assigned to the AT&T IP Flexible Reach - EF service.

Figure 4-13: Configuring Proxy Set for AT&T IP Flexible Reach - EF Service

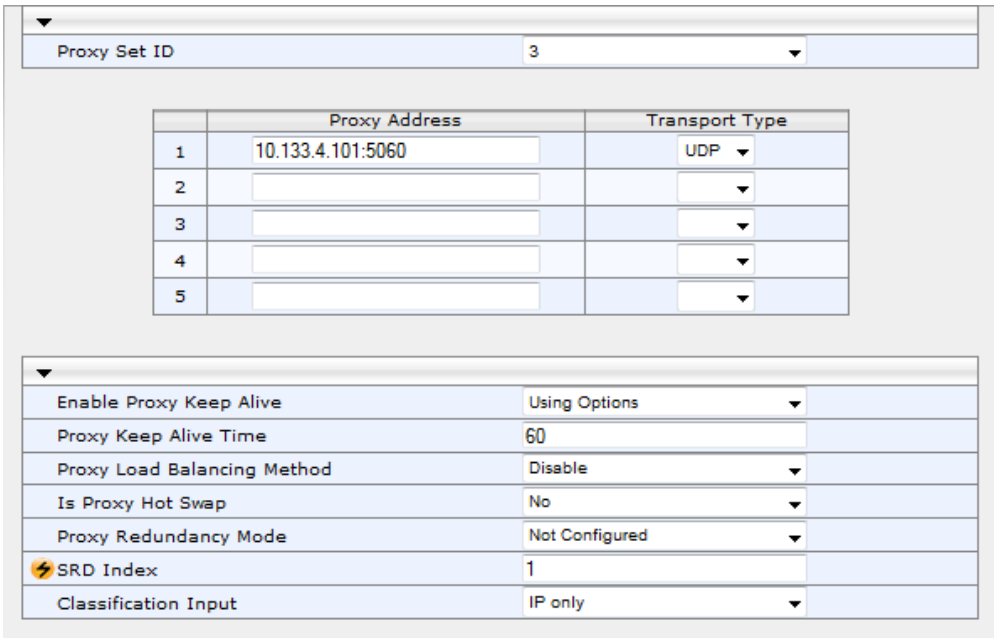


   b. Click **Submit**.

4. Add a Proxy Set for the Fax supporting ATA:
   a. Configure the following parameters:

Parameter	Settings
Proxy Set ID	**3**
Proxy Address	**10.133.4.101:5060** This is the ATA IP address or FQDN and destination port.
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
SRD Index	**1** This enables classification by Proxy Set for this SRD in the IP Group assigned to the Fax supporting ATA.

Figure 4-14: Configuring Proxy Set for Fax Supporting ATA



b. Click **Submit**.

4.5 Step 5: Configure IP Groups

This step describes how to create IP Groups. An IP Group represents a SIP entity behavior in the E-SBC's network. In our example scenario, you need to create IP Groups for the following entities:

- Lync Server 2013 (Mediation Server) on the LAN
- AT&T IP Flexible Reach - EF service on the WAN
- Fax supporting ATA (Optional)

These IP Groups are later used by the SBC application for routing calls.

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group for the Lync Server 2013 Mediation Server:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**1**
Type	**Server**
Description	**CorpLabW15**
Proxy Set ID	**1**
SIP Group Name	**FE.ILync15.local**
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

   c. Click **Submit**.
3. Add an IP Group for the AT&T IP Flexible Reach - EF service:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**2**
Type	**Server**
Description	**ATT_E_IPFR**
Proxy Set ID	**2**
SIP Group Name	**207.242.225.210**
SRD	**2**
Media Realm Name	**MRwan**
IP Profile ID	**2**

   c. Click **Submit**.

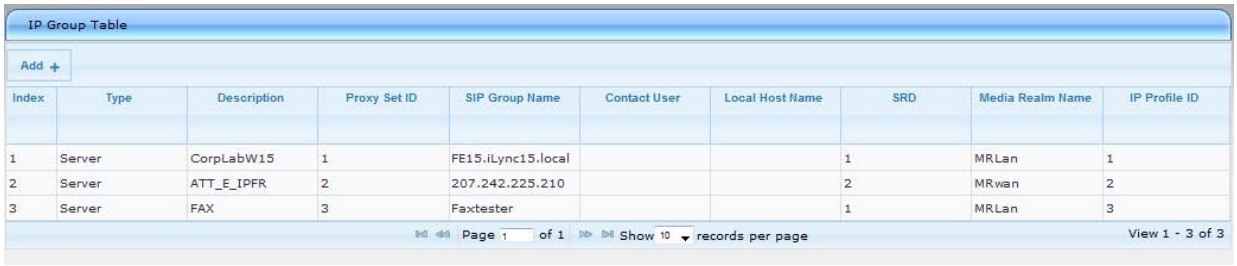
4. Add an IP Group for the AT&T IP Flexible Reach - EF service:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**3**
Type	**Server**
Description	**FAX**
Proxy Set ID	**3**
SRD	**1**
Media Realm Name	**MRwan**
IP Profile ID	**3**

   c. Click **Submit**.

The configured IP Group table is shown below:

Figure 4-15: Configuring IP Groups



4.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. In our example scenario, the IP Profiles are used to configure the SRTP / TLS modes and other parameters that differ between the two entities - Lync Server 2013 and AT&T IP Flexible Reach - EF service. Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 52).

In our example, you need to add an IP Profile for each entity:

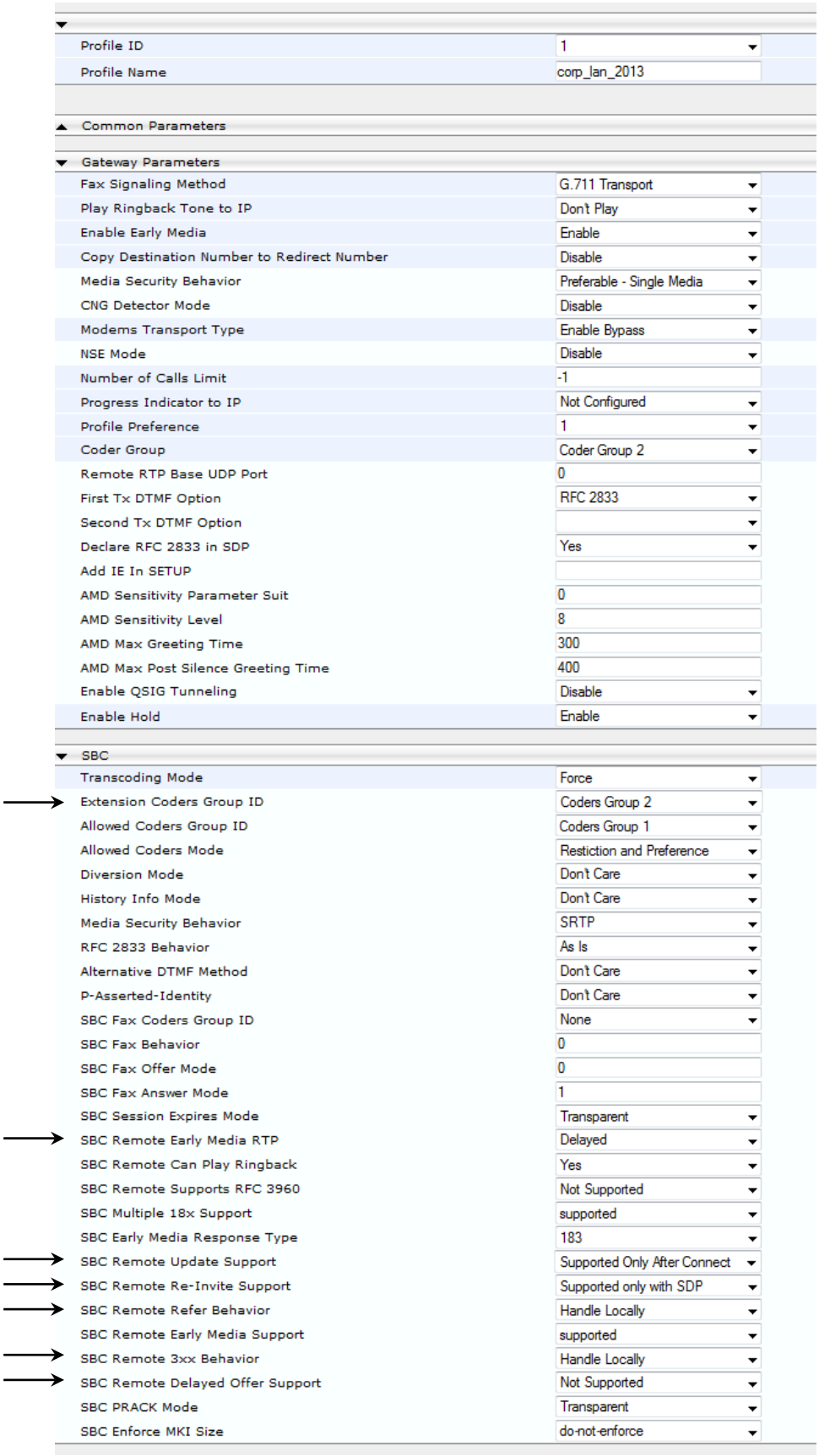
- **Microsoft Lync Server 2013** - to operate in secure mode using SRTP and TLS
- **AT&T IP Flexible Reach - EF service** - to operate in non-secure mode using RTP and UDP

➢ **To configure IP Profiles:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Add an IP Profile for Lync Server 2013:
   a. Configure the parameters as follows:

Parameter	Settings
Profile ID	**1**
Transcoding Mode	**Force**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 1**
Media Security Behavior	**SRTP**
SBC Remote Early Media RTP	**Delayed** This is required because when Lync Server 2013 sends a SIP 18x response, it does not immediately send an RTP to the remote side.
SBC Early Media Response Type	**183**
SBC Remote Update Support	**Supported Only After Connect**
SBC Remote Re-INVITE Support	**Supported Only With SDP**
SBC Remote Refer Behavior	**Handle Locally** This is required as Lync Server 2013 does not support receipt of REFER messages.
SBC Remote 3xx Behavior	**Handle Locally** This is required as Lync Server 2013 does not support receipt of SIP 3xx responses.
SBC Remote Delayed Offer Support	**Not Supported**

Figure 4-16: Configuring IP Profile for Lync Server 2013



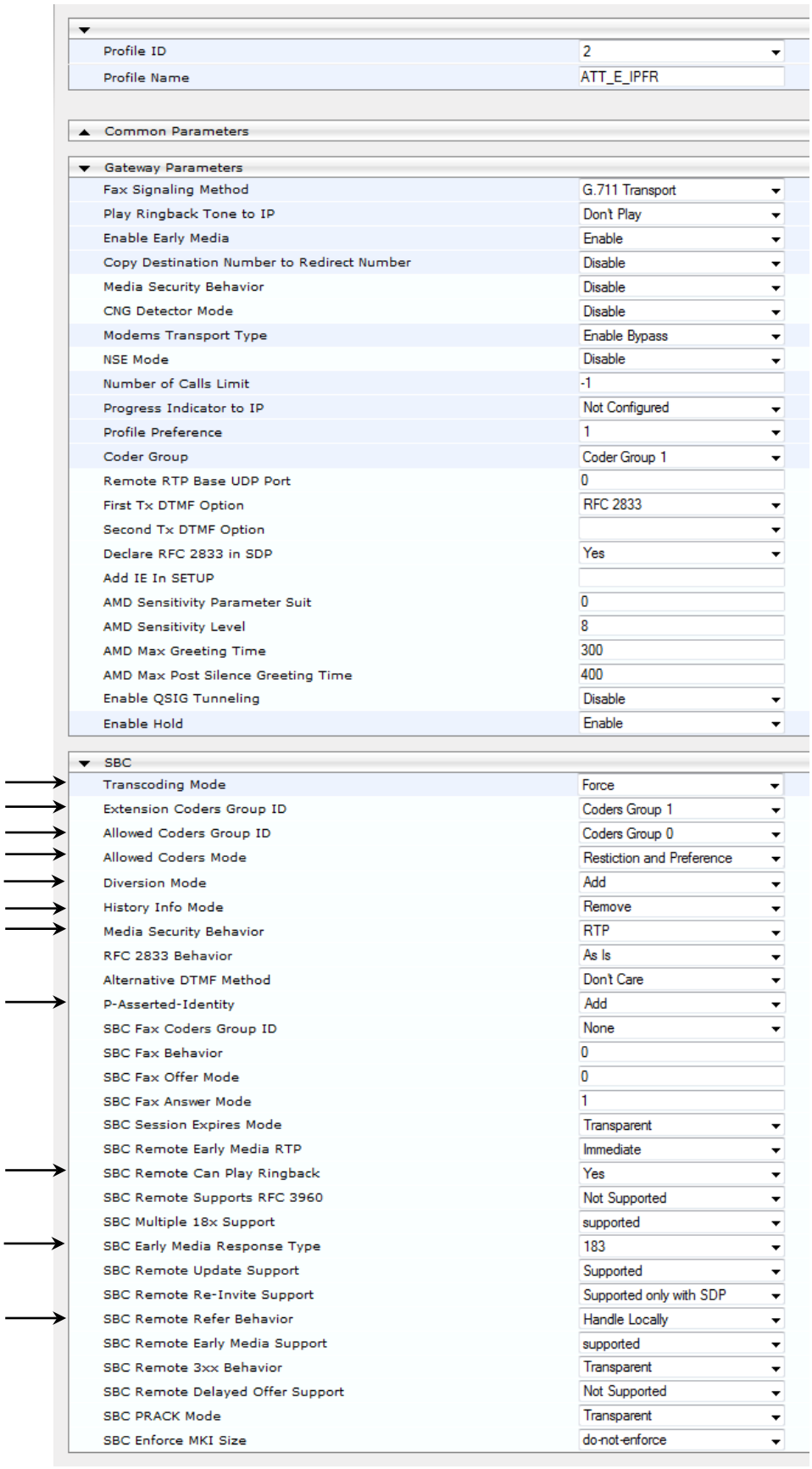
Profile ID	1
Profile Name	corp_lan_2013
Common Parameters	
Gateway Parameters	
Fax Signaling Method	G.711 Transport
Play Ringback Tone to IP	Don't Play
Enable Early Media	Enable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Preferable - Single Media
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Coder Group 2
Remote RTP Base UDP Port	0
First Tx DTMF Option	RFC 2833
Second Tx DTMF Option	
Declare RFC 2833 in SDP	Yes
Add IE In SETUP	
AMD Sensitivity Parameter Suit	0
AMD Sensitivity Level	8
AMD Max Greeting Time	300
AMD Max Post Silence Greeting Time	400
Enable QSIG Tunneling	Disable
Enable Hold	Enable
SBC	
Transcoding Mode	Force
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 1
Allowed Coders Mode	Restiction and Preference
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	SRTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Delayed
SBC Remote Can Play Ringback	Yes
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	supported
SBC Early Media Response Type	183
SBC Remote Update Support	Supported Only After Connect
SBC Remote Re-Invite Support	Supported only with SDP
SBC Remote Refer Behavior	Handle Locally
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Handle Locally
SBC Remote Delayed Offer Support	Not Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce

b. Click **Submit**.

3. Add an IP Profile for the AT&T IP Flexible Reach - EF service:
   a. Configure the parameters as follows:

Parameter	Settings
Profile ID	**2**
Transcoding Mode	**Force**
Extension Coders Group ID	**Coders Group 0**
Allowed Coders Group ID	**Coders Group 1**
Allowed Coders Mode	**Restrict and Preference** This enables the received SDP offer to list Allowed coders first and then restrict the original coders received in the SDP to the list.
Diversion Mode	**Add** This provides a proper Diversion Header for forward calls based off of the received History Info header from Lync Server 2013 prior to delivery to AT&T IPFR - EF services.
History Info Mode	**Remove** This is utilized on a forward from Lync Server 2013 and is removed when sending to AT&T IPFR - EF services.
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** This is required for anonymous calls.
SBC Remote Can Play Ringback	**No** This is required as Lync Server 2013 does not provide a Ringback tone for incoming calls.
SBC Early Media Response Type	**183**
SBC Remote Refer Behavior	**Handle Locally** E-SBC handles the incoming REFER request itself without forwarding the REFER towards the SIP Trunk.

Figure 4-17: Configuring IP Profile for AT&T IP Flexible Reach - EF Service

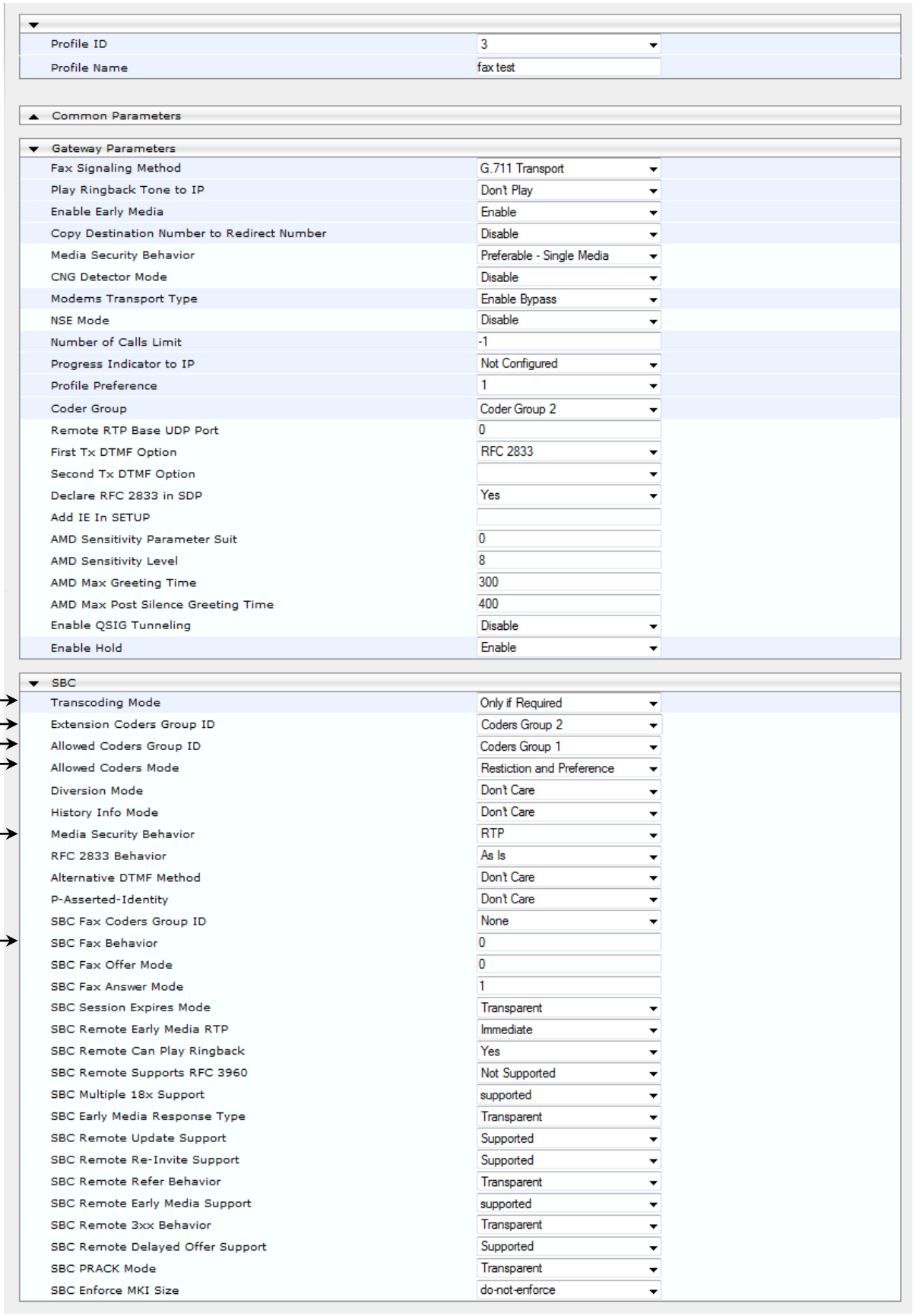


b. Click **Submit**.

4. Add an IP Profile for the fax supporting ATA:
   a. Configure the parameters as follows:

Parameter	Settings
Profile ID	**3**
Transcoding Mode	**Only if Required**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 1**
Allowed Coders Mode	**Restriction and Preference** This enables the received SDP offer to list Allowed coders first and then restrict the original coders received in the SDP to the list.
Media Security Behavior	**RTP**
SBC Fax Behavior	**0** This is the default setting and enables the device to forward the received fax as is (i.e., without intervention).

Figure 4-18: Configuring IP Profile for Fax Supporting ATA



Profile ID	3
Profile Name	fax test
Common Parameters	
Gateway Parameters	
Fax Signaling Method	G.711 Transport
Play Ringback Tone to IP	Don't Play
Enable Early Media	Enable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Preferable - Single Media
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Coder Group 2
Remote RTP Base UDP Port	0
First Tx DTMF Option	RFC 2833
Second Tx DTMF Option	
Declare RFC 2833 in SDP	Yes
Add IE In SETUP	
AMD Sensitivity Parameter Suit	0
AMD Sensitivity Level	8
AMD Max Greeting Time	300
AMD Max Post Silence Greeting Time	400
Enable QSIG Tunneling	Disable
Enable Hold	Enable
SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 1
Allowed Coders Mode	Restiction and Preference
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Immediate
SBC Remote Can Play Ringback	Yes
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	supported
SBC Early Media Response Type	Transparent
SBC Remote Update Support	Supported
SBC Remote Re-Invite Support	Supported
SBC Remote Refer Behavior	Transparent
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Transparent
SBC Remote Delayed Offer Support	Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce

b. Click **Submit**.

4.7 Step 7: Configure Coders

This step describes how to configure coders (termed *Coder Groups*). You can configure up to four different and unique Coder Groups. As Lync Server 2013 supports the G.711 coder while the network connection to AT&T IP Flexible Reach - EF Service may prefer or restrict you to operate with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder as the preferred vocoder for the AT&T IP Flexible Reach - EF service.

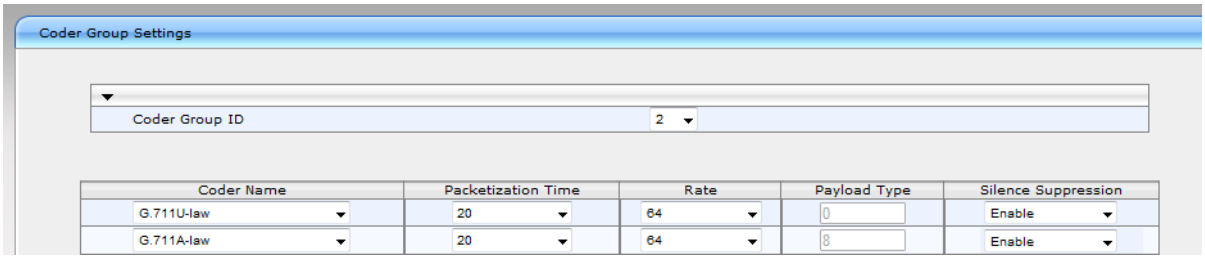
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 54).

➢ **To configure coders:**

1. Add a Coder Group for Lync Server 2013.
   a. Configure the parameters as follows:

Parameter	Settings
Coder Group ID	**2**
Coder Name	**G.711 U-law**
Coder Name	**G.711 A-law**
Silence Suppression	**Enable**

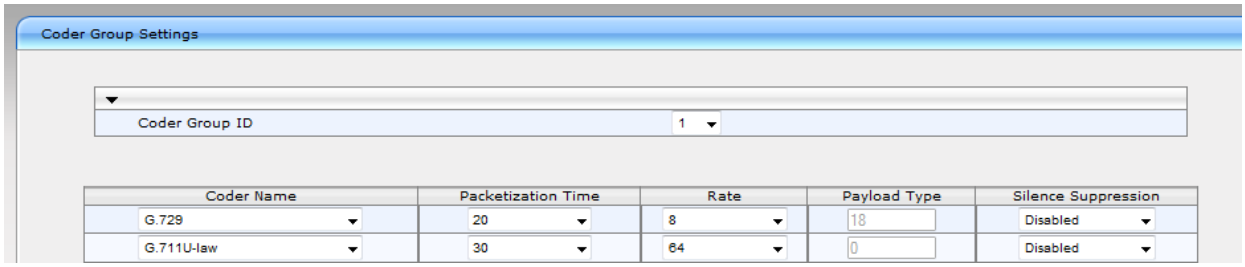
Figure 4-19: Configuring Coders for Lync Server 2013



2. Add a Coder Group for AT&T IP Flexible Reach - EF service:
   a. Configure the parameters as follows:

Parameter	Settings
Coder Group ID	**1**
Coder Name	**G.729**
Coder Name	**G.711 U-law with Packetization Time set to 30**
Silence Suppression	**Disabled**

Figure 4-20: Configuring Coders for AT&T IP Flexible Reach - EF Service



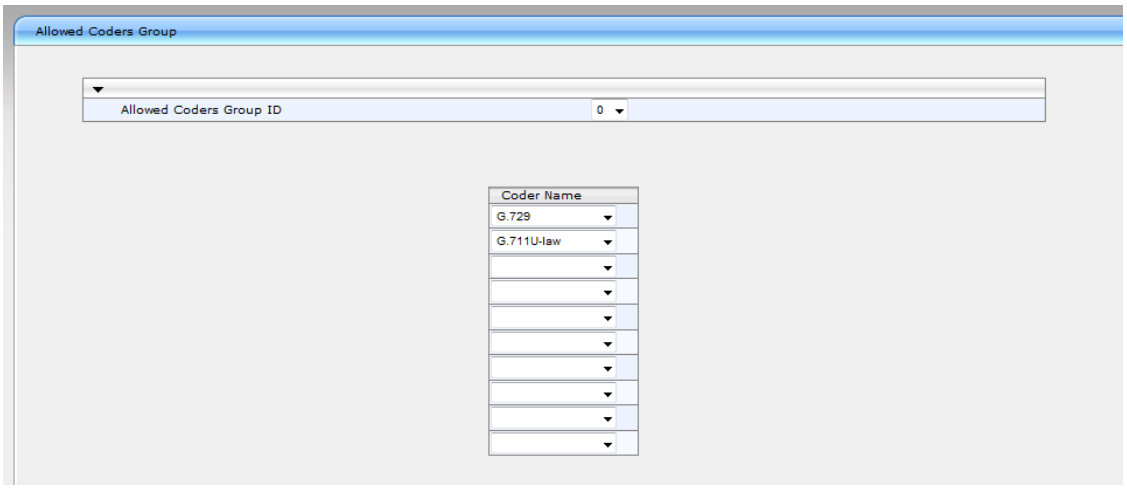
   a. Click **Submit**.

The procedure below adds an Allowed Coders Group to ensure that voice sent to the AT&T IP Flexible Reach - EF service uses the G.729 coder whenever possible as the preferred choice. Note that this Allowed Coders Group ID (and its *restriction and preference*) was assigned to the IP Profile belonging to the AT&T IP Flexible Reach - EF service in the previous step (see Section 4.6 on page 54).

➢ **To set a preferred coder for the AT&T IP Flexible Reach - EF service:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).

Figure 4-21: Setting Preferred Coder for AT&T IP Flexible Reach - EF Service

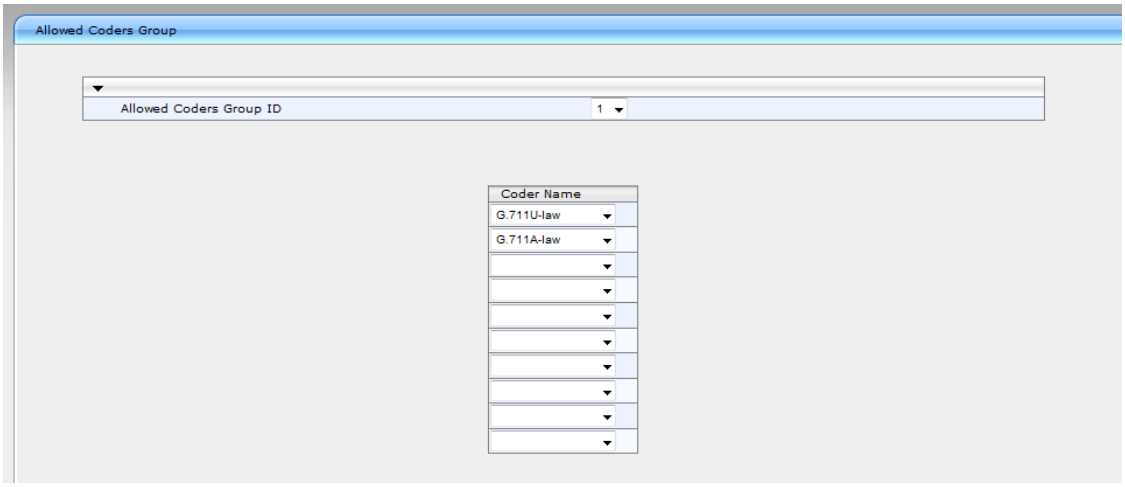


2. From the 'Allowed Coders Group ID' drop-down list, select **0**.
3. From the 'Coder Name' drop-down list, select **G.729**.
4. Click **Submit**.

➢ **To set a preferred coder for the Lync Server 2013:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).

Figure 4-22: Setting Preferred Coder for Lync Server 2013



2. From the 'Allowed Coders Group ID' drop-down list, select **1**.
3. From the 'Coder Name' drop-down list, select **G.711 U-law and G711 A-law**.
4. Click **Submit**.

4.8 Step 8: SIP TLS Connection Configuration

This step describes how to configure the E-SBC for using a TLS connection with the Lync Server 2013 Mediation Server. This is essential for a secure SIP TLS connection.

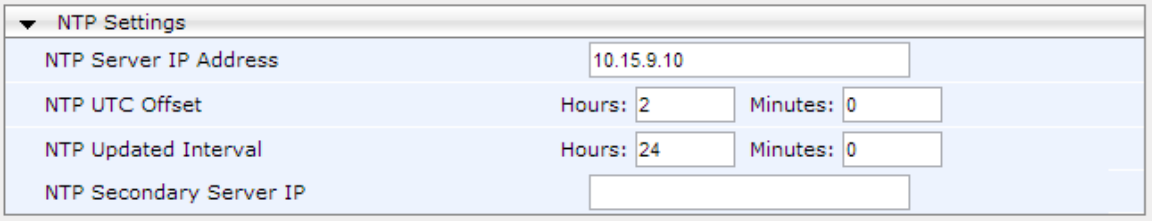
4.8.1 Step 8a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or third-party server) to ensure that the E-SBC receives accurate and current date and time. This is necessary for validating certificates of remote parties.

➢ **To configure the NTP server address:**

1. Open the Application Settings page (**Configuration** tab > **System** > **Application Settings**); the following screen appears.

Figure 4-23: Configuring NTP Server Address



2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., "10.15.9.10").
3. Click **Submit**.

4.8.2 Step 8b: Configure a Certificate

This step describes how to exchange a certificate with the Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Lync Server.

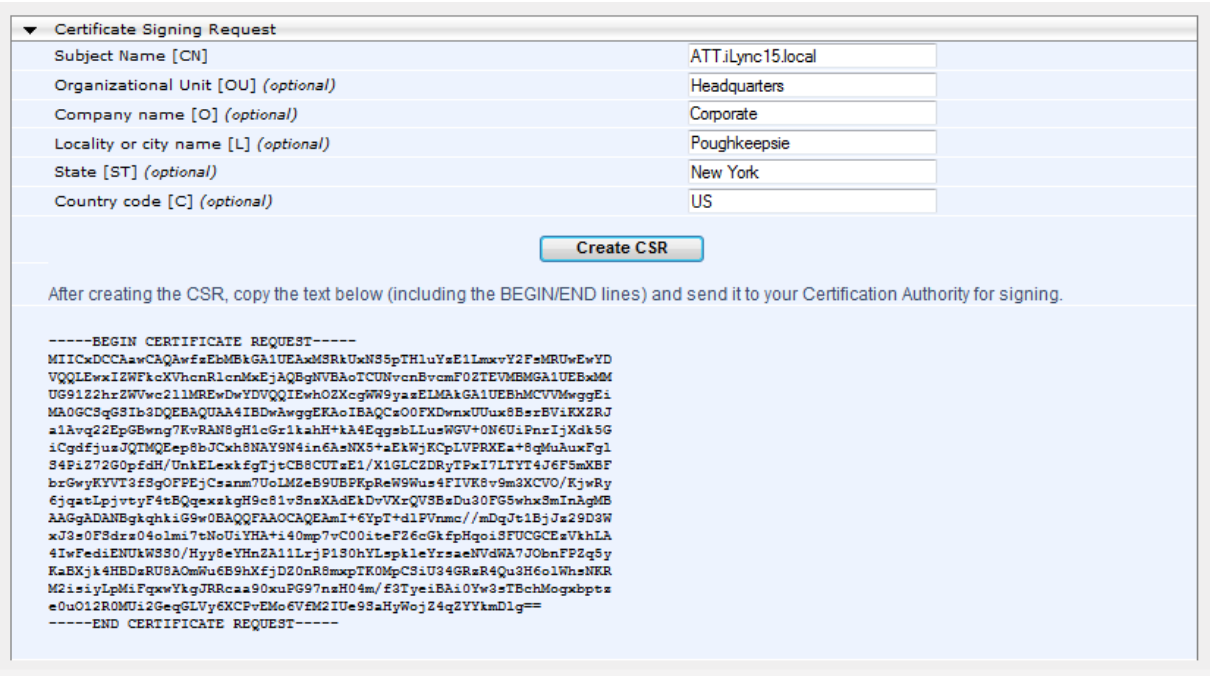
It is composed of the following steps:

1. Generating a Certificate Signing Request (CSR)
2. Requesting Device Certificate from CA
3. Obtaining Trusted Root Certificate from CA
4. Deploying Device and Trusted Root certificates on the E-SBC

➢ **To configure a certificate:**

1. Open the Certificates page (**Configuration** tab > **System** > **Certificates**); the following screen appears:

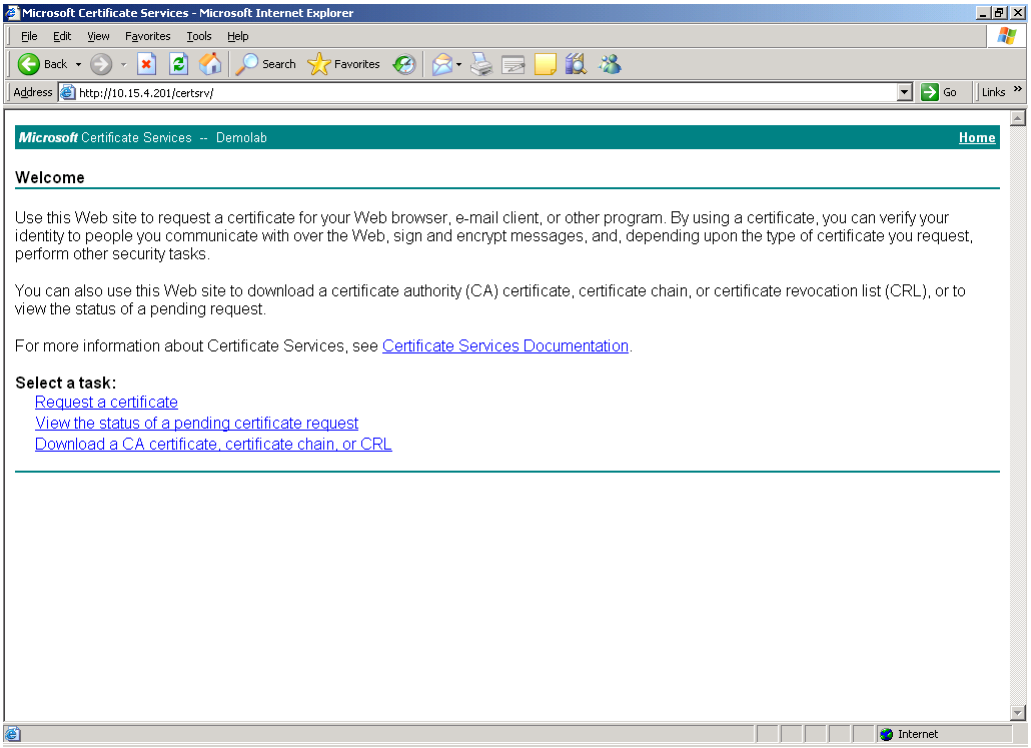
Figure 4-24: Configuring Certificates



2. In the Subject Name field, enter the media gateway name (e.g., "ATT.iLync15.local"). This name must be equivalent to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 19).
3. Click **Create CSR**; a certificate request is generated.
4. Copy the CSR (from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----") to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.

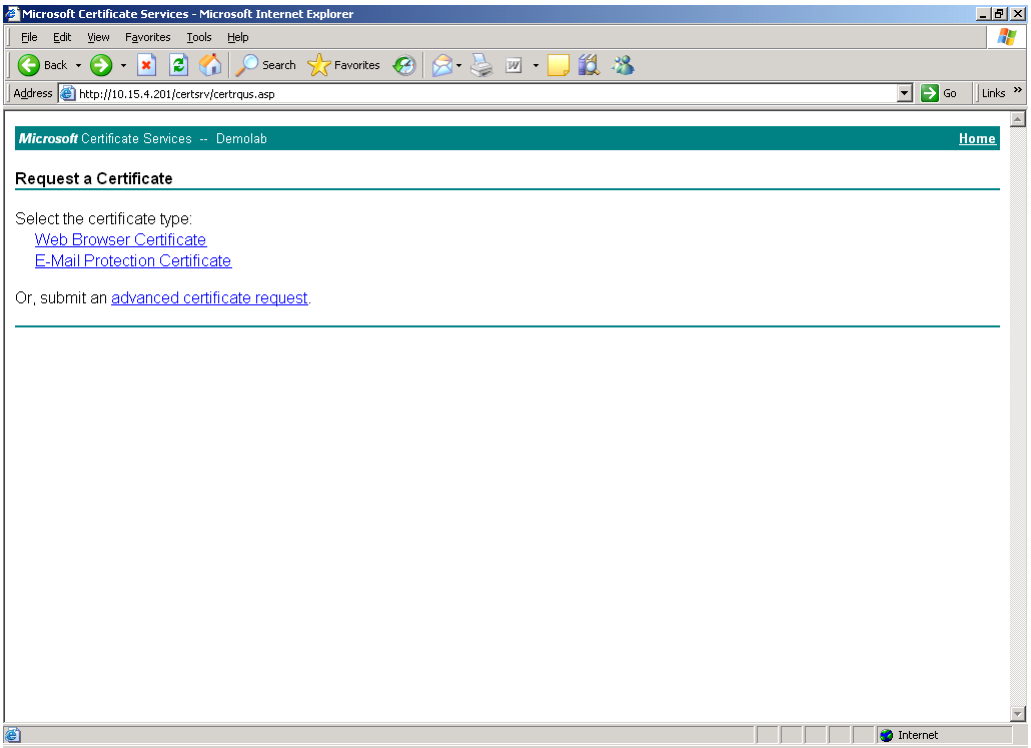
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-25: Navigating to Microsoft Certificate Services Web Site



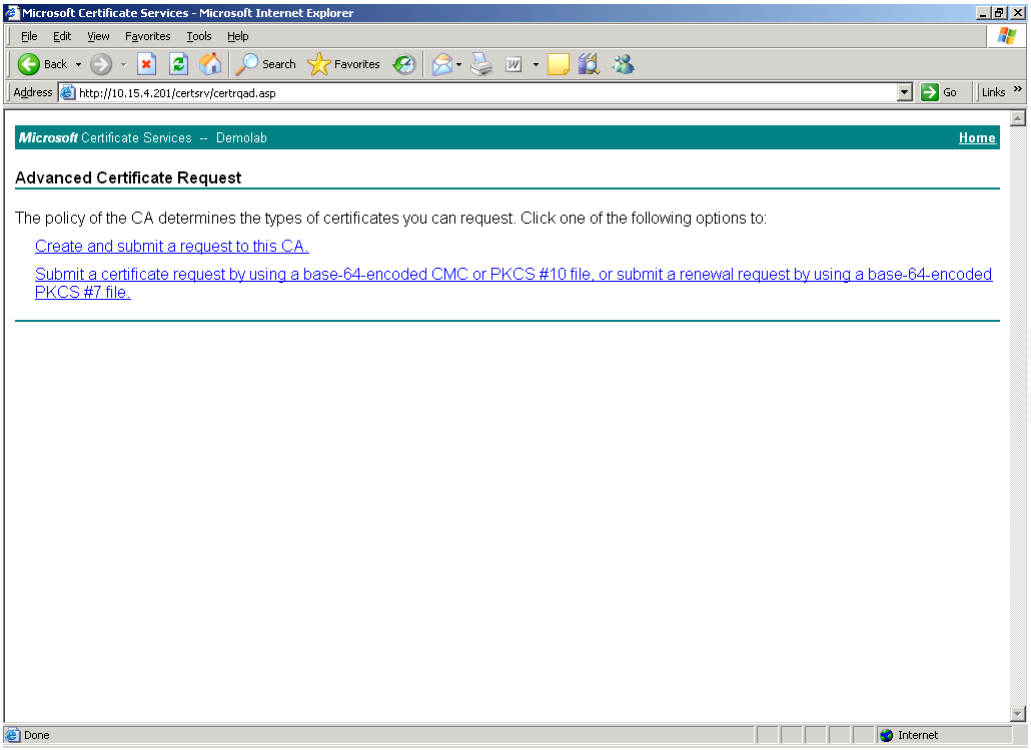
6. Click **Request a certificate**.

Figure 4-26: Requesting a Certificate



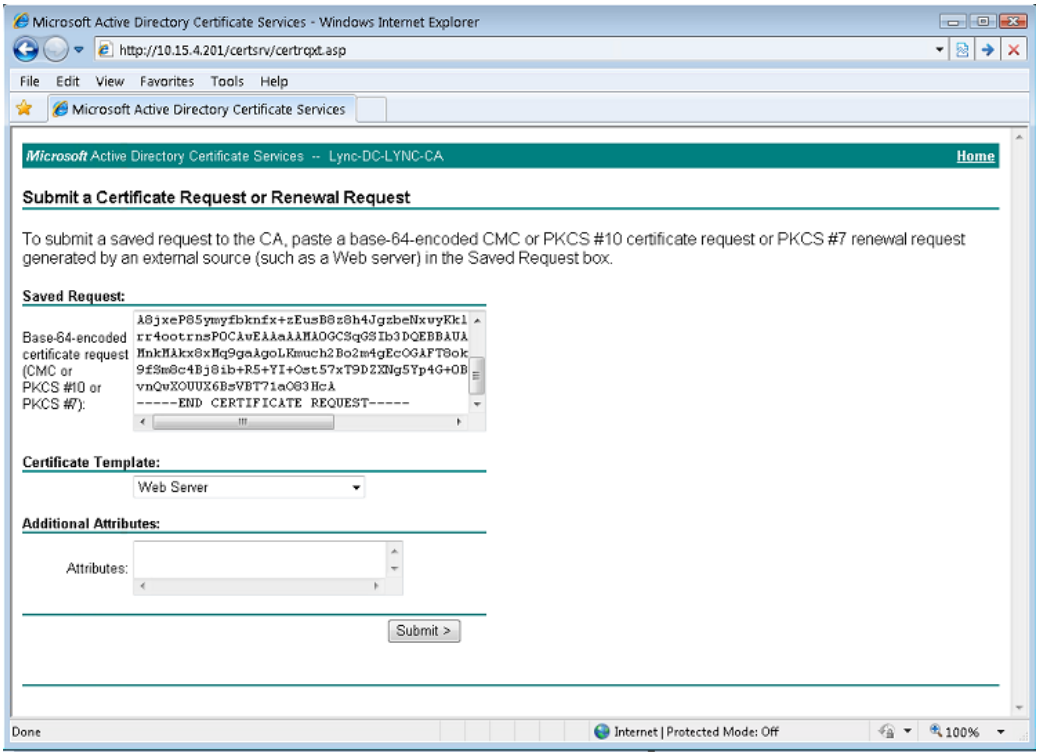
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-27: Selecting Advanced Certificate Request



8. Click **Submit a certificate request ...**, and then click **Next**.

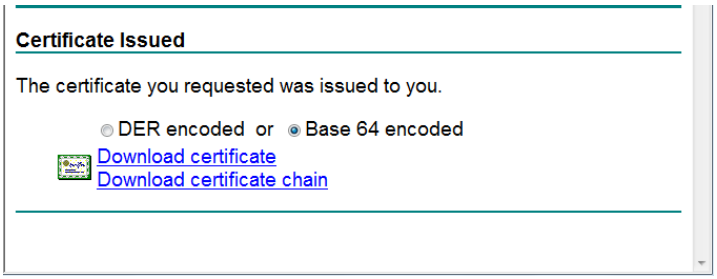
Figure 4-28: Submitting a Certificate Request



9. Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Base64 Encoded Certificate Request' field.

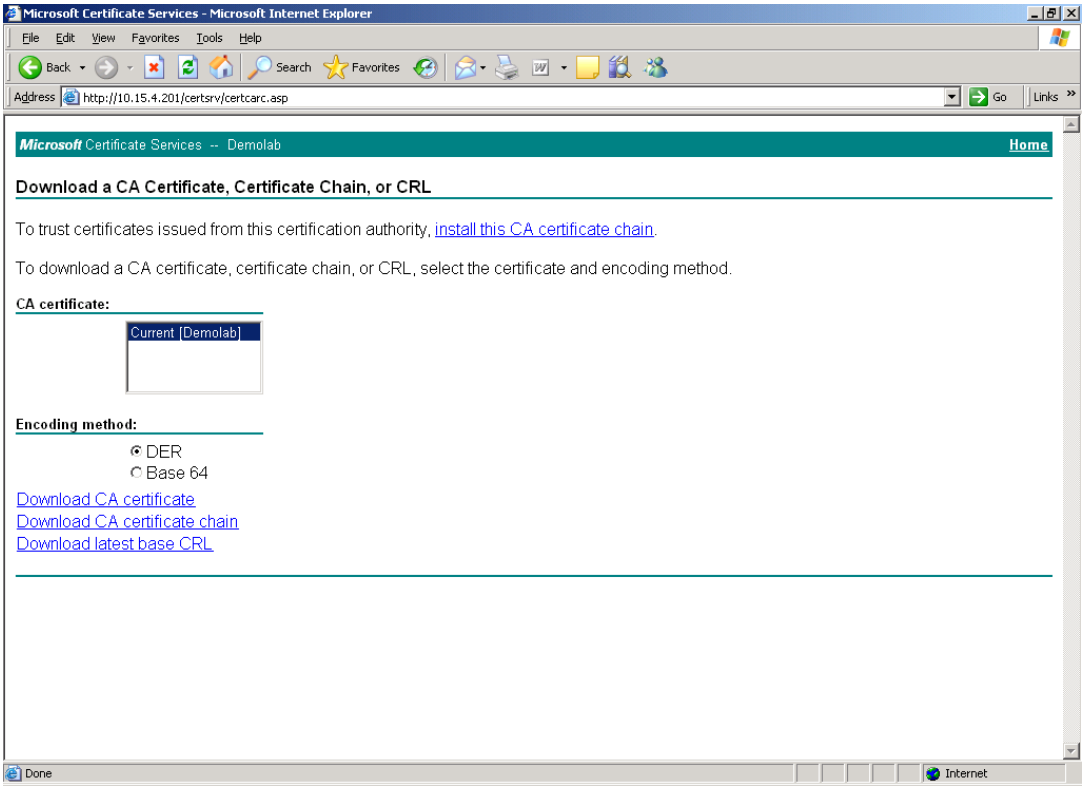
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-29: Displaying Certificate Issued



12. Select the **Base 64 encoded** option for encoding, and then click **Download CA certificate**.
13. Save the file with the name *gateway.cer* to a folder on your computer.
14. Click the **Home** button (or navigate to the certificate server at http://<Certificate Server>/CertSrv).
15. Click the **Download a CA certificate**, **certificate chain, or CRL**.

Figure 4-30: Downloading a CA Certificate



16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file with the name *certroot.cer* to a folder on your computer.

19. In the E-SBC's Web interface, return to the Certificates page and do the following:
    a. In the 'Device Certificate' field, click **Browse** and select the *gateway.cer* certificate file that you saved on your computer in Step 13, and then click **Send File** to upload the certificate to the E-SBC.
    b. In the 'Trusted Root Certificate Store' field, click **Browse** and select the *certroot.cer* certificate file that you saved on your computer in Step 18, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-31: Uploading Certificate

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 103).

4.9 Step 9: Configure SRTP

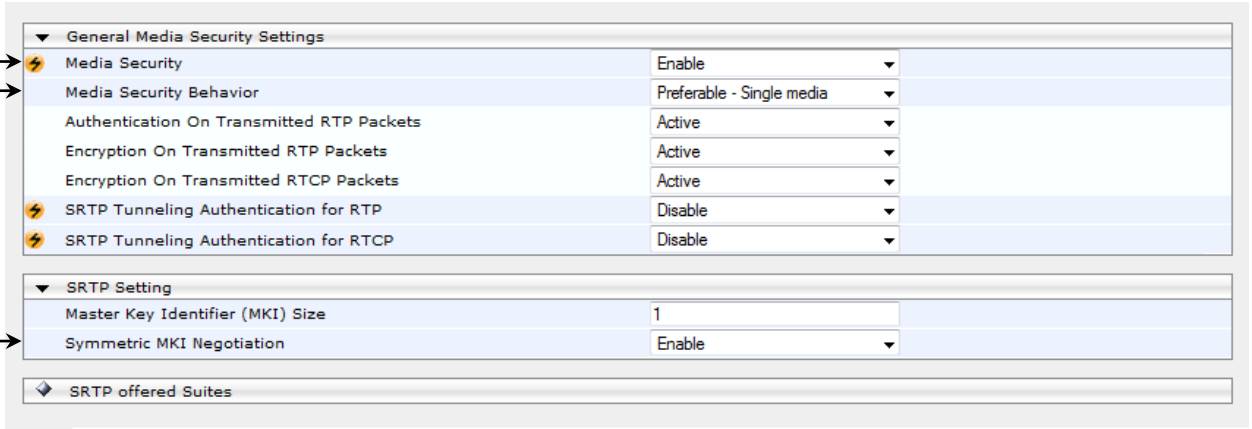
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), you need to configure the E-SBC to operate in the same manner.

Note that SRTP was enabled for Lync Server 2013 when you added an IP Profile for Lync Server 2013 (see Section 4.6 on page 54).

➢ **To configure media security:**

1. Open the Media Security page (**Configuration** tab > **Media** > **Media Security**).

Figure 4-32: Configuring Media Security



2. Configure the parameters as follows:

Parameter	Settings
Media Security	**Enable**
Master Key Identifier (MKI) Size	**1**
Symmetric MKI Negotiation	**Enable**

3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 103).

4.10 Step 10: Configure Number of Media Channels

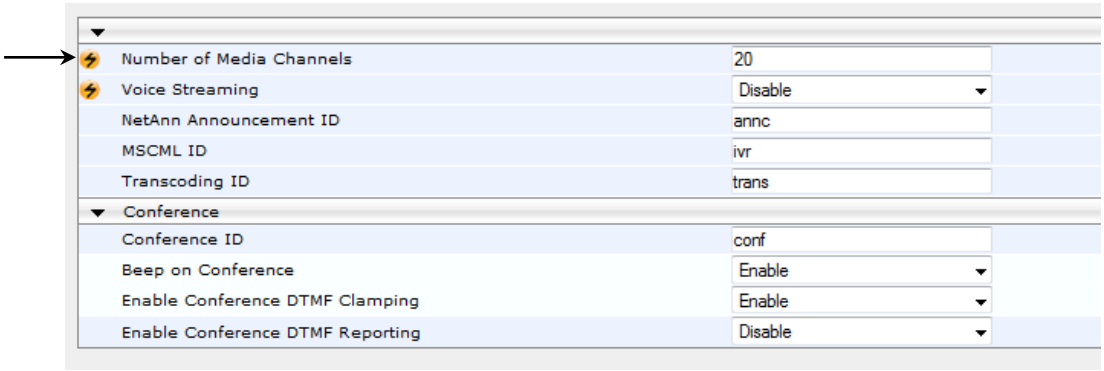
This step describes how to configure the number of media channels for IP-based media. To perform coder transcoding, define digital signaling processors (DSP) channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to sessions.

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

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

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

Figure 4-33: Configuring the Number of Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g.,"20").
3. Click **Submit**.

4.11 Step 11: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules (which are done in the IP-to-IP Routing table). These rules define the route for forwarding SIP messages (e.g., INVITE) received on one IP interface to another.

The SIP message is routed according to a rule whose configured input characteristics (e.g., Source IP Group) match those of the message. If the characteristics of an incoming message do not match the first rule in the table, they are then compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

In our example scenario, you need to add the following IP-to-IP routing rules to route calls between Lync Server 2013 (LAN) and AT&T IP Flexible Reach - EF service (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the WAN
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Terminate SIP OPTIONS messages on the E-SBC that are received from the ATA
- Calls from LAN to WAN.
- Calls from WAN to Fax supporting LAN ATA.
- Calls from LAN ATA to WAN.
- Calls from WAN to LAN.

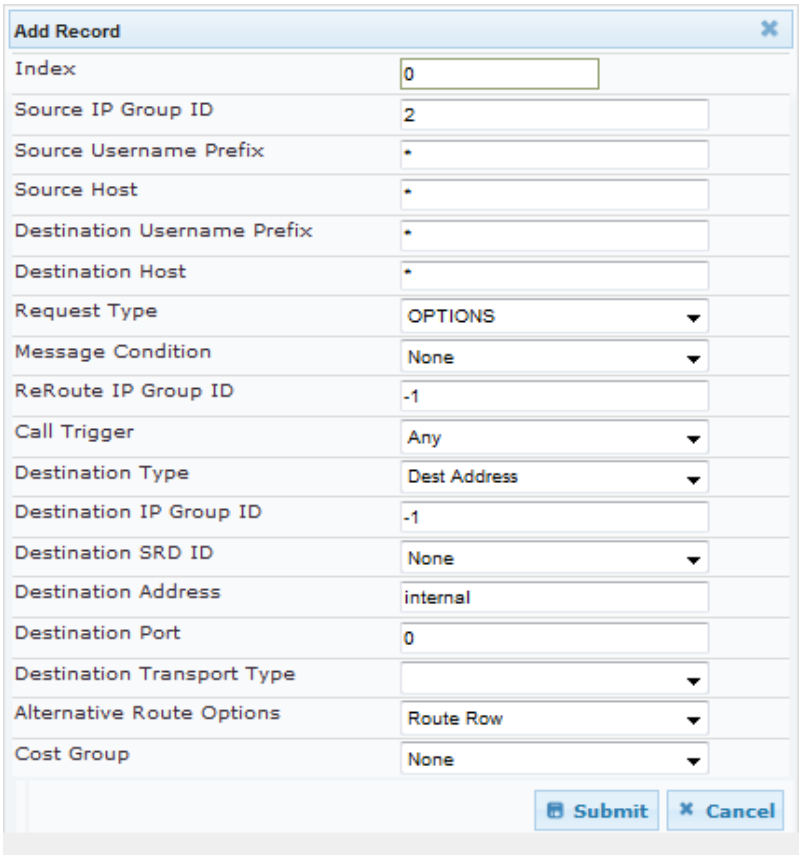
The routing rules use IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 52, IP Group ID 1 was assigned to Lync Server 2013, IP Group ID 2 to AT&T IP Flexible Reach - EF service, and IP Group ID 3 to the Fax supporting ATA.

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

1. Open the IP2IP Routing Table page (**Configuration** > **VoIP** > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to terminate SIP OPTIONS messages received from the WAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**0**
Source IP Group ID	**2**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

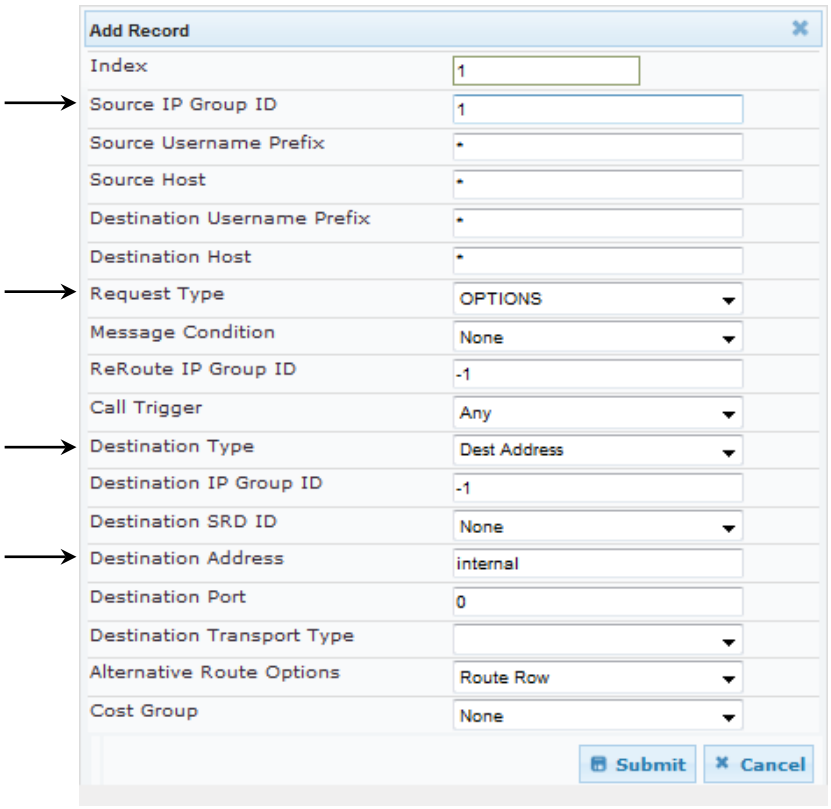
Figure 4-34: Configuring IP-to-IP Routing Rules



3. Add a rule to terminate SIP OPTIONS messages received from the LAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**1**
Source IP Group ID	**1**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

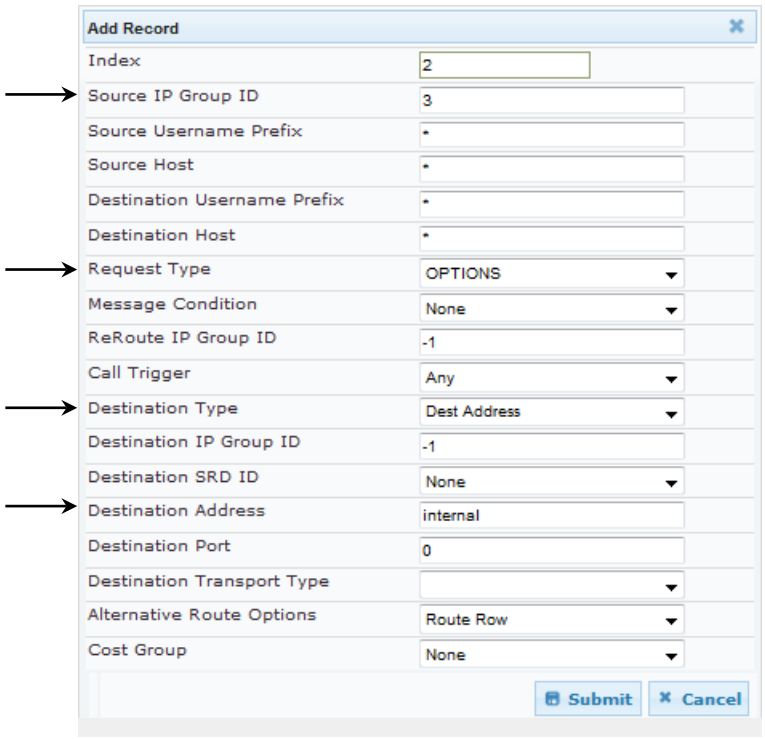
Figure 4-35: Adding Rule to Terminate SIP Options from LAN



4. Add a rule to terminate SIP OPTIONS messages received from the ATA:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**2**
Source IP Group ID	**2**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

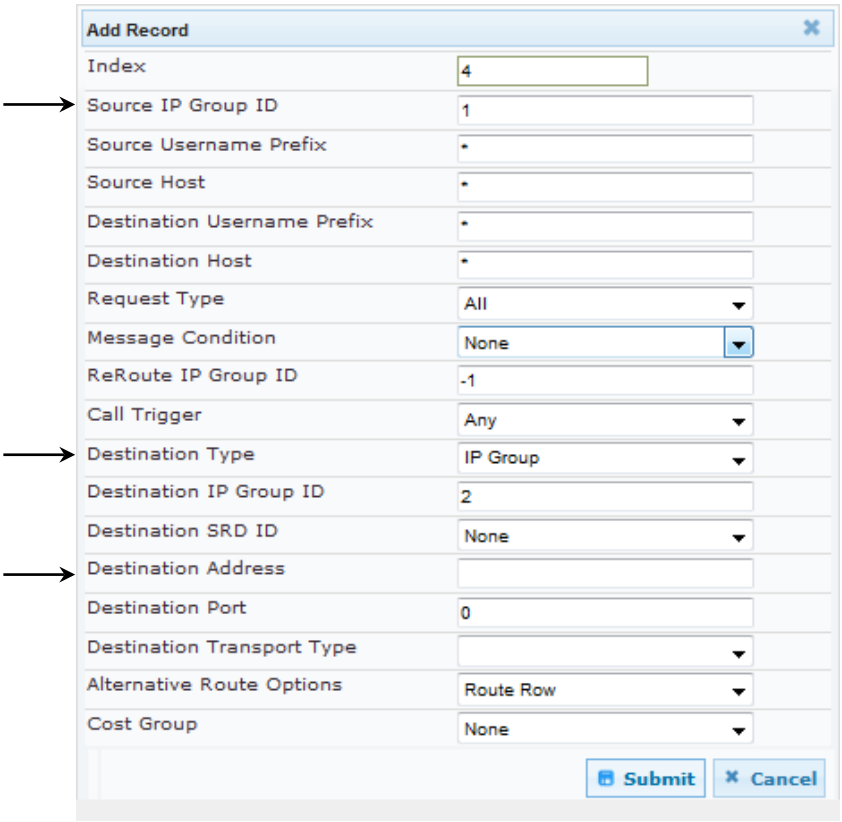
Figure 4-36: Adding Rule to Terminate SIP Options from ATA



5. Add a rule to route calls from LAN to WAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**4**
Source IP Group ID	**1**
Destination Type	**IP Group**
Destination IP Group ID	**2**

Figure 4-37: Configuring IP-to-IP Routing Rule for LAN to WAN

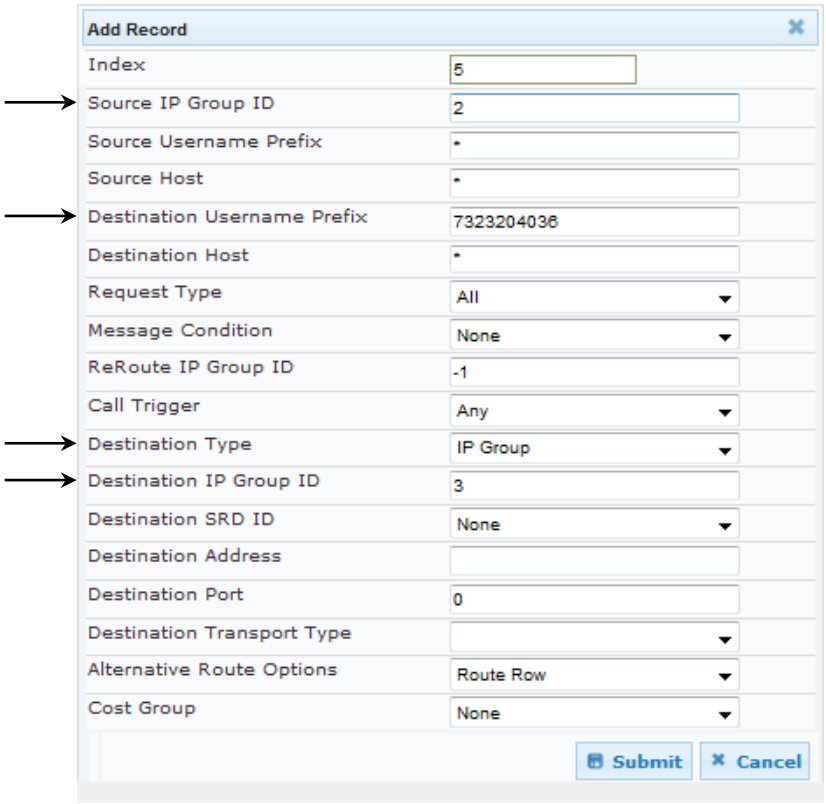


   c. Click **Submit**.

6. Add a rule to route calls from WAN to LAN Fax supporting ATA:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**5**
Source IP Group ID	**2**
Destination Username Prefix	**7323204036** (screening of fax number)
Destination Type	**IP Group**
Destination IP Group ID	**3**

Figure 4-38: Configuring IP-to-IP Routing Rule for WAN to LAN Fax ATA

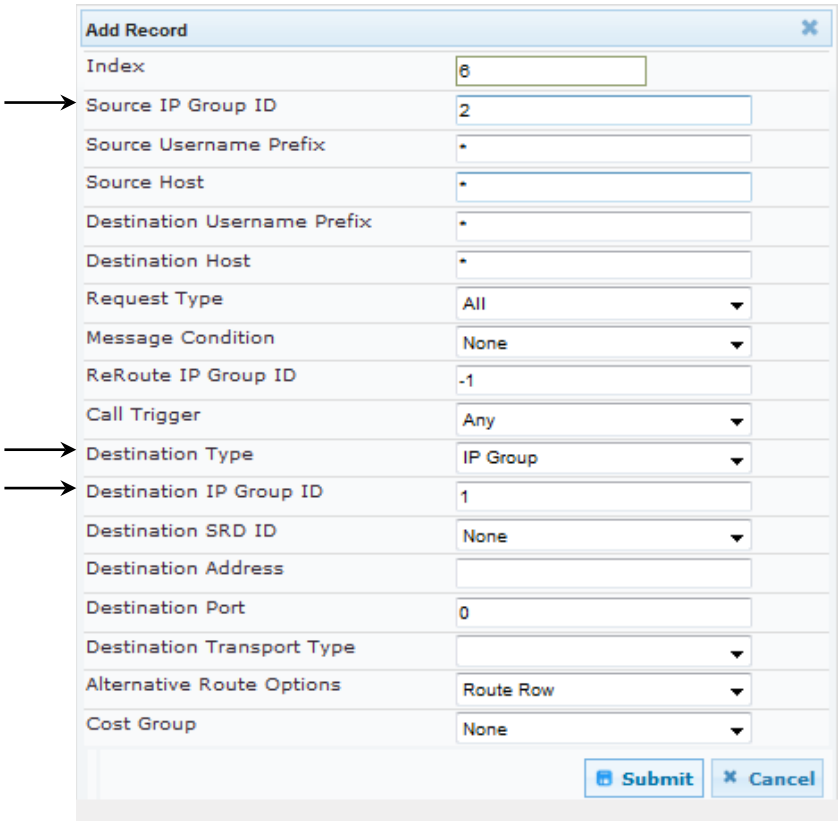


   c. Click **Submit**.

7. Add a rule to route calls from WAN to LAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**6**
Source IP Group ID	**2**
Destination Type	**IP Group**
Destination IP Group ID	**1**

Figure 4-39: Configuring IP-to-IP Routing Rule for WAN to LAN

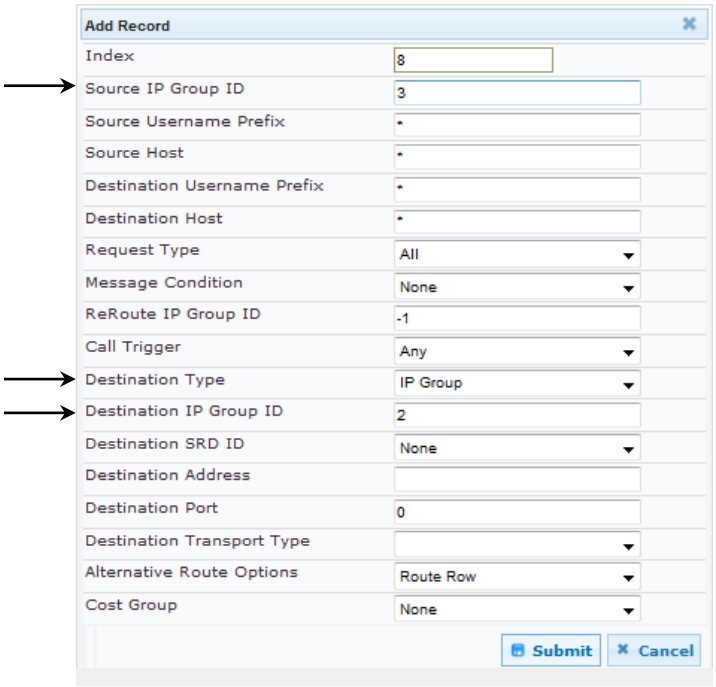


   c. Click **Submit**.

8. Add a rule to route calls from Fax ATA LAN to WAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**8**
Source IP Group ID	**3**
Destination Type	**IP Group**
Destination IP Group ID	**2**

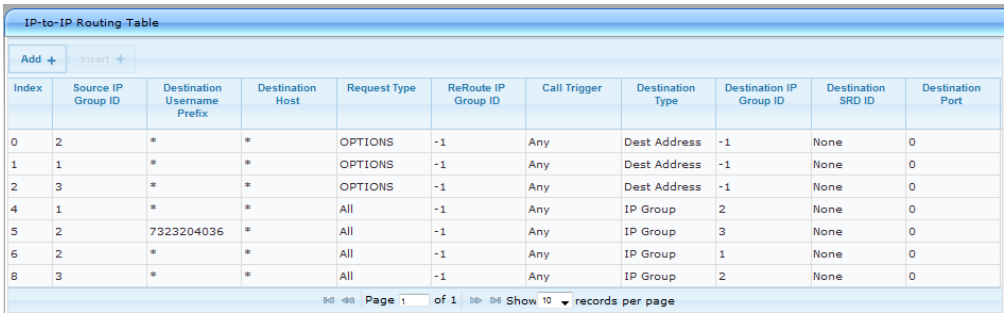
Figure 4-40: Configuring IP-to-IP Routing Rule for WAN to LAN



   c. Click **Submit**.

The figure below shows the above configured routing rules in the IP-to-IP Routing Table:

Figure 4-41: Displaying Configured IP-to-IP Routing Rules



Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	ReRoute IP Group ID	Call Trigger	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Port
0	2	*	*	OPTIONS	-1	Any	Dest Address	-1	None	0
1	1	*	*	OPTIONS	-1	Any	Dest Address	-1	None	0
2	3	*	*	OPTIONS	-1	Any	Dest Address	-1	None	0
4	1	*	*	All	-1	Any	IP Group	2	None	0
5	2	7323204036	*	All	-1	Any	IP Group	3	None	0
6	2	*	*	All	-1	Any	IP Group	1	None	0
8	3	*	*	All	-1	Any	IP Group	2	None	0

Page 1 of 1 Show 10 records per page

Note: This is a routing configuration example. It will require change according to the local deployment topology. See User's Manual for further details.

4.12 Step 12: Configure IP-to-IP Manipulation

This step describes how to configure IP-to-IP manipulation rules. These rules concern number manipulation of the source and / or destination number. The manipulation rules use IP Groups to denote the source and destination of the call. In general, manipulation can be performed as it pertains to incoming or outgoing directions during call handling. As configured in Section 4.5 on page 52, IP Group ID 1 was assigned to Lync Server 2013, IP Group ID 2 to the AT&T IP Flexible Reach - EF service, and IP Group ID 3 to the Fax supporting ATA.

Note: Adapt the manipulation table according to you environment dial plan. Below is an example configuration performed within both the inbound as well as outbound manipulation tables. You may consolidate rules within the usage of the Outbound manipulation table. The below references are for example purposes.

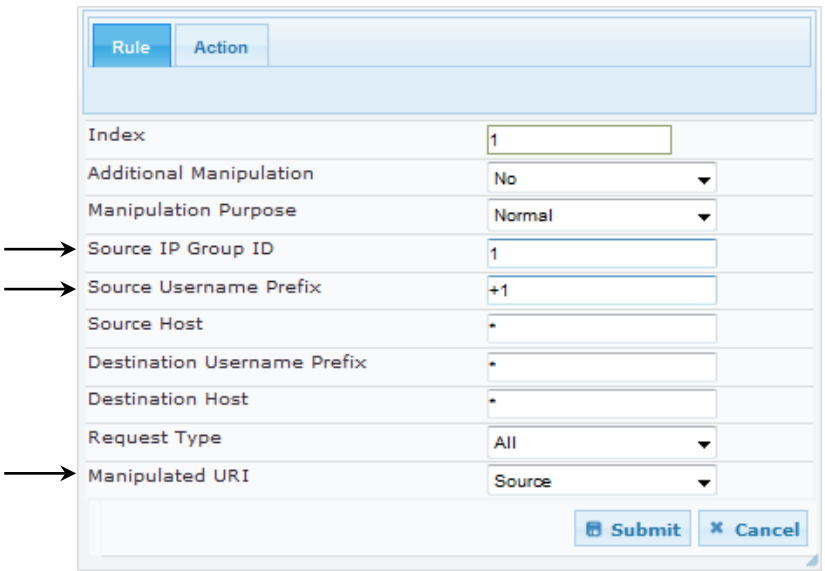
The procedure below provides an example of configuring a manipulation rule that adds the plus "+1" to the destination number for calls from IP Group 2 (AT&T IP Flexible Reach - EF service) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number ("*").

➢ **To configure a number manipulation rule:**

1. Open the IP to IP Inbound Manipulation page (**Configuration** > **VoIP** > **SBC** > **Manipulation SBC** > **IP to IP Inbound**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Settings
Index	**1**
Source IP Group ID	**1**
Source Username Prefix	**+1**
Manipulated URI	**Source**

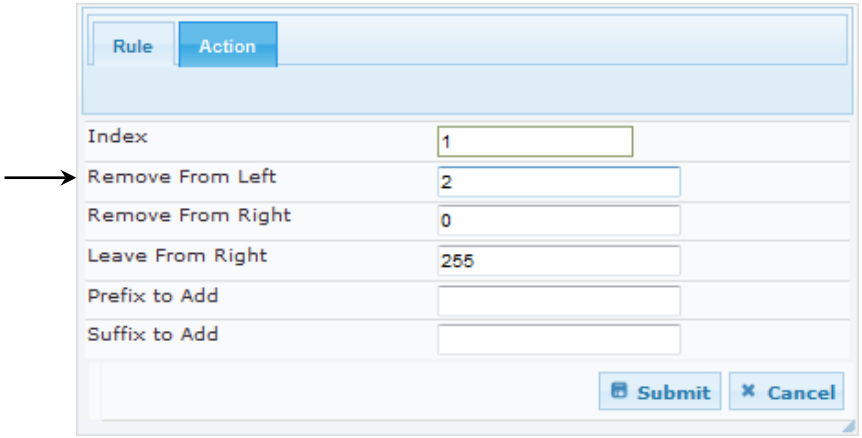
Figure 4-42: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Remove from Left	**2**

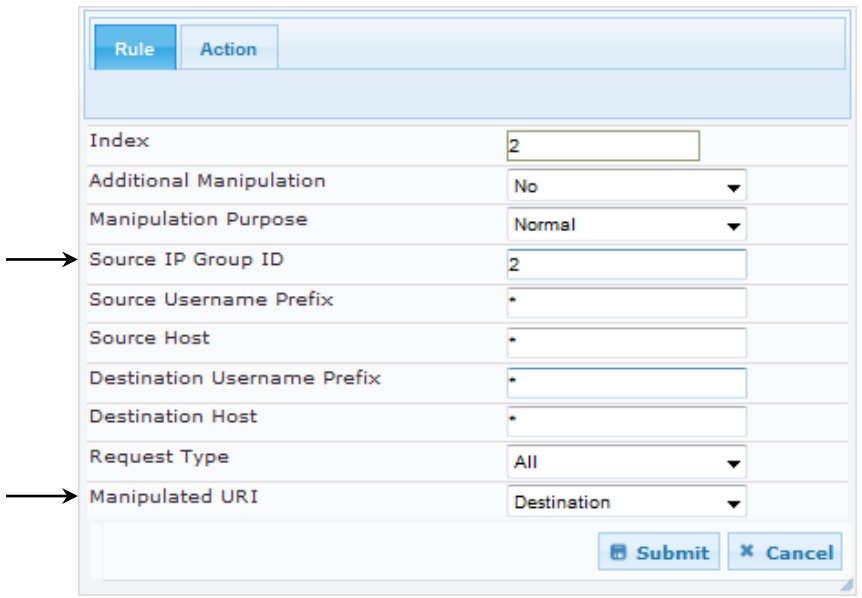
Figure 4-43: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



5. Click **Submit**.
6. Click **Add**.
7. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Settings
Index	**2**
Source IP Group ID	**2**
Manipulated URI	**Destination**

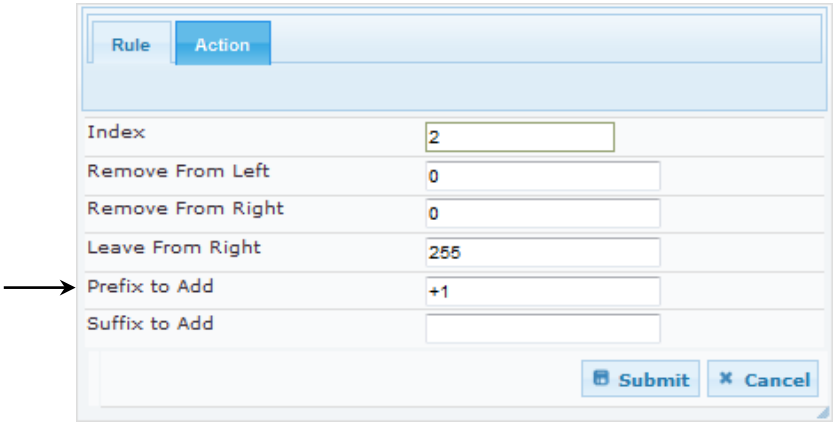
Figure 4-44: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Prefix to Add	**+1**

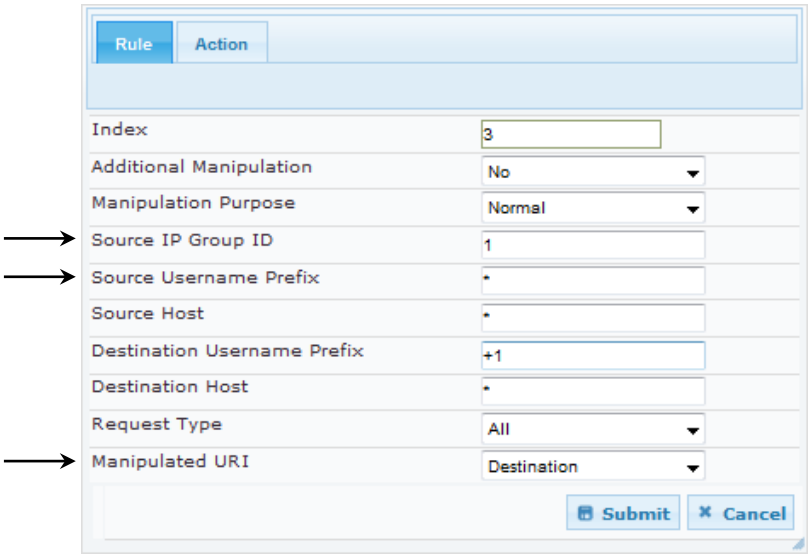
Figure 4-45: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



9. Click **Submit**.
10. Click **Add**.
11. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Settings
Index	**3**
Source IP Group ID	**1**
Destination Username Prefix	**+1**
Manipulated URI	**Destination**

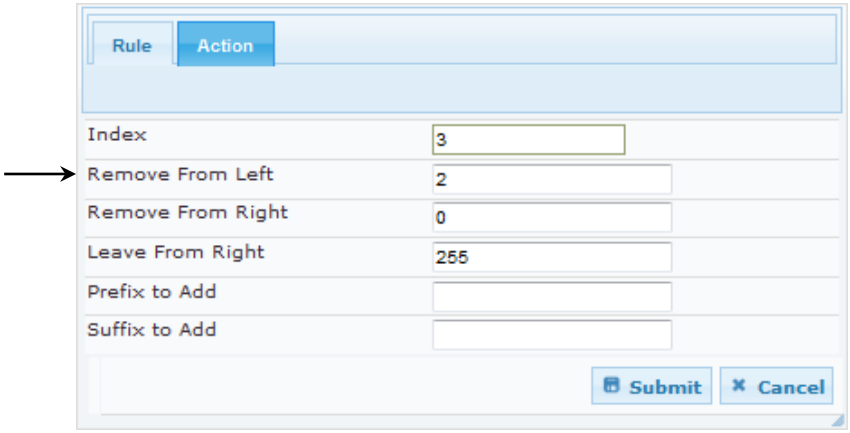
Figure 4-46: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Remove From Left	**2**

Figure 4-47: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



13. Click **Submit**.

The IP to IP Inbound table displayed below includes manipulation rules for calls between IP Group 1 (i.e., Lync Server 2013) and IP Group 2 (i.e., AT&T IP Flexible Reach - EF service):

Figure 4-48: Configuring IP to IP Inbound Manipulation Rules

Rule Index	Description
1	Calls received from IP Group 1 with source number prefix of "+1", remove the "+1" from this prefix source number.
2	Calls received from IP Group 2 that have any destination number (*), add "+1" to the prefix of the destination number.
3	Calls received from IP Group 1 that have a prefix destination number of "+1", remove "+1" from this prefix.

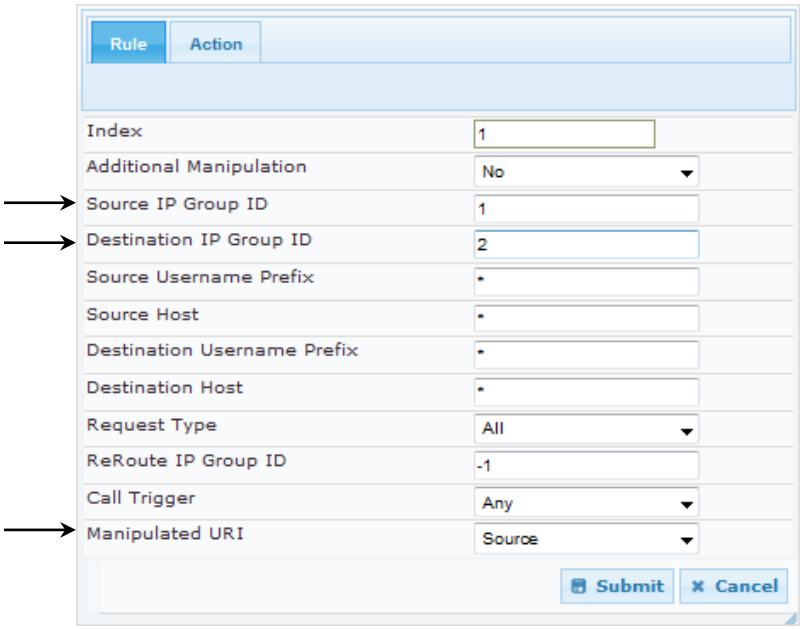
The procedure below provides an example of configuring a manipulation rule that adds the plus "+1" to the destination number for calls from IP Group 2 (AT&T IP Flexible Reach - EF service) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number ("*").

➢ **To configure a number manipulation rule:**

1. Open the IP to IP Outbound Manipulation page (**Configuration** > **VoIP** > **SBC** > **Manipulation SBC** > **IP to IP Outbound**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Settings
Index	**1**
Source IP Group	**1**
Destination IP Group	**2**
Manipulated URI	**Source**

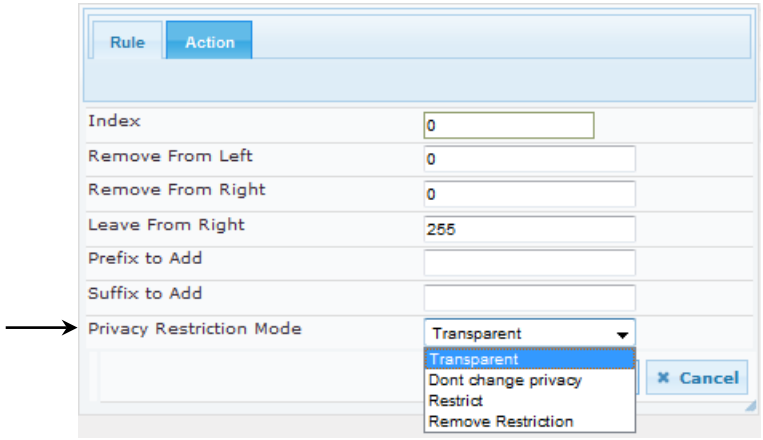
Figure 4-49: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Privacy Restriction Mode	**Transparent**, **Restrict** or **Remove Restriction**

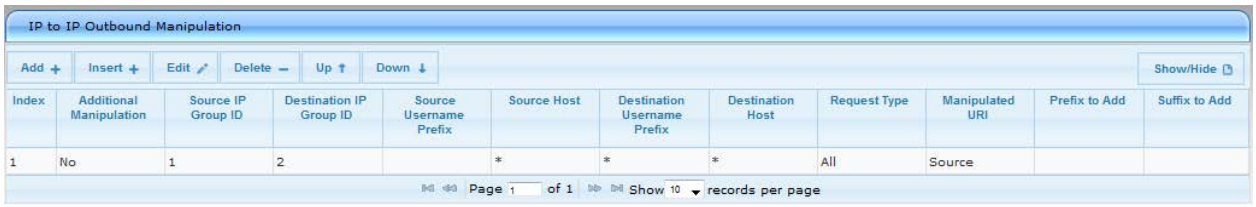
Figure 4-50: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

The IP to IP Outbound table displayed below includes a manipulation rule for calls between IP Group 1 (i.e., Lync Server 2013) and IP Group 2 (i.e., AT&T IP Flexible Reach - EF service):

Figure 4-51: Configuring IP to IP Outbound Manipulation Rules



Rule Index	Description
1	Calls received from IP Group 1 with a destination of IP Group 2 manipulate the Privacy Restriction Mode. This example would apply to all source numbers but may be refined to reflect a specific DID. See User's Manual for further details.

4.13 Step 13: Configure SIP Message Manipulation Rules

This step describes how to configure SIP message manipulation rules (done in the Message Manipulations table). SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

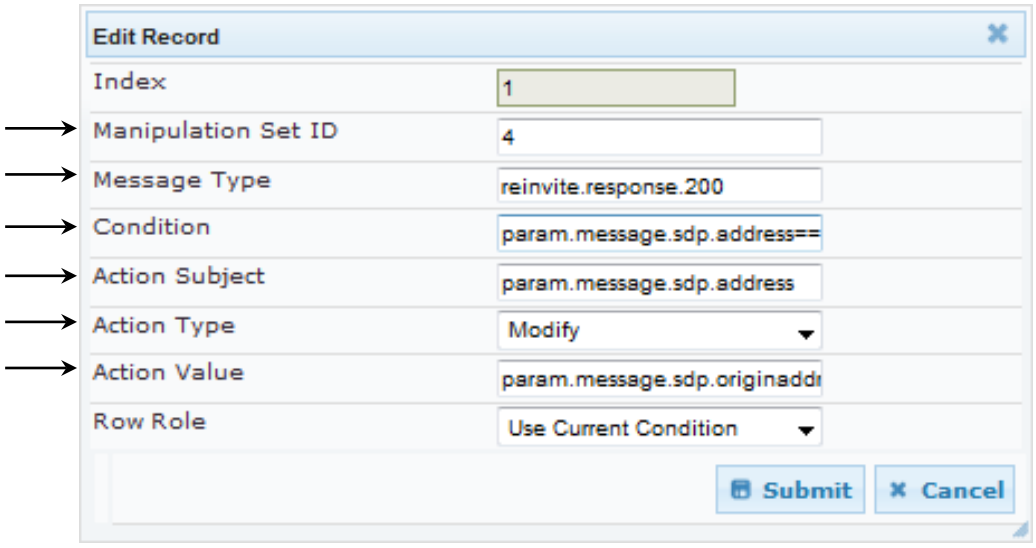
In our example scenario we set a manipulation for SIP 200OK response for Re-INVITE that in the SDP the IP address is '0.0.0.0' (hold) the manipulation change the IP address to the SBC IP address.

➢ **To configure SIP message manipulation rules for Index 1:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 4:

Rule Index	Setting
Index	**1**
Manipulation Set ID	**4**
Message Type	**reinvite.response.200**
Condition	**param.message.sdp.address=='0.0.0.0'**
Action Subject	**param.message.sdp.address**
Action Type	**Modify**
Action Value	**param.message.sdp.originaddress**

Figure 4-52: Configuring SIP Message Manipulation – Index 1

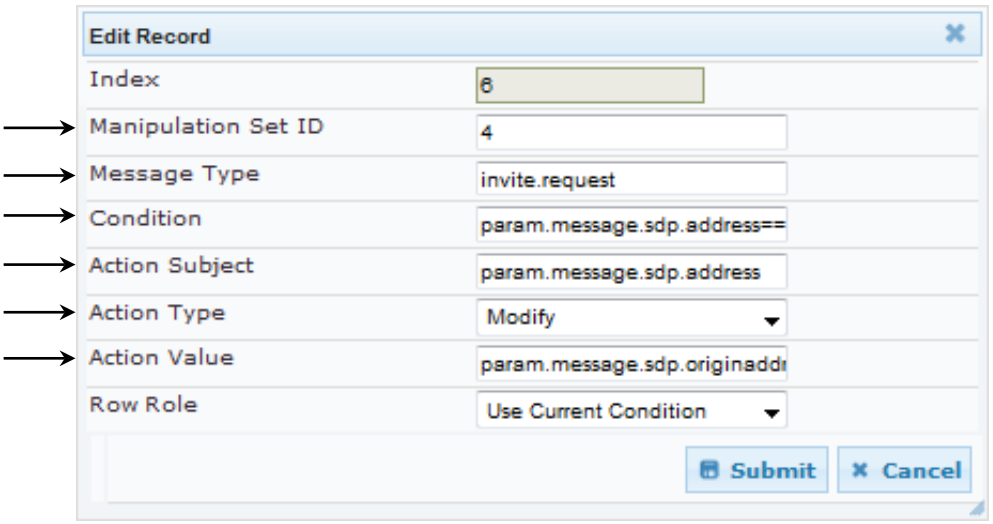


➢ **To configure SIP message manipulation rules for Index 6:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 4:

Rule Index	Setting
Index	**6**
Manipulation Set ID	**4**
Message Type	**invite.request**
Condition	**param.message.sdp.address=='0.0.0.0'**
Action Subject	**param.message.sdp.address**
Action Type	**Modify**
Action Value	**param.message.sdp.originaddress**

Figure 4-53: Configuring SIP Message Manipulation – Index 6

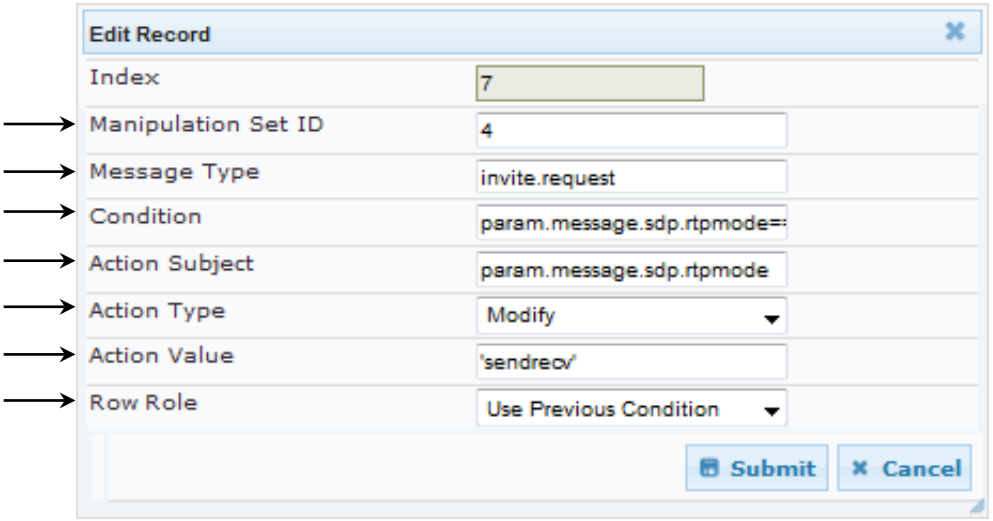


➢ **To configure SIP message manipulation rules for Index 7:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 4:

Rule Index	Setting
Index	**7**
Manipulation Set ID	**4**
Message Type	**invite.request**
Condition	**param.message.sdp.rtpmode=='inactive'**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**'sendrecv'**
Row Role	**Use Previous Condition**

Figure 4-54: Configuring SIP Message Manipulation – Index 7

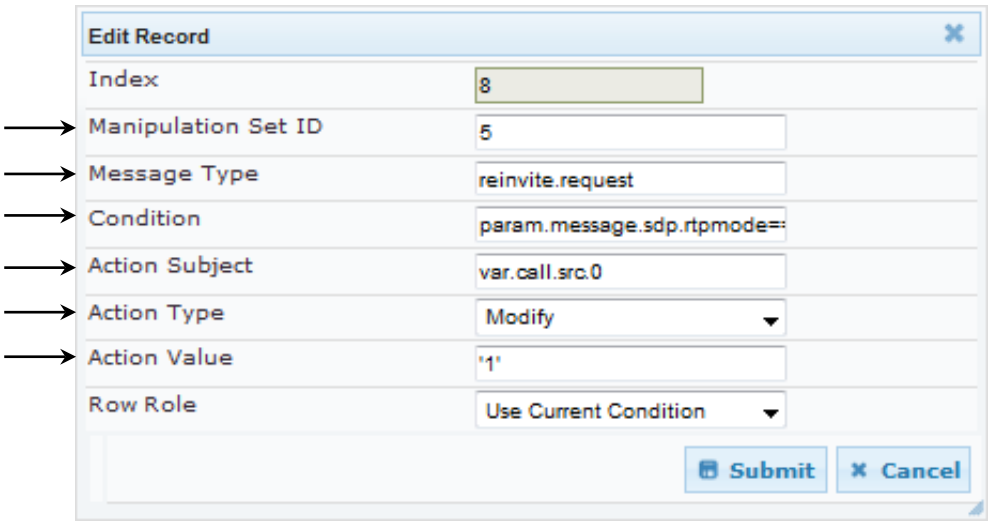


➢ **To configure SIP message manipulation rule for Index 8:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 5:

Rule Index	Setting
Index	**8**
Manipulation Set ID	**5**
Message Type	**reinvite.request**
Condition	**param.message.sdp.rtpmode=='sendonly'**
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'1'**

Figure 4-55: Configuring SIP Message Manipulation – Index 8

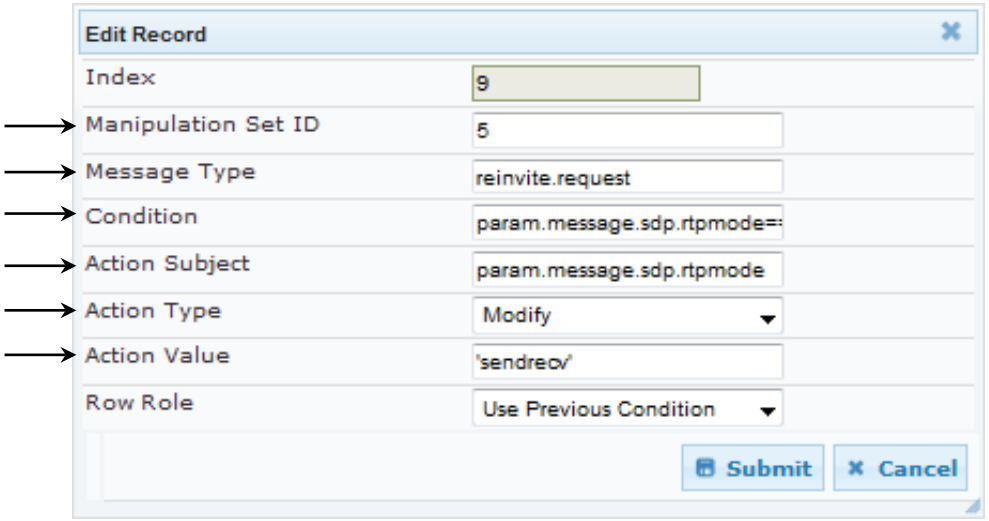


➢ **To configure SIP message manipulation rule for Index 9:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 5:

Rule Index	Setting
Index	**9**
Manipulation Set ID	**5**
Message Type	**reinvite.request**
Condition	**param.message.sdp.rtpmode=='sendonly'**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**'sendrecv'**
Row Role	**Use Previous Condition**

Figure 4-56: Configuring SIP Message Manipulation – Index 9

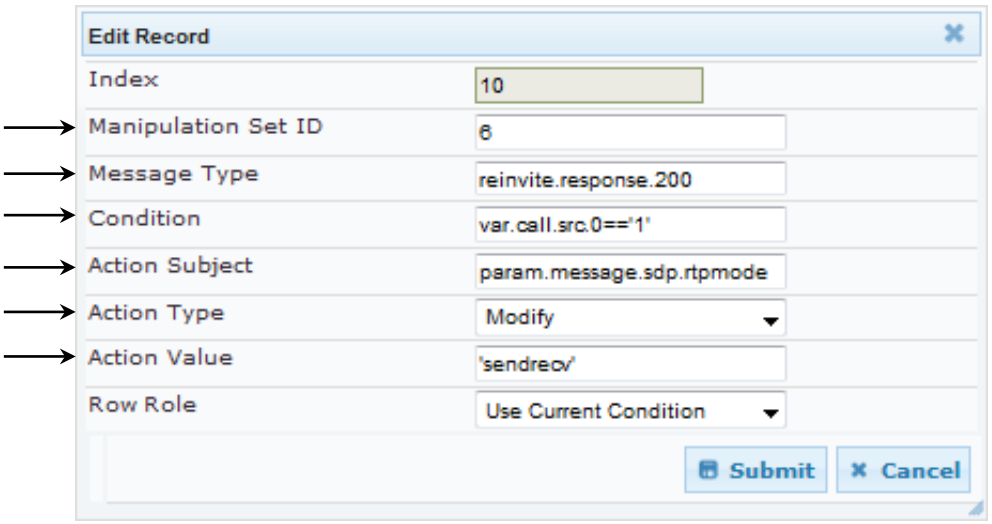


➢ **To configure SIP message manipulation rules for Index 10:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 6:

Rule Index	Setting
Index	**10**
Manipulation Set ID	**6**
Message Type	**reinvite.response.200**
Condition	**var.call.src.0=='1'**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**'sendrecv'**

Figure 4-57: Configuring SIP Message Manipulation – Index 10

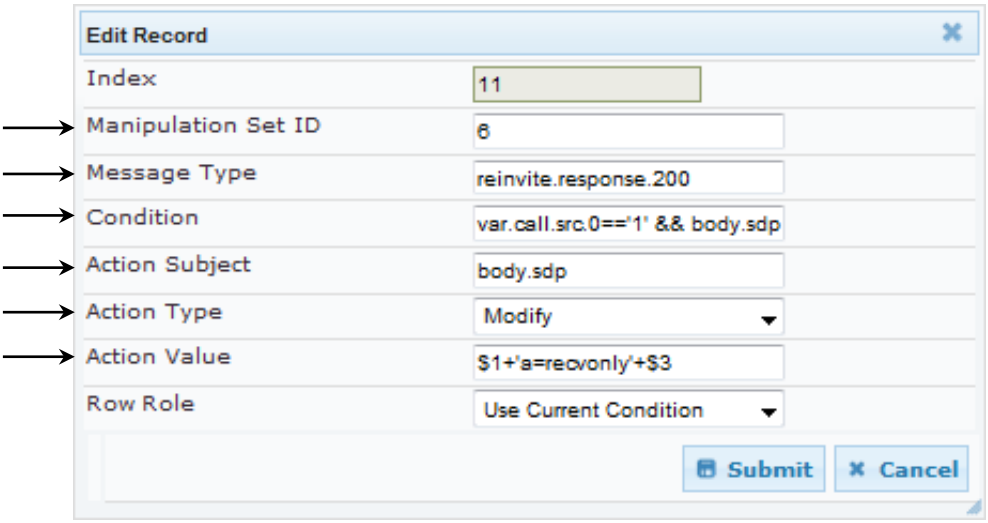


➢ **To configure SIP message manipulation rule for Index 11:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 6:

Rule Index	Setting
Index	**11**
Manipulation Set ID	**6**
Message Type	**reinvite.response.200**
Condition	**var.call.src.0=='1' && body.sdp regex (.*)(a=sendrecv)(.*)**
Action Subject	**body.sdp**
Action Type	**Modify**
Action Value	**$1+'a=recvonly'+$3**

Figure 4-58: Configuring SIP Message Manipulation – Index 11

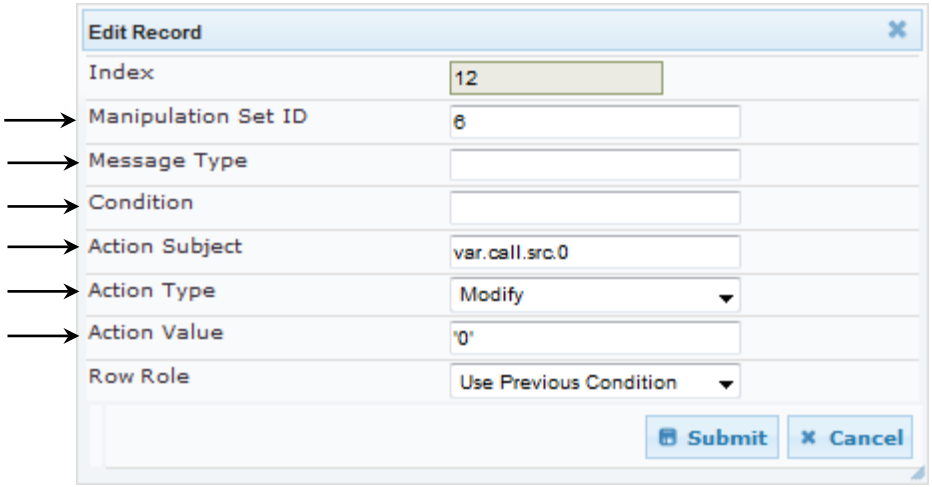


➢ **To configure SIP message manipulation rules for Index 12:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 6:

Rule Index	Setting
Index	**12**
Manipulation Set ID	**6**
Message Type	
Condition	
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'0'**
Row Role	**Use Previous Condition**

Figure 4-59: Configuring SIP Message Manipulation – Index 12

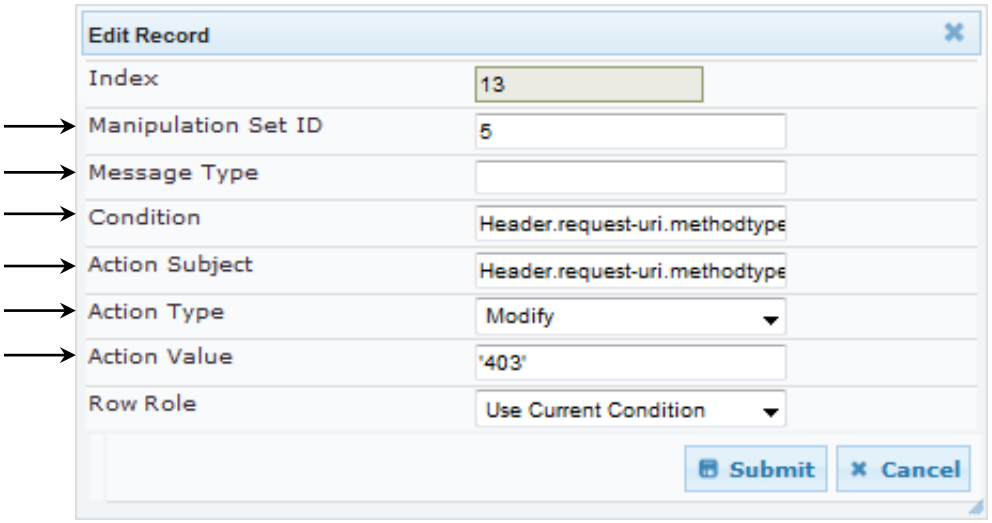


➢ **To configure SIP message manipulation rule for Index 13:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 5:

Rule Index	Setting
Index	**13**
Manipulation Set ID	**5**
Message Type	
Condition	**Header.request-uri.methodtype == '487'**
Action Subject	**Header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'403'**

Figure 4-60: Configuring SIP Message Manipulation – Index 13

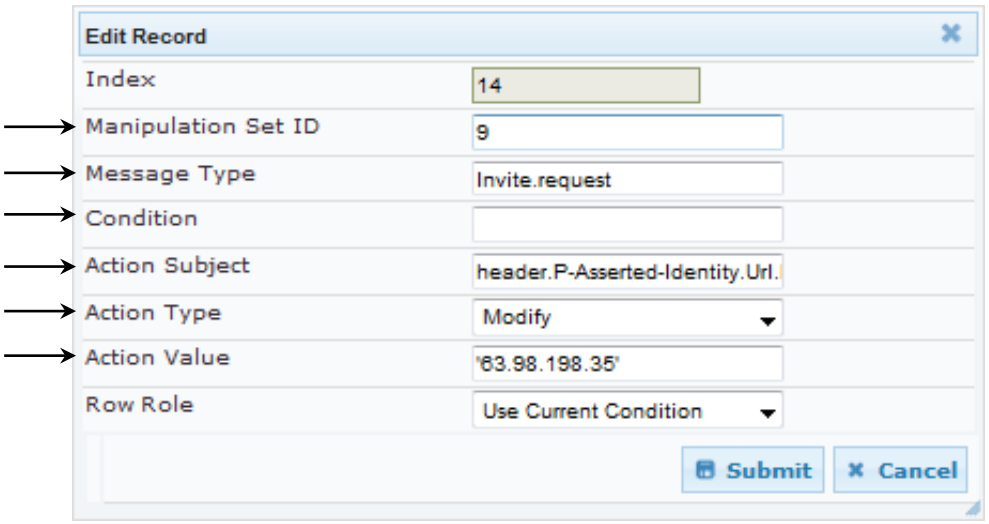


➢ **To configure SIP message manipulation rule for Index 14:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 9:

Rule Index	Setting
Index	**14**
Manipulation Set ID	**9**
Message Type	**Invite.request**
Condition	
Action Subject	**header.P-Asserted-Identity.Url.Host**
Action Type	**Modify**
Action Value	**'63.98.198.35'**

Figure 4-61: Configuring SIP Message Manipulation – Index 14

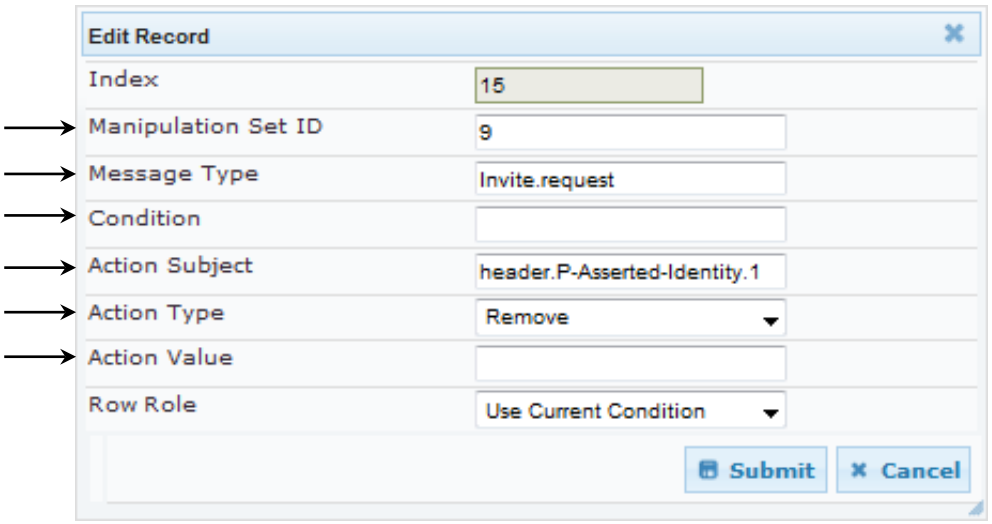


➢ **To configure SIP message manipulation rule for Index 15:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 9:

Rule Index	Setting
Index	**15**
Manipulation Set ID	**9**
Message Type	**Invite.request**
Condition	
Action Subject	**header.P-Asserted-Identity.1**
Action Type	**Remove**
Action Value	

Figure 4-62: Configuring SIP Message Manipulation – Index 15

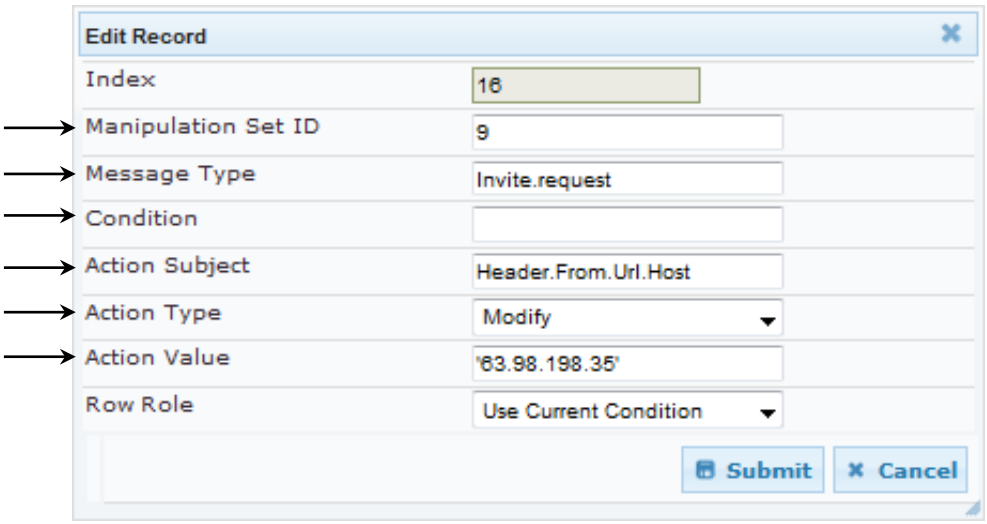


➢ **To configure SIP message manipulation rule for Index 16:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 9:

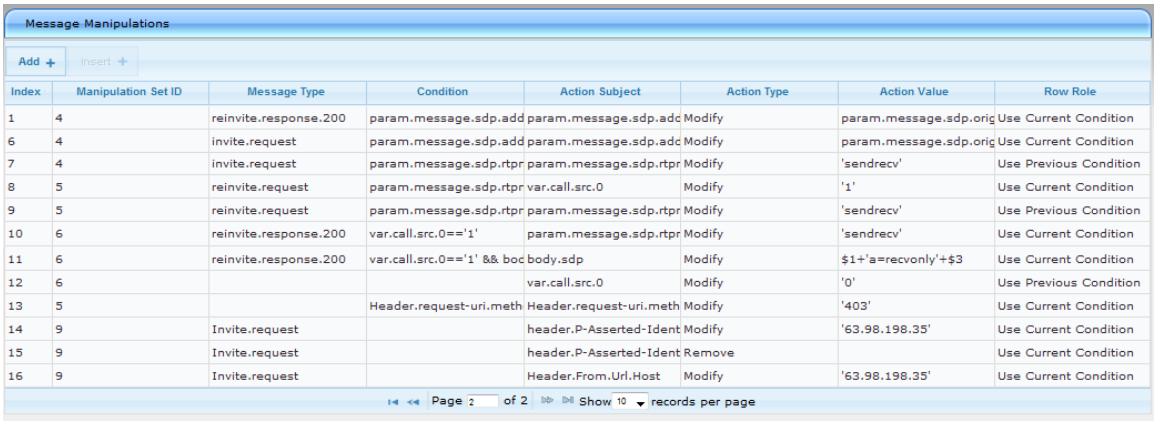
Rule Index	Setting
Index	**16**
Manipulation Set ID	**9**
Message Type	**Invite.request**
Condition	
Action Subject	**Header.From.Url.Host**
Action Type	**Modify**
Action Value	**'63.98.198.35'**

Figure 4-63: Configuring SIP Message Manipulation – Index 16



The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set IDs 4, 5, 6, and 9) which are executed for messages sent to and from the AT&T IP Flexible Reach - EF service (IP Group 2) as well as the Lync Server 2013 (IP Group 1). These rules within the Manipulation Set IDs can be further enhanced by linking interdependencies via the Row Role setting for each rule. Some of the items are dependent or related to the deployment (rules 14 and 16) while others are specifically required to enable proper interworking between AT&T IP Flexible Reach - EF service and Lync Server 2013 (rules 1, 6, 7, 8, 9, 10, 11, 12, 13, and 15). There are some that also show specific interworking linkage which must be performed in the specific order as well (rule 6 must be performed and true prior to rule 7, Rule 9 is dependent on rule 8, and rule 12 is dependent on rule 11). The specific items are needed to support simultaneous ring feature, Music on Hold, proper P-Asserted Identity header, and Host URL presentation. See User's Manual for further details concerning the full capabilities of header manipulation. The Manipulation Set IDs are indexed and utilized from within the IP Group table.

Figure 4-64: Configuring SIP Message Manipulation – Example

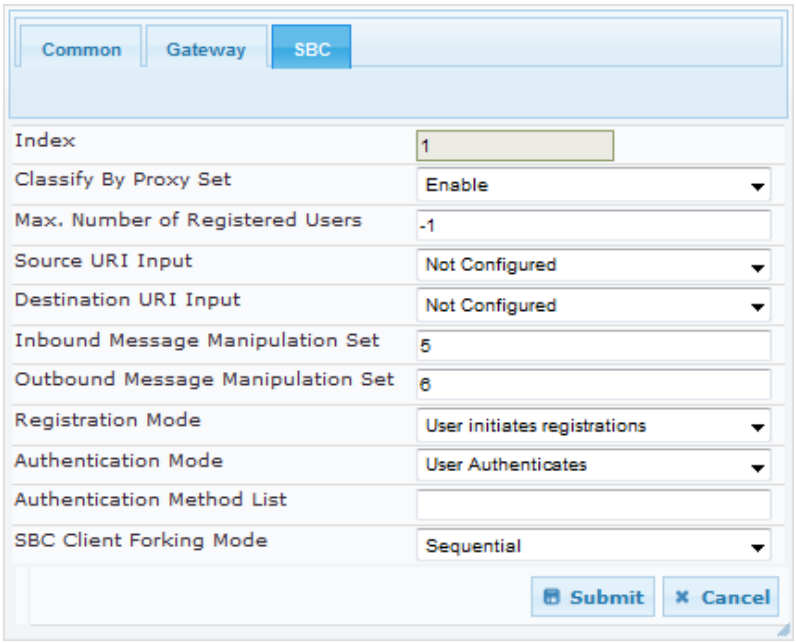


Rule Index	Description
1	SIP 200OK response that contains '0.0.0.0' (hold) in the SDP IP address. It changes the IP address to the SBC IP address.
6	SIP INVITE Request that contains '0.0.0.0' (simultaneous ring) in the SDP IP address. It changes the IP address to the SBC IP address.
7	If the manipulation rule Index 6 (above) is executed, then the following rule is also done on the same SIP message: if the RTP mode within the SDP is set to "inactive" change it to "sendrcv"
8	SIP re-INVITE Request that contains within the SDP, an RTP mode that is set to "sendonly" (MS Lync initiated Hold), creates a variable and sets it to "1". This manages the call process handling for the state of the call.
9	If the manipulation rule Index 8 (above) is executed, then the following rule is also executed on the same SIP message: if the RTP mode within the SDP is set to "sendonly" change it to "sendrcv"
10	A SIP re-INVITE Response while the current call state has a variable set to "1", sets within the SDP, an RTP mode of "sendrecv" (response from AT&T to MS Lync initiated Hold attempt).
11	SIP re-INVITE Response while the current call state for the call has variable set to "1" and within the SDP an RTP mode of "sendrecv" (response from AT&T to MS Lync initiated Hold attempt). It sets within the SDP, an RTP mode of "recvonly" (response from AT&T to MS Lync initiated Hold attempt to normalize call processing state back to MS Lync for the proper reply to the initially received "sendonly").
12	If the manipulation rule Index 12 (above) is executed, then the following rule is also executed. It checks the variable for its current state. If the variable is found to be set to "1" it then sets it to "0" to manage the call process handling for the state of the call. The call is now truly on hold and can support Music on Hold.
13	SIP message type "487" is received during initial call setup as related to a Cancel. The method type will be changed to a '403' prior to delivery of the message to AT&T services to enable interworking with some of the Enhanced IP Flexible Reach features.

14	SIP INVITE Request is received from MS Lync 2013 and has the P-Asserted Identity header modified to reflect the IP address of the SBC prior to delivery to AT&T IP Flexible Reach - EF service. This will be unique to each deployment.
15	SIP INVITE Request is received from MS Lync 2013 and has the second P-Asserted Identity header removed prior to delivery to AT&T IP Flexible Reach - EF service. The original header is broken into two headers and the second portion is removed
16	SIP INVITE Request is received from MS Lync 2013 and has the From header modified to reflect the IP address of the SBC prior to delivery to AT&T IP Flexible Reach - EF service. This will be unique to each deployment.

3. Assign the Manipulation Set IDs 5 and 6 to IP Group 1:
   a. Open the IP Group Table page (**Configuration** > **VoIP** > **Control Network** > **IP Group Table**).
   b. Select the row of IP Group 1, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Inbound Message Manipulation Set' field to "5".
   e. Set the 'Outbound Message Manipulation Set' field to "6".

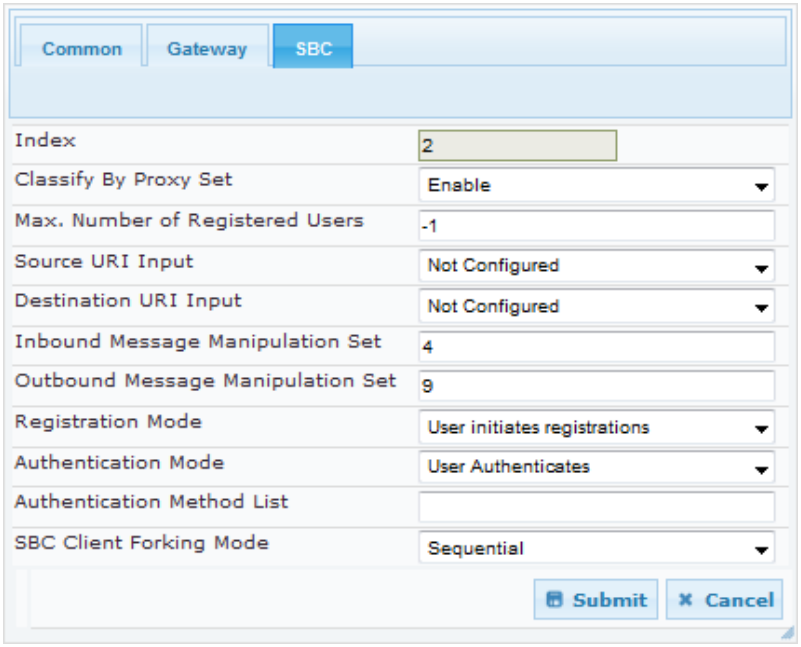
Figure 4-65: Assigning Manipulation Rule to IP Group 1



   f. Click **Submit**.

4. Assign the Manipulation Set ID 4 and 9 to IP Group 2:
   a. Open the IP Group Table page (**Configuration** > **VoIP** > **Control Network** > **IP Group Table**).
   b. Select the row of IP Group 2, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Inbound Message Manipulation Set' field to "4".
   e. Set the 'Outbound Message Manipulation Set' field to "9".

Figure 4-66: Assigning Manipulation Rule to IP Group 2



f. Click **Submit**.

4.14 Step 15: Miscellaneous Configuration

This step describes miscellaneous E-SBC configuration.

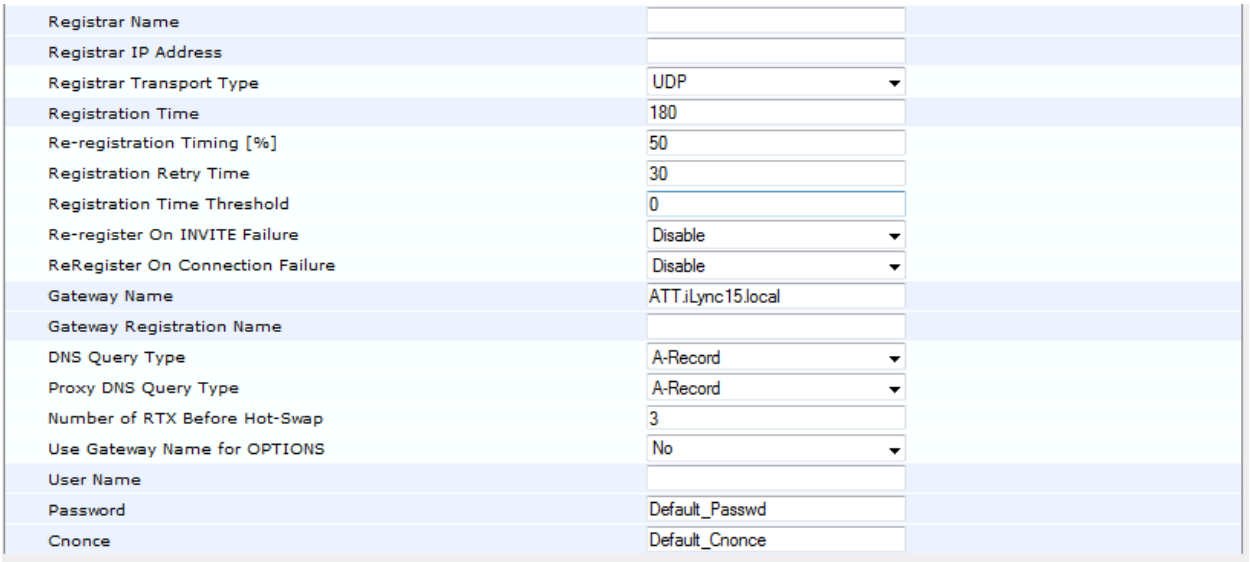
4.14.1 Step 15a: Configure DNS Query Methods

This step describes how to configure DNS query modes. The example lab configuration utilized an A-Record-based DNS query for FQDN resolution to the proper IP address for the Proxy Set (i.e., Lync Server 2013). Set this according to the deployment requirements. The settings shown are the default settings.

➢ **To configure DNS query methods:**

1. Open the Advance Parameters page (**Configuration** > **VoIP** > **SIP Definitions** > **Proxy & Registration**).
2. From the 'DNS Query Type' drop-down list, select **A-Record**.
3. From the 'Proxy DNS Query Type' drop-down list, select **A-Record**.

Figure 4-67: Configuring DNS Query Methods



4. Click **Submit**.

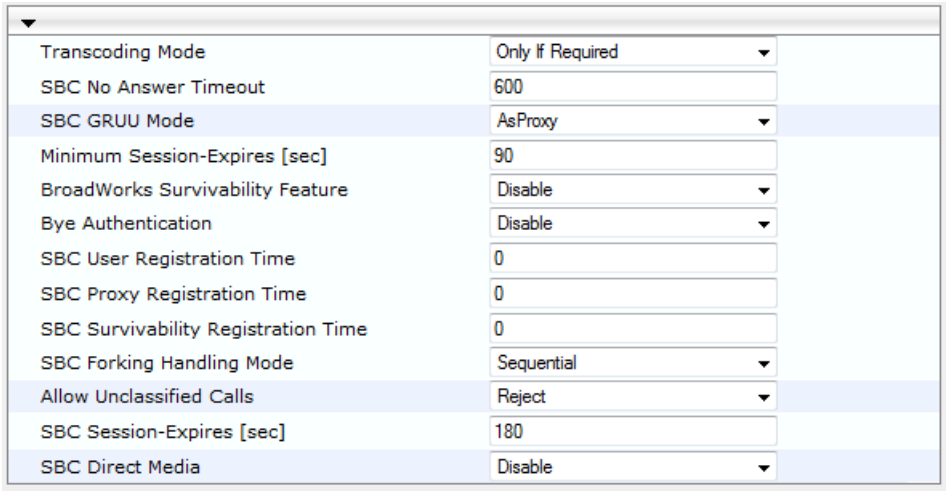
4.14.2 Step 15b: Configure Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received due to call forking of an INVITE. In our example scenario, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC reopens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if 180 response without SDP is received. It's mandatory to set this field for the Lync Server 2013 environment.

➢ **To configure call forking:**

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

Figure 4-68: Configuring Forking Mode



3. Click **Submit**.

4.14.3 Step 15c: Configure SRTP Behavior upon Rekey Mode

This step describes how to configure SRTP Behavior upon Rekey mode.

➢ **To configure SRTP Behavior upon Rekey Mode:**

1. Open the Admin page: append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.133.4.100/AdminPage).
2. In the left pane, click ***ini* Parameters**.

Figure 4-69: Configuring SRTP Behavior upon Rekey Mode

3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
RESETSRTPSTATEUPONREKEY	**1** Enables Reset SRTP State Upon Re-key.
SBCMAXFORWARDSLIMIT	**70** Enables compatibility with the offering from Lync Server 2013.

4. Click the **Apply New Value** button for each field to take effect.

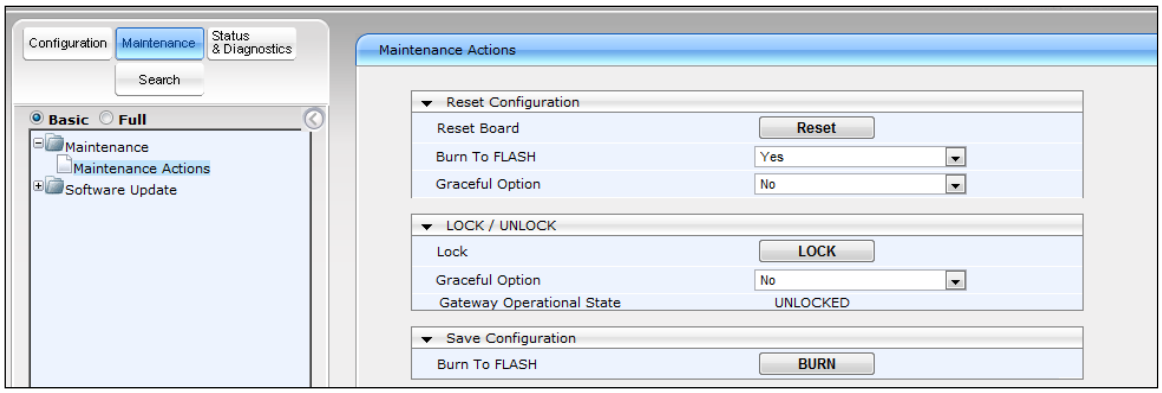
4.15 Step 16: Reset the E-SBC

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

➢ **To reset the E-SBC:**

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

Figure 4-70: Resetting the E-SBC



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

Reader's Notes

A AudioCodes INI File

The *ini* file configuration of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 39, is shown below:

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

;Board: Mediant 1000
;Board Type: 47
;Serial Number: 2967088
;Slot Number: 1
;Software Version: 6.60A.031.014
;DSP Software Version: 620AE3 => 660.04
;Board IP Address: 63.98.198.35
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 63.98.198.33
;Ram size: 495M   Flash size: 64M
;Num of DSP Cores: 8  Num DSP Channels: 30
;Num of physical LAN ports: 7
;Profile: NONE
;Key features:;Board Type: Mediant 1000 ;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
;PSTN FALLBACK Supported ;E1Trunks=4 ;T1Trunks=4 ;DSP Voice
features: IpmDetector RTCP-XR ;DATA features: Eth-Port=6 ;IP
Media: Conf VoicePromptAnnounc(H248.9) TrunkTesting ;Channel Type:
RTP DspCh=30 IPMediaDspCh=30 ;PSTN Protocols: IUA=4 ;Security:
IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;Control Protocols: MSFT CLI TRANSCODING=20 TestCall=10 MGCP
MEGACO H323 SIP TPNCP SASurvivability SBC=120 ;Default
features:;Coders: G711 G726;

;--------- Mediant-1000 HW components ---------
;
; Slot # : Module type : # of ports : # of DSPs
;----------------------------------------------
;      1 : Empty
;      2 : FALC56      :          1 :         2
;      3 : Empty
;      4 : Empty
;      5 : Empty
;      6 : Empty
;----------------------------------------------


[SYSTEM Params]



[BSP Params]
```

```
PCMLawSelect = 3
BaseUDPPort = 16400

[Analog Params]


[ControlProtocols Params]

RTCPInterval = 5000




[Voice Engine Params]

CallerIDType = 0
FaxModemBypassCoderType = 1
CNGDetectorMode = 0
DisableRTCPRandomize = 1
EnableDSPIPMDetectors = 1
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'


[SIP Params]

MEDIACHANNELS = 20
ISREGISTERNEEDED = 1
SIPDESTINATIONPORT = 5067
PLAYRBTONE2TEL = 3
GWDEBUGLEVEL = 5
ENABLEEARLYMEDIA = 1
SIPGATEWAYNAME = 'ATT.iLync15.local'
PROXYREDUNDANCYMODE = 1
DISCONNECTONBROKENCONNECTION = 0
ISFAXUSED = 2
SIPTRANSPORTTYPE = 2
TCPLOCALSIPPORT = 5068
TLSLOCALSIPPORT = 5067
MEDIASECURITYBEHAVIOUR = 3
MULTIPTIMEFORMAT = 1
COMFORTNOISENEGOTIATION = 0
REDUNDANTROUTINGMODE = 2
ENABLESBCAPPLICATION = 1
ENABLESINGLEDSPTRANSCODING = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLEEARLY183 = 1
SBCMAXFORWARDSLIMIT = 70
ENABLESYMMETRICMKI = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
```

```
SBCSESSIONEXPIRES = 3600
RESETSRTPSTATEUPONREKEY = 1

[SCTP Params]


[VXML 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_0_1", 1, 1, 4, "User Port #0",
"GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 1, 4, "User Port #1",
"GROUP_1", "Redundant";
PhysicalPortsTable 2 = "GE_7_1", 1, 2, 4, "User Port #2",
"GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_7_2", 1, 2, 4, "User Port #3",
"GROUP_2", "Redundant";
PhysicalPortsTable 4 = "GE_7_3", 1, 3, 4, "User Port #4",
"GROUP_3", "Active";
PhysicalPortsTable 5 = "GE_7_4", 1, 3, 4, "User Port #5",
"GROUP_3", "Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1,
EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, GE_0_1, GE_0_2;
EtherGroupTable 1 = "GROUP_2", 2, GE_7_1, GE_7_2;
EtherGroupTable 2 = "GROUP_3", 2, GE_7_3, GE_7_4;

[ \EtherGroupTable ]
```

```
[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 5, 10, 10.133.4.100, 16, 10.133.4.1, 1,
"Voice", 10.15.25.1, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 6, 10, 63.98.198.35, 16, 63.98.198.33, 2,
"Public", 0.0.0.0, 0.0.0.0, GROUP_2;

[ \InterfaceTable ]


[ 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 1 = "MRLan", Voice, , 16500, 10, 16590, 1;
CpMediaRealm 2 = "MRwan", Public, , 16400, 10, 16490, 0;

[ \CpMediaRealm ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm,
SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers,
SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "LanSRD", "MRLan", 0, 0, -1, 1;
SRD 2 = "WanSRD", "MRwan", 0, 0, -1, 1;

[ \SRD ]
```

```
[ ProxyIp ]

; ** NOTE: Changes were made to active configuration.
; **       The data below is different from current values.
FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE15.iLync15.local", 2, 1;
ProxyIp 1 = "207.242.225.210:5060", 0, 2;
ProxyIp 2 = "10.133.4.101:5060", 0, 3;

[ \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_SBCAllowedCodersGroupID, 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 1 = "corp_lan_2013", 1, 2, 2, 10, 10, 46, 40, 0, 0, 0,
0, 2, 0, 0, 0, 1, -1, 1, 0, 3, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0,
```

```
1, 1, 2, 1, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0,
1, 1, 0, 3, 2, 1, 2, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, -1, 0;
IpProfile 2 = "ATT_E_IPFR", 1, 1, 2, 10, 10, 46, 40, 0, 0, 0, 0,
2, 0, 0, 0, 1, -1, 1, 0, 2, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0, 0,
0, 2, 2, 0, 0, 0, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 0, 2,
1, 0, 3, 0, 1, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0;
IpProfile 3 = "fax test", 1, 2, 2, 10, 10, 46, 40, 0, 0, 0, 0, 2,
0, 0, 0, 1, -1, 1, 0, 3, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, 1,
2, 2, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2,
1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, -1, 0;

[ \IpProfile ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode;
ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;
ProxySet 1 = 1, 30, 0, 1, 1, 0, -1;
ProxySet 2 = 1, 20, 0, 0, 2, 0, -1;
ProxySet 3 = 1, 60, 0, 0, 1, 0, -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 1 = 0, "CorpLabW15", 1, "FE15.iLync15.local", "", 0, -1, -
1, 0, -1, 1, "MRLan", 1, 1, -1, 5, 6, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "ATT_E_IPFR", 2, "207.242.225.210", "", 0, -1, -1,
0, -1, 2, "MRwan", 1, 2, -1, 4, 9, 0, 0, "", 0, -1, -1, "";
IPGroup 3 = 0, "FAX", 3, "Faxtester", "", 0, -1, -1, 0, -1, 1,
"MRLan", 1, 3, -1, -1, -1, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
```

```
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress,
IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,
IP2IPRouting_AltRouteOptions, IP2IPRouting_CostGroup;
IP2IPRouting 0 = 2, "*", "*", "*", "*", 6, , -1, 0, 1, -1, ,
"Internal", 0, -1, 0, ;
IP2IPRouting 1 = 1, "*", "*", "*", "*", 6, , -1, 0, 1, -1, ,
"Internal", 0, -1, 0, ;
IP2IPRouting 2 = 3, "*", "*", "*", "*", 6, , -1, 0, 1, -1, ,
"Internal", 0, -1, 0, ;
IP2IPRouting 4 = 1, "*", "*", "*", "*", 0, , -1, 0, 0, 2, , "", 0,
-1, 0, ;
IP2IPRouting 5 = 2, "*", "*", "7323204036", "*", 0, , -1, 0, 0, 3,
, "", 0, -1, 0, ;
IP2IPRouting 6 = 2, "*", "*", "*", "*", 0, , -1, 0, 0, 1, , "", 0,
-1, 0, ;
IP2IPRouting 8 = 3, "*", "*", "*", "*", 0, , -1, 0, 0, 2, , "", 0,
-1, 0, ;

[ \IP2IPRouting ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort,
SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD,
SIPInterface_MessagePolicy, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 0 = "Voice", 2, 5060, 5068, 5067, 1, , -1, 0, 500;
SIPInterface 1 = "Public", 2, 5060, 5060, 5061, 2, , -1, 0, 500;

[ \SIPInterface ]


[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index =
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix,
IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix,
IPInboundManipulation_DestHost, IPInboundManipulation_RequestType,
IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight,
IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
```

```
IPInboundManipulation 1 = 0, 0, 1, "+1", "*", "*", "*", 0, 0, 2,
0, 255, "", "";
IPInboundManipulation 2 = 0, 0, 2, "*", "*", "*", "*", 0, 1, 0, 0,
255, "+1", "";
IPInboundManipulation 3 = 0, 0, 1, "*", "*", "+1", "*", 0, 1, 2,
0, 255, "", "";

[ \IPInboundManipulation ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix,
IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID,
IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight,
IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 1 = 0, 1, 2, "", "*", "*", "*", 0, -1, 0,
0, 0, 0, 255, "", "", 3;

[ \IPOutboundManipulation ]




[ CodersGroup1 ]

; ** NOTE: Changes were made to active configuration.
; **       The data below is different from current values.
FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = "g729", 20, 0, -1, 0;
CodersGroup1 1 = "g711Ulaw64k", 30, 0, -1, 0;

[ \CodersGroup1 ]


[ CodersGroup2 ]

; ** NOTE: Changes were made to active configuration.
; **       The data below is different from current values.
```

```
FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0;
CodersGroup2 1 = "g711Alaw64k", 20, 0, -1, 0;

[ \CodersGroup2 ]


[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g729";
AllowedCodersGroup0 1 = "g711Ulaw64k";

[ \AllowedCodersGroup0 ]


[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Ulaw64k";
AllowedCodersGroup1 1 = "g711Alaw64k";

[ \AllowedCodersGroup1 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 1 = 4, "reinvite.response.200",
"param.message.sdp.address=='0.0.0.0'",
"param.message.sdp.address", 2, "param.message.sdp.originaddress",
0;
MessageManipulations 6 = 4, "invite.request",
"param.message.sdp.address=='0.0.0.0'",
"param.message.sdp.address", 2, "param.message.sdp.originaddress",
0;
MessageManipulations 7 = 4, "invite.request",
"param.message.sdp.rtpmode=='inactive'",
"param.message.sdp.rtpmode", 2, "'sendrecv'", 1;
MessageManipulations 8 = 5, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2,
"'1'", 0;
MessageManipulations 9 = 5, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'",
"param.message.sdp.rtpmode", 2, "'sendrecv'", 1;
MessageManipulations 10 = 6, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2,
"'sendrecv'", 0;
```

```
MessageManipulations 11 = 6, "reinvite.response.200",
"var.call.src.0=='1' && body.sdp regex (.*)(a=sendrecv)(.*)",
"body.sdp", 2, "$1+'a=recvonly'+$3", 0;
MessageManipulations 12 = 6, "", "", "var.call.src.0", 2, "'0'",
1;
MessageManipulations 13 = 5, "", "Header.request-uri.methodtype ==
'487'", "Header.request-uri.methodtype", 2, "'403'", 0;
MessageManipulations 14 = 9, "Invite.request", "", "header.P-
Asserted-Identity.Url.Host", 2, "'63.98.198.35'", 0;
MessageManipulations 15 = 9, "Invite.request", "", "header.P-
Asserted-Identity.1", 1, "", 0;
MessageManipulations 16 = 9, "Invite.request", "",
"Header.From.Url.Host", 2, "'63.98.198.35'", 0;

[ \MessageManipulations ]


[ RoutingRuleGroups ]
```

B Configuring Analog Devices (ATA's)

This section describes how to configure the analog device entity to route its calls to the AudioCodes E-SBC. The analog device entity must be configured to send all calls to the E-SBC without any registration process.

Note: The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series, the FXS supported modules of the Mediant/E-SBC 1000 product line, as well as the integrated FXS interfaces of the Mediant/E-SBC 800 product line.

B.1 Step 1: Configure IP Address of the MP-11x

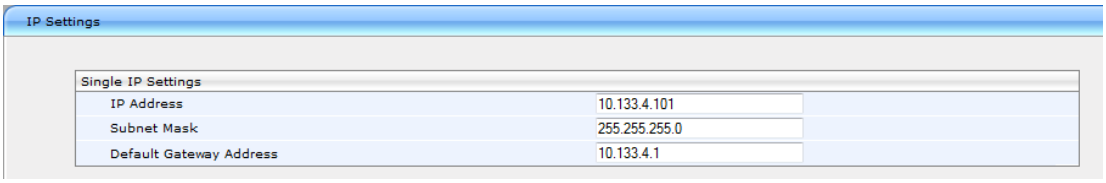
This step describes how to configure the IP address settings of the MP-11x. Refer to the Installation Manual for further details.

➢ **To configure IP Address of the MP-11x:**

- Open the 'IP Settings' page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).

  Make applicable changes for the IP address, Subnet Mask, and Default Gateway Address. See Installation Manual for detailed instructions.

Figure 4-71: Configuring IP Address of the MP-11x



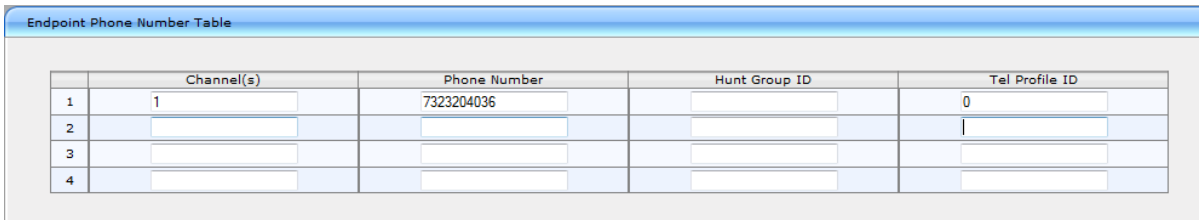
B.2 Step 2: Configure Endpoint Phone Numbers

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 "7323204036" (IP address 10.133.4.101) with all routing directed to the AudioCodes E-SBC (10.133.4.100).

➢ **To configure Endpoint Phone Numbers :**

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

Figure 4-72: Configuring Endpoint Phone Numbers



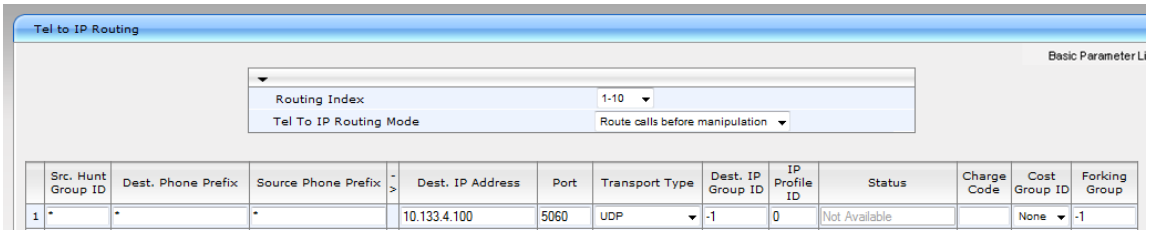
B.3 Step 3: Configure Tel-to-IP Routing Rules

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 centralized E-SBC device to be sent onwards to the AT&T IP Flexible Reach - EF service.

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

- Open the Tel to IP Routing page (**Configuration** tab > **VoIP** menu> **GW and IP 2 IP** > **Routing** > **Tel to IP Routing**).

Figure 4-73: Configuring Tel-to-IP Routing Rules



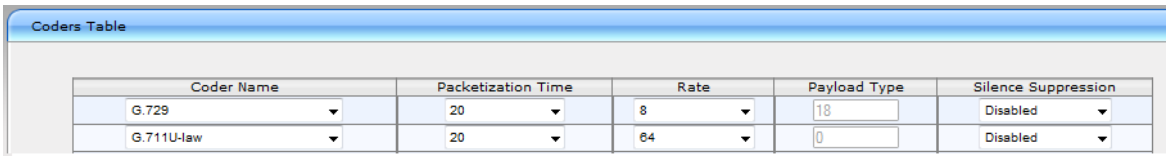
B.4 Step 4: Configure Coders for MP-11x

This step describes how to configure the coders for the MP-11x. Notice that the first choice is 'G.729'. Even though the device will be used exclusively for Fax support, the AT&T network must first see the originating attempt displayed as 'G.729'. Once the call is answered on the other side of the AT&T network, the infrastructure can then support the transition to T.38 support. This is a unique interworking caveat of AT&T.

➢ **To configure coders for MP-11x:**

- Open the 'Coders' page (**Configuration** tab > **VoIP** menu > **Coders and Profile Definition** > **Coders**).

Figure 4-74: Configuring Coders for MP-11x



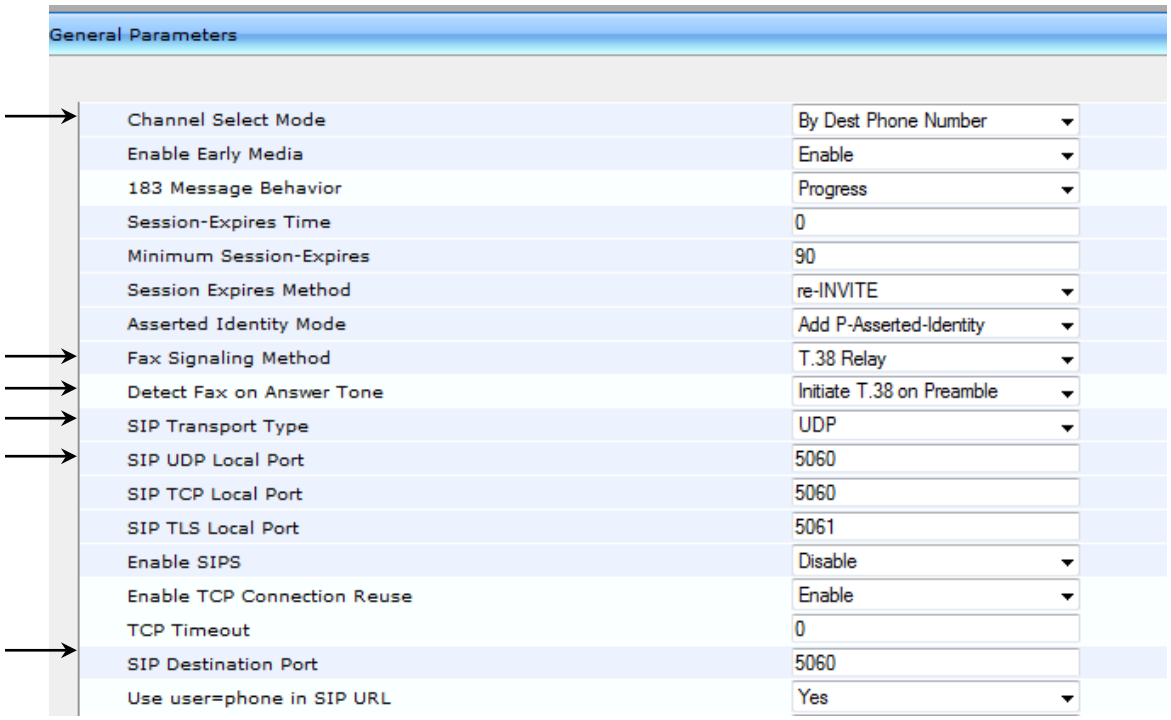
B.5 Step 5: Configure SIP UDP Transport Type and Fax Signaling Method

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

➢ **To configure SIP UDP Transport Type and fax signaling method:**

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

Figure 4-75: Configuring SIP UDP Transport Type and Fax Signaling Method



2. From the 'Channel Select Mode' drop-down list, select **By Dest Phone Number.**
3. From the 'Fax Signaling Method' drop-down list, select **T.38 Relay.**
4. From the 'Detect Fax on Answer Tone' drop-down list, select **Initiate T.38 Relay on Preamble.**
5. From the 'SIP Transport Type' drop-down list, select **UDP**.
6. In the 'SIP UDP Local Port' field, enter **5060** (corresponding to the Centralized E-SBC UDP transmitting port configuration).
7. In the 'SIP Destination Port', enter **5060** (corresponding to the Centralized E-SBC UDP listening port configuration).

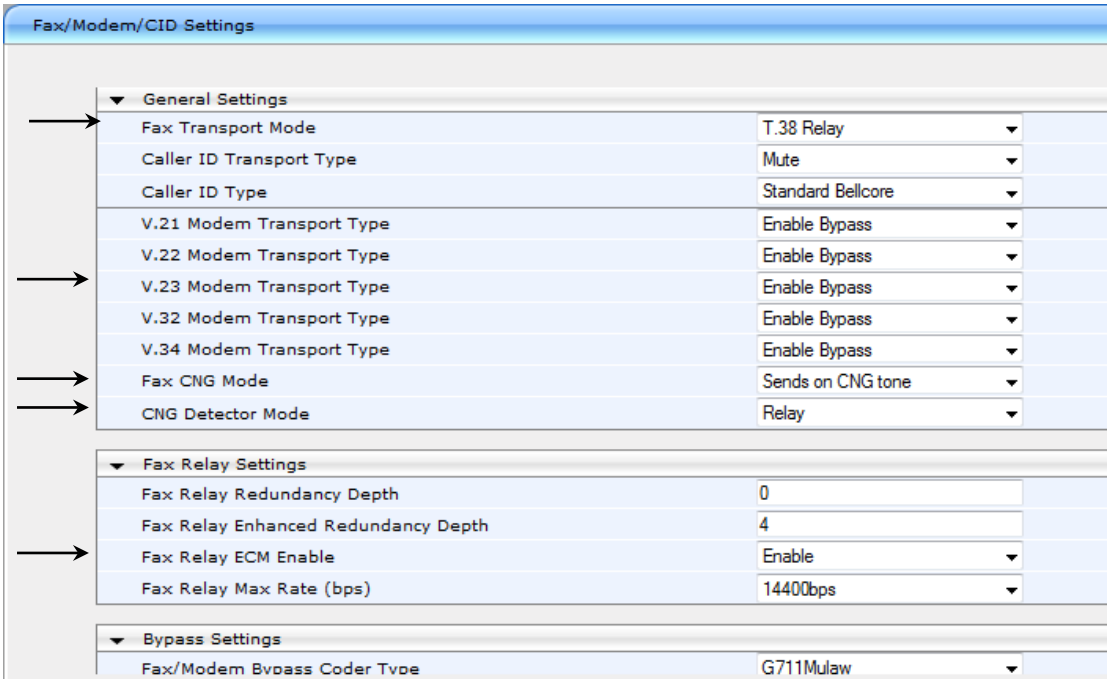
B.6 Step 6: Configure Base Media Fax Settings

This step describes how to configure the base media fax settings for the MP-11x device.

➢ **To configure the base media fax settings :**

1. Open the 'SIP General Parameters' page (**Configuration** tab > **VoIP** menu > **Media** > **Fax/Modem/CID Settings**).

Figure 4-76: Configuring Base Media Fax Settings



2. From the 'Fax Transport Mode' drop-down list, select **T.38 Relay.**
3. From the 'V.x Transport Type' drop-down lists, select **Enable Bypass**.
4. From the 'Fax CNG Mode' drop-down lists, select **Send on CNG tone**.
5. From the 'Fax Relay ECM Enable' drop-down lists, select **Enable**.
6. From the 'CNG Detector Mode' drop-down lists, select **Relay**.

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com