Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2013 & BluIP SIP Trunk using Mediant E-SBC

Microsoft Partner
Gold Communications

Lync

bluIP™

AudioCodes

October 2013

Document # LTRT-39310

Table of Contents

List of Figures

List of Tables

Reader's Notes

Notice

This document describes how to connect Microsoft Lync Server 2013 and BluIP SIP Trunk using AudioCodes Mediant E-SBC product series, which includes the Mediant 800 Gateway & E-SBC, Mediant 1000B Gateway & E-SBC, Mediant 3000 Gateway & E-SBC, Mediant 2600 E-SBC, and Mediant 4000 E-SBC.

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: October-17-2013

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.

Reader's Notes

1 Introduction

This Configuration Note shows how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between BluIP's SIP Trunk and Microsoft's Lync Server 2013 environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and BluIP Partners who are responsible for installing and configuring BluIP's SIP Trunk and Microsoft's Lync Server 2013 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.60A.241.010
Protocol	▪ SIP/UDP (to the BluIP SIP Trunk) ▪ SIP/TCP or TLS (to the Lync Front End Server)
Additional Notes	Force transcoding is required because 360 Networks (originating partner for BluIP Direct Inward Dialing (DIDs)) requires RTCP events. Specific interworking for Music on Hold, Session Timer, RTCP and Fax are supported.

2.2 BluIP SIP Trunking Version

Table 2-2: BluIP Version

Vendor/Service Provider	BluIP / BroadSoft
SSW Model/Service	BroadSoft Application Server
Software Version	BroadSoft Release 17 SP 4
Protocol	SIP
Additional Notes	T.38 and G.711 fallback are supported but do not support VBD for Fax. The network does not allow the Session Timer to transverse the network.

2.3 Microsoft Lync Server 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2013 5.0.8308.0
Protocol	SIP
Additional Notes	None

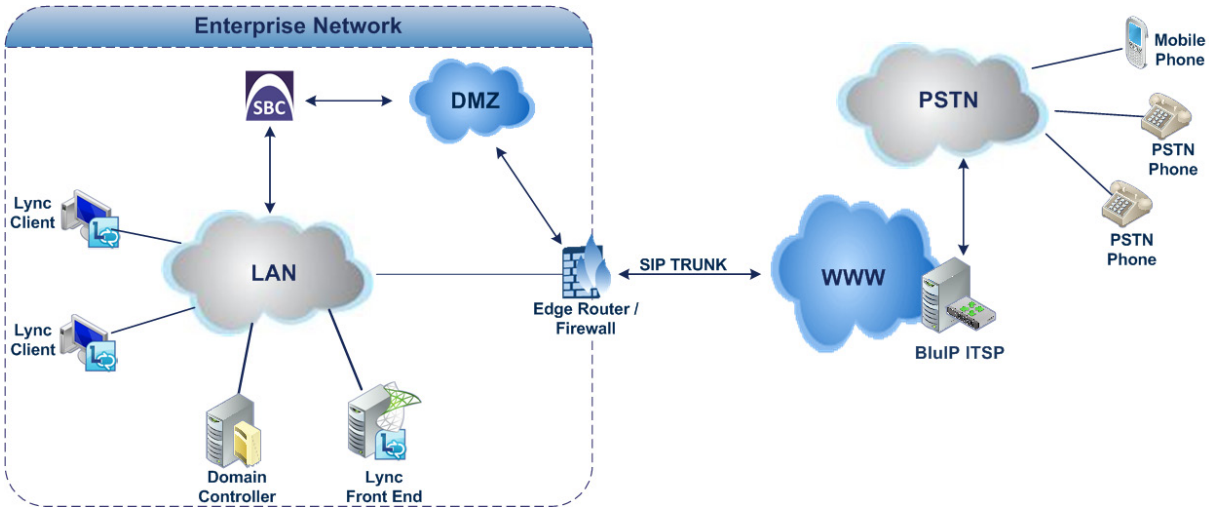
2.4 Interoperability Test Topology

Interoperability testing between AudioCodes E-SBC and BluIP SIP Trunk with Lync 2013 was performed using the following topology setup:

- Enterprise deployed with Microsoft Lync Server 2013 in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using BluIP's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between Lync Server 2013 network in the Enterprise LAN and BluIP's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Lync with BluIP SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN ▪ BluIP SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ BluIP SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ BluIP SIP Trunk supports G.711U-law and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ BluIP SIP Trunk operates with RTP media type

2.4.2 Known Limitations

No limitations were observed in the interoperability tests performed for AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and BluIP's SIP Trunk that prohibited service.

However, there was an enhanced interworking which enabled the use of customer/client enterprise based Music on Hold to be supported from the Microsoft Lync 2013 infrastructure over the BluIP SIP trunk. Natively, the BluIP SIP trunk supports Hold functionality in the format of '0.0.0.0' and 'Inactive'. Microsoft supports the *Send-Only* method within the SDP of the re-INVITE. Message manipulation handling was added to provide the Music on Hold feature functionality of the Microsoft Lync 2013 environment to operate over the BluIP infrastructure. This was done to also assist with the regular Hold feature.

When a call is placed on hold using the 'Inactive' mode, the call is disconnected by BluIP, at the five minute duration of the Hold feature. This is related to the lack of received RTCP events. With the addition of the unique interworking, the Microsoft Lync side also needs RTCP reports and disconnects within 30 seconds. Therefore, the need to force transcoding is required in both directions.

BluIP's call originating partner requires an interworking of a Session Timer with a value of less than 300 seconds for a session refresh. This is necessary to update a call scenario state that originated from the PSTN over the SIP trunk, which during the call flow, transitions to have an inactive media state. This happens so as not to prematurely disconnect the call. However, BluIP does not support Session Timer negotiation directly or transparently. Therefore, the SBC state-of-the art, feature-rich functionality, enables the device to compensate for such occurrences by terminating the Session Timer negotiation on the Lync facing side of the E-SBC within 300 seconds, while allowing the UPDATE messages from the Lync environment to transverse the device and be delivered to BluIP and their subsequent partners. This refreshes the session prior to expiry.

Another observation of the BluIP infrastructure showed that the BluIP SIP Trunking service does not support the use of G.711 VBD (Voice Band Data) for supporting Fax. T.38 fax support was utilized for all fax services.

Reader's Notes

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 but are beyond the scope of this document.

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

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

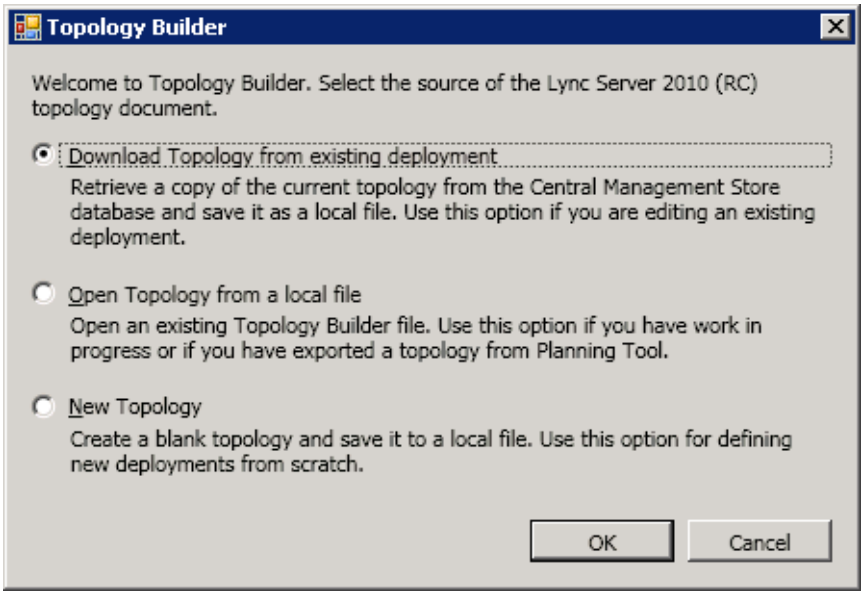
➢ **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**

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**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder

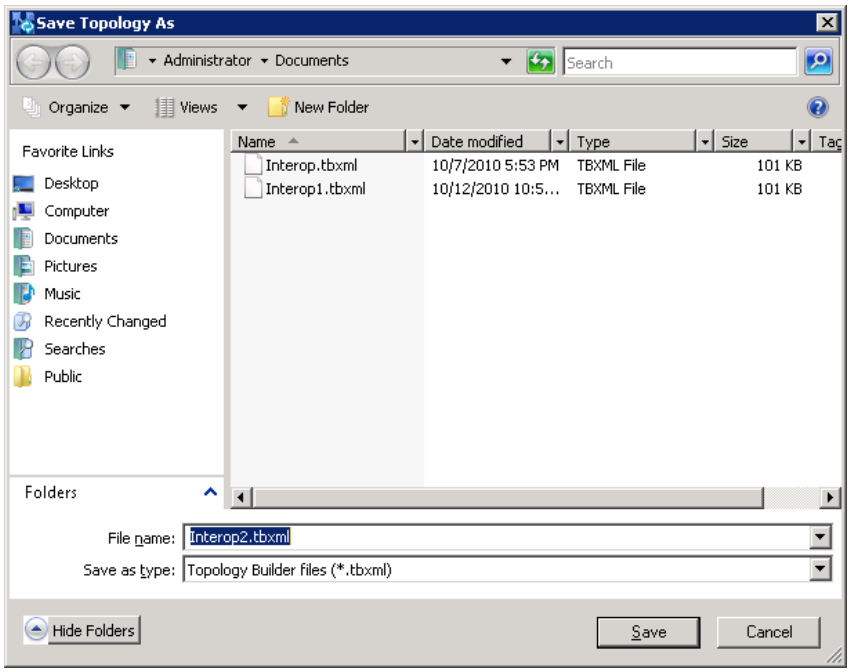
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

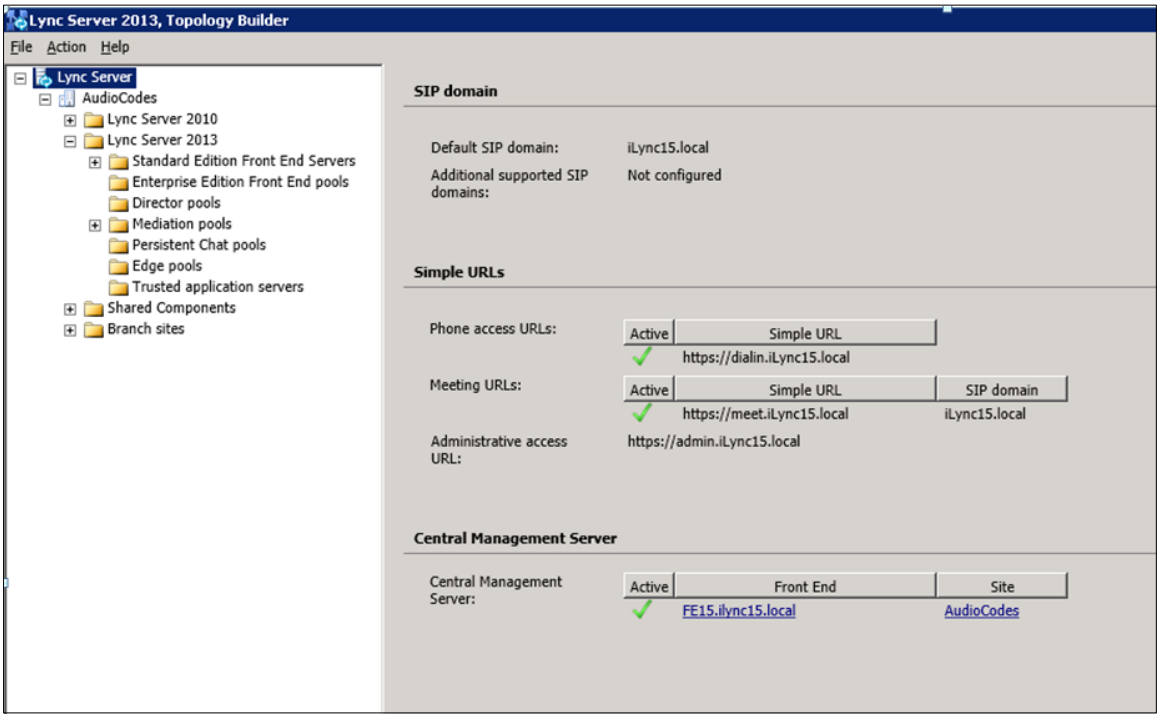
Figure 3-3: Save Topology



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.

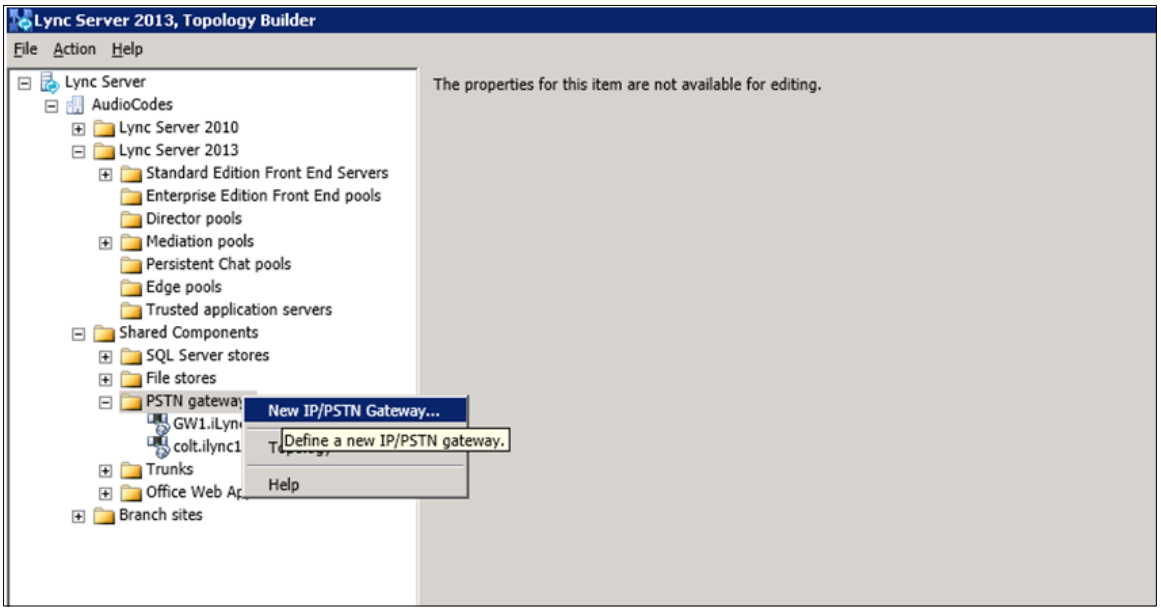
   The Topology Builder screen with the downloaded topology is displayed:

Figure 3-4: Downloaded Topology



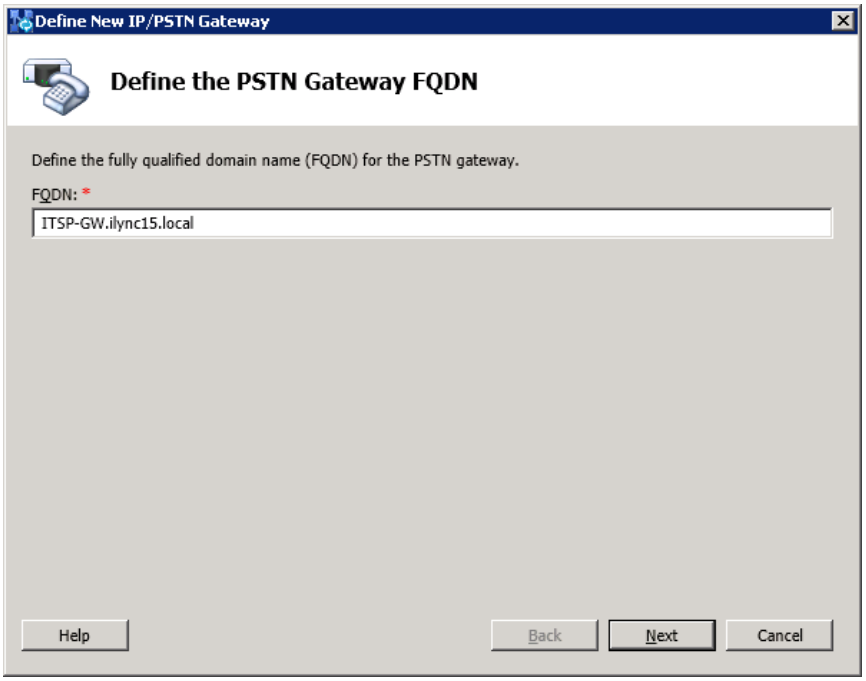
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



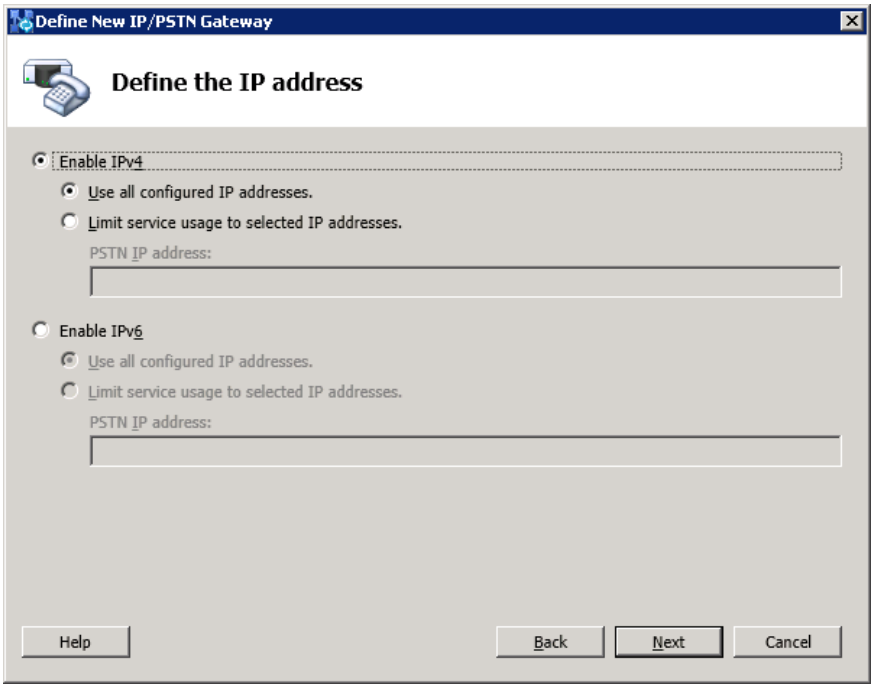
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP-GW.ilync15.local**). Update this FQDN in the relevant DNS record, and then click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



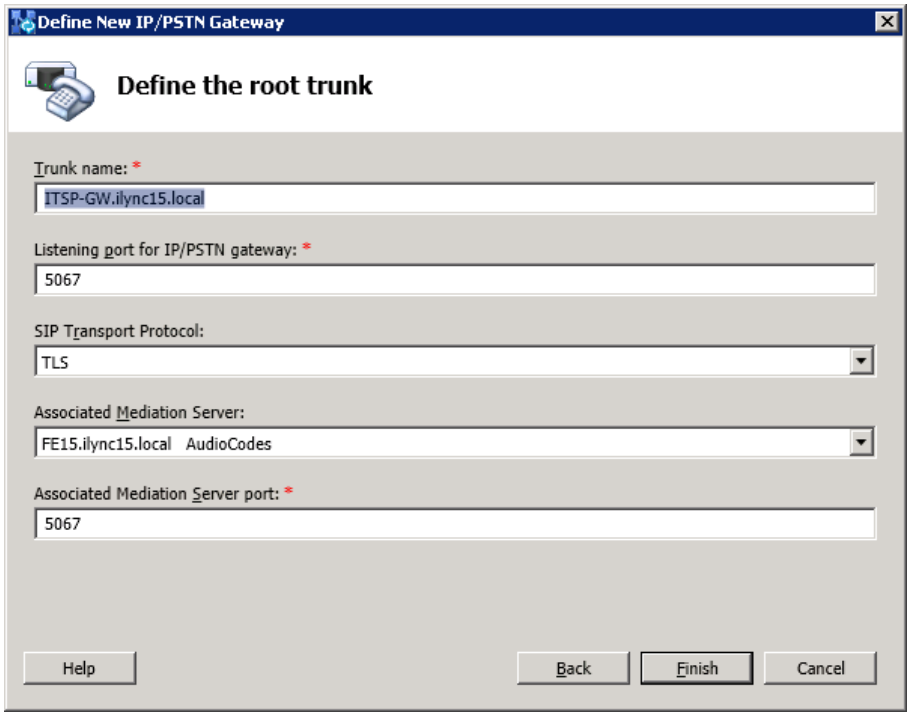
6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

7. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP and FQDN, and gateway listening port.

Notes:

- 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.

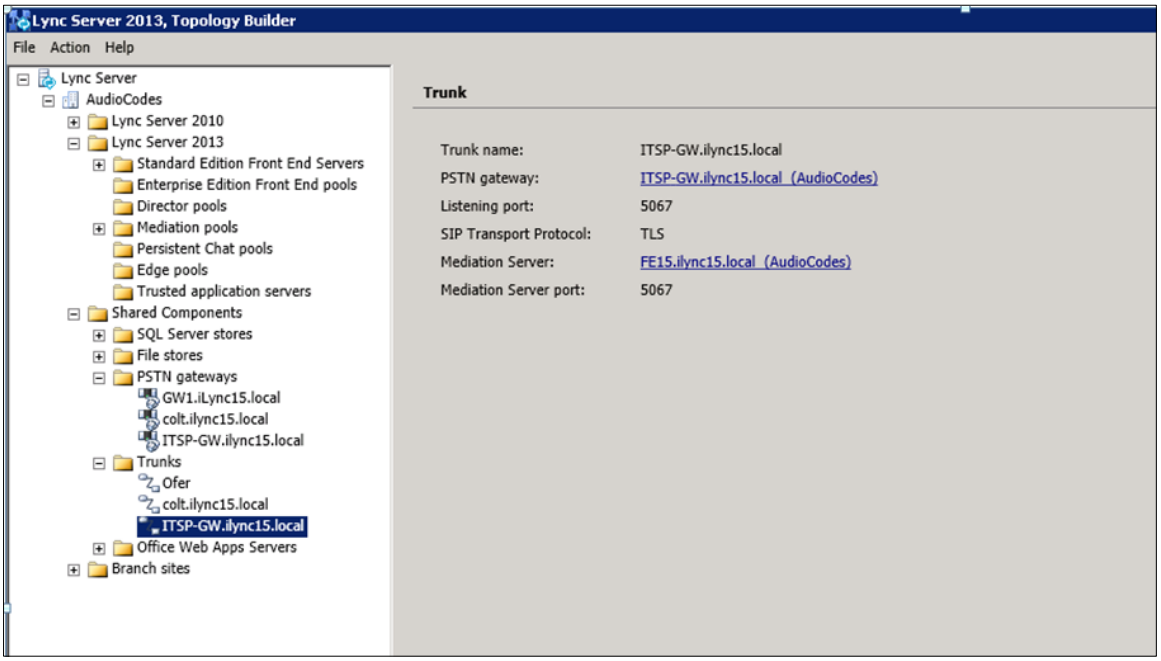
Figure 3-8: Define the Root Trunk



a. In the 'Listening Port for IP/PSTN Gateway' field, enter 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 (e.g., **5067**).
b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses.
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
e. Click **Finish**.

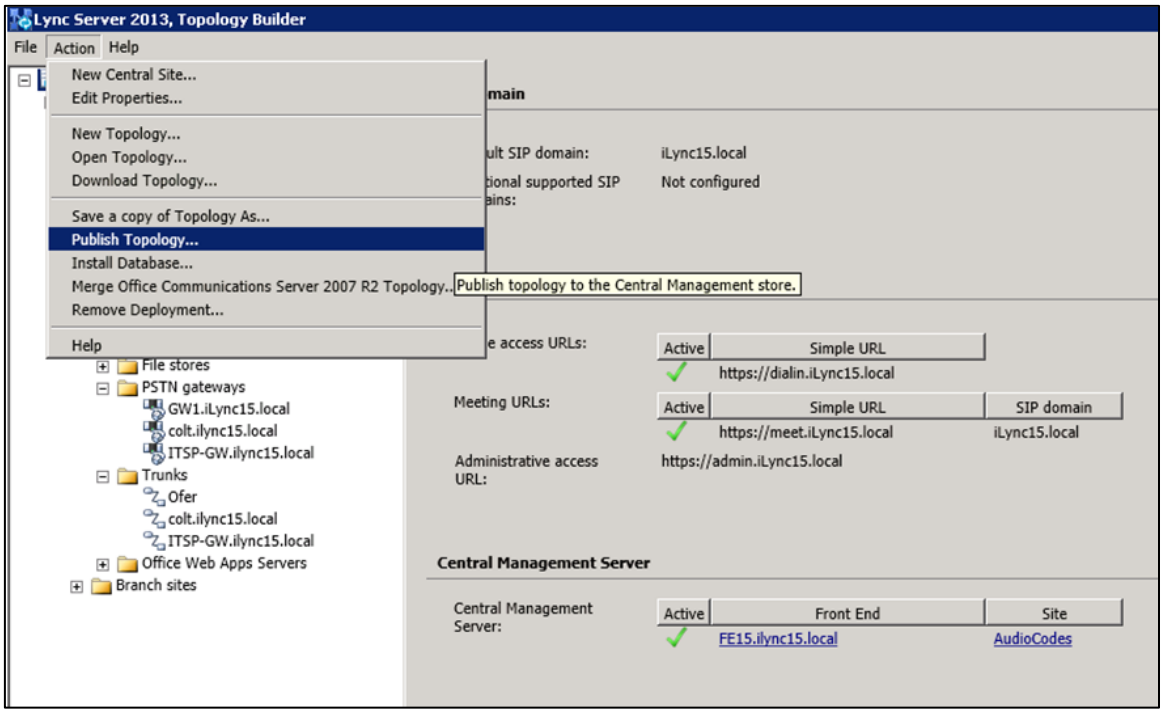
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

Figure 3-9: E-SBC added as IP/PSTN Gateway and Trunk Created



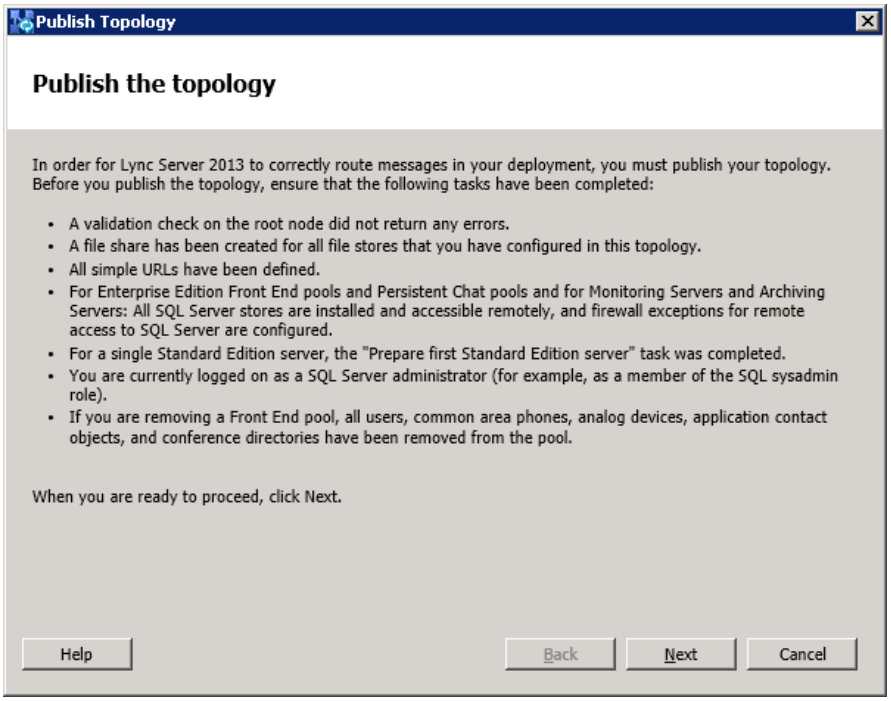
8. Publish the topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



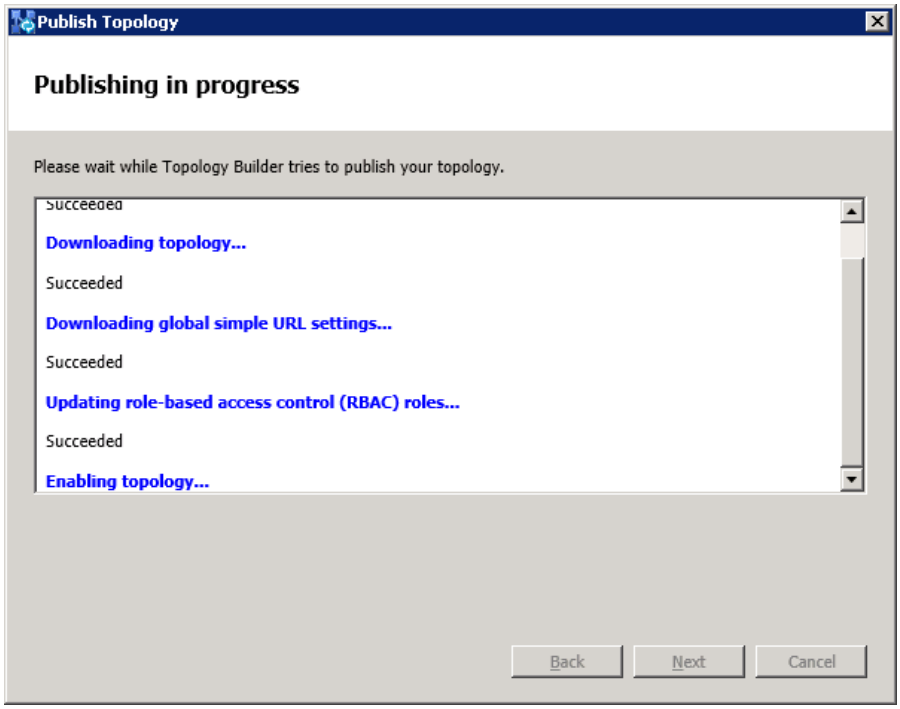
The following is displayed:

Figure 3-11: Publish the Topology



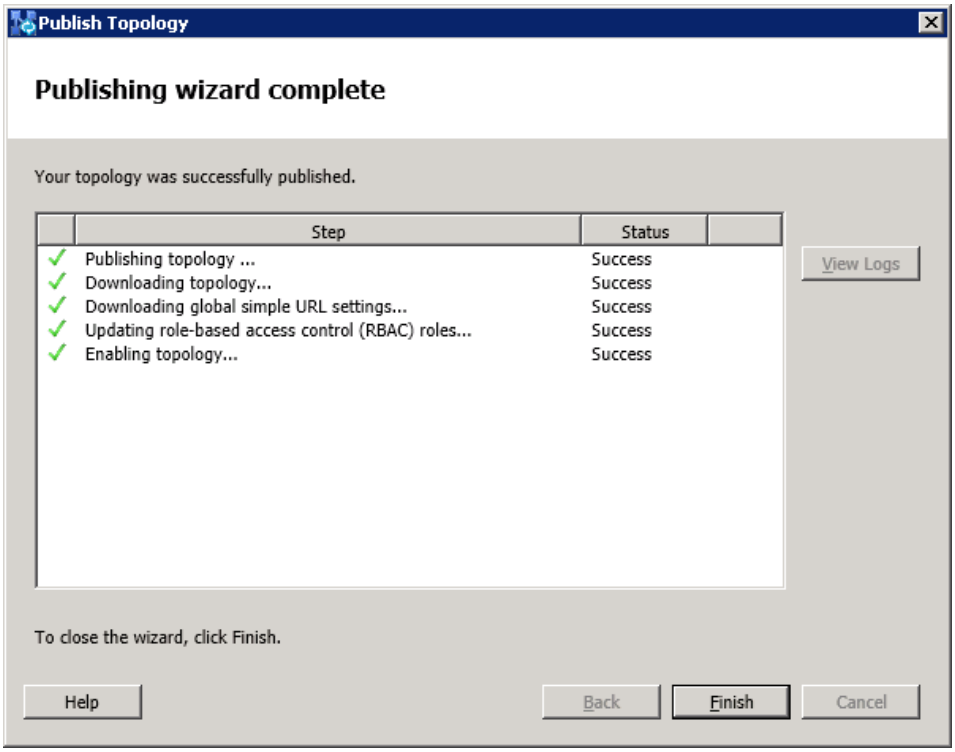
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. 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 to associate it with the E-SBC PSTN gateway.

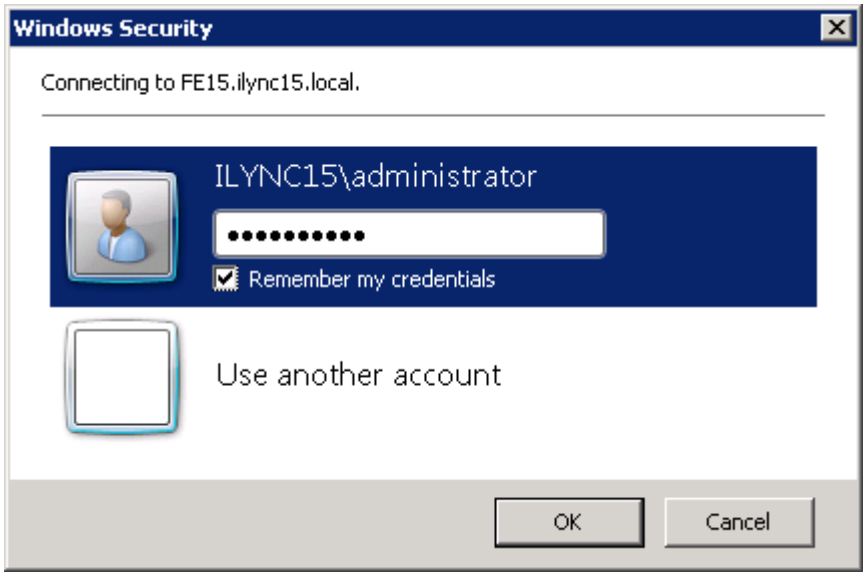
➢ **To configure the "route" on Lync Server 2013:**

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

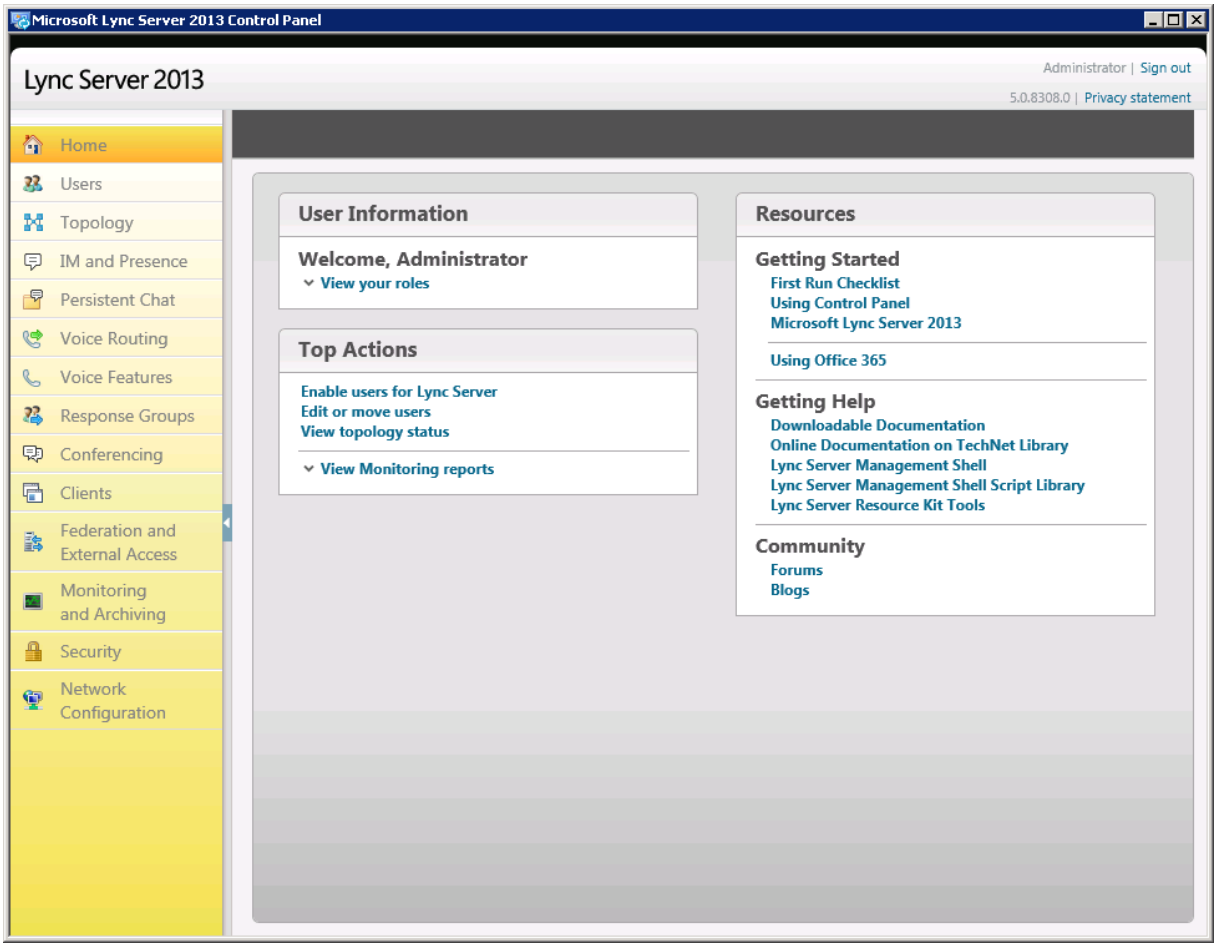
You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



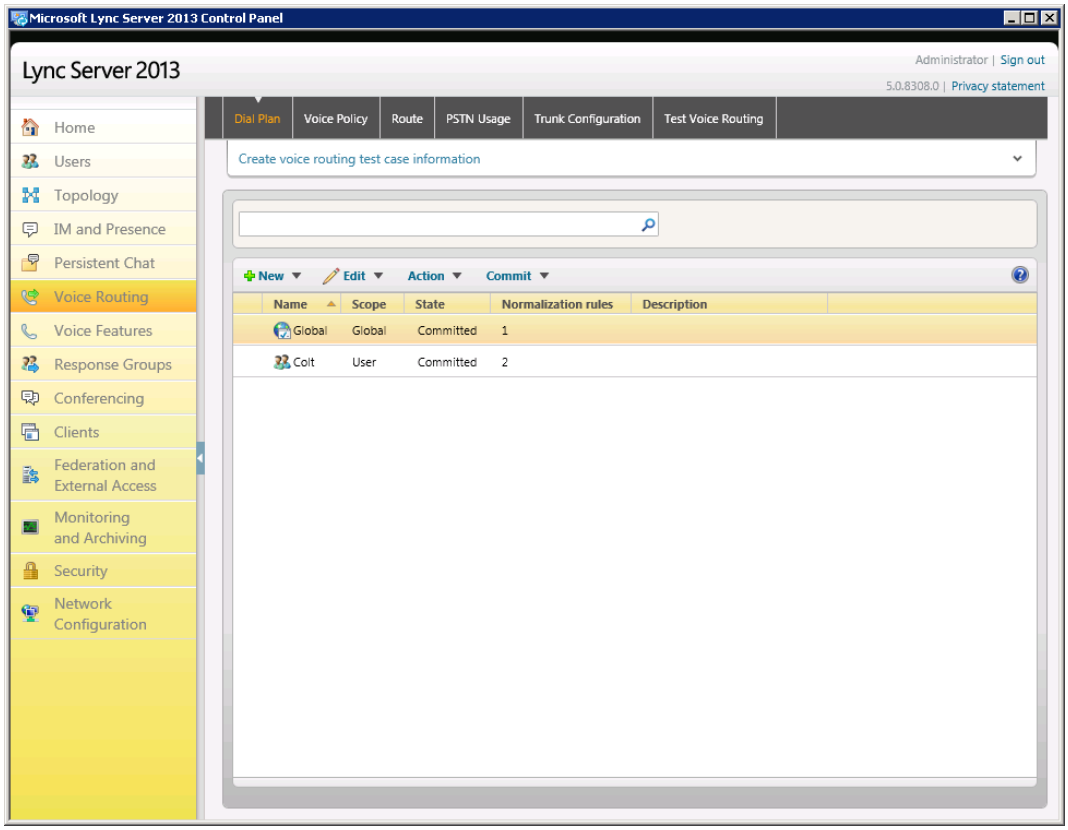
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



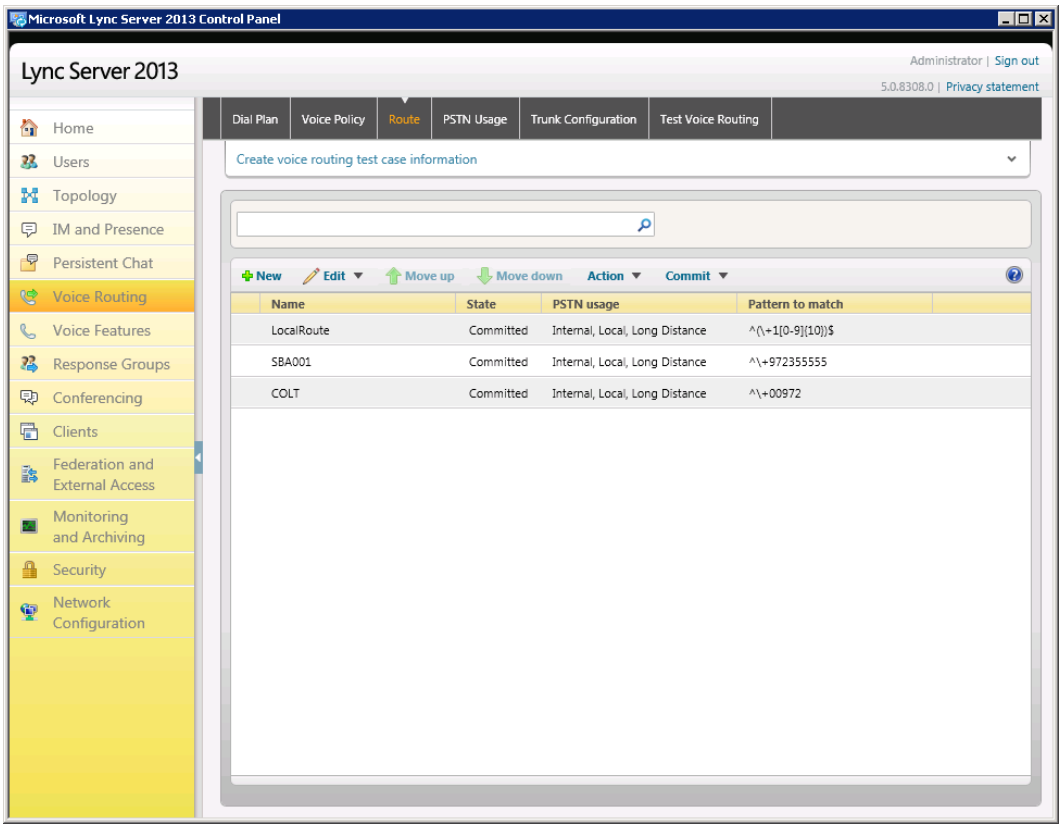
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



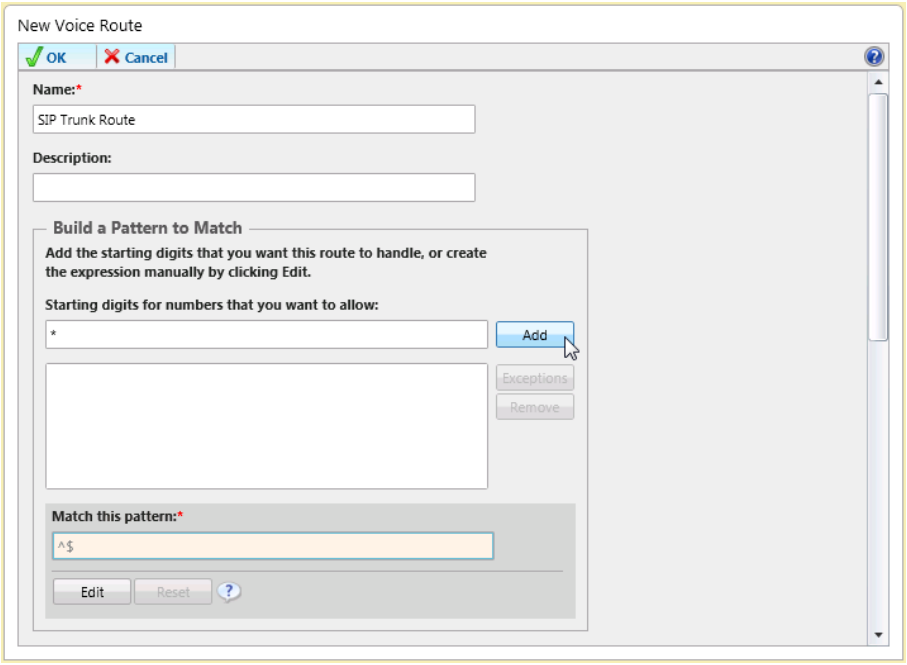
4. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



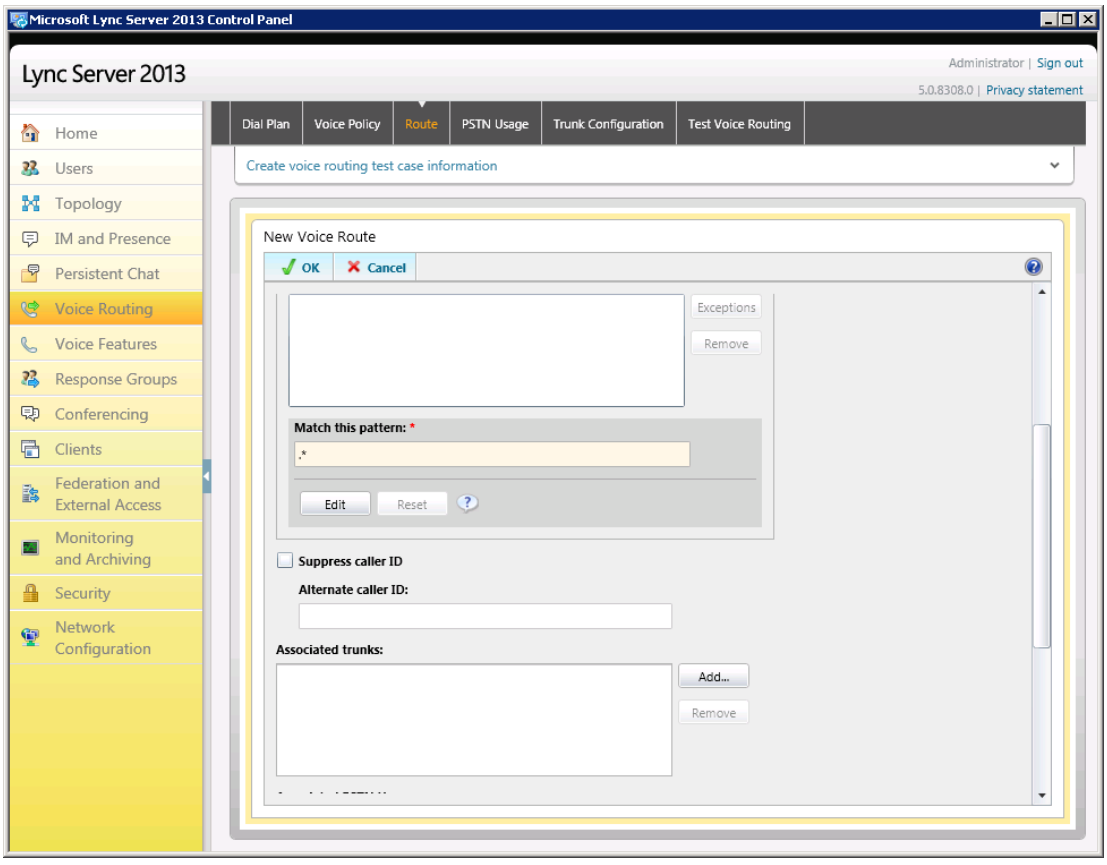
5. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



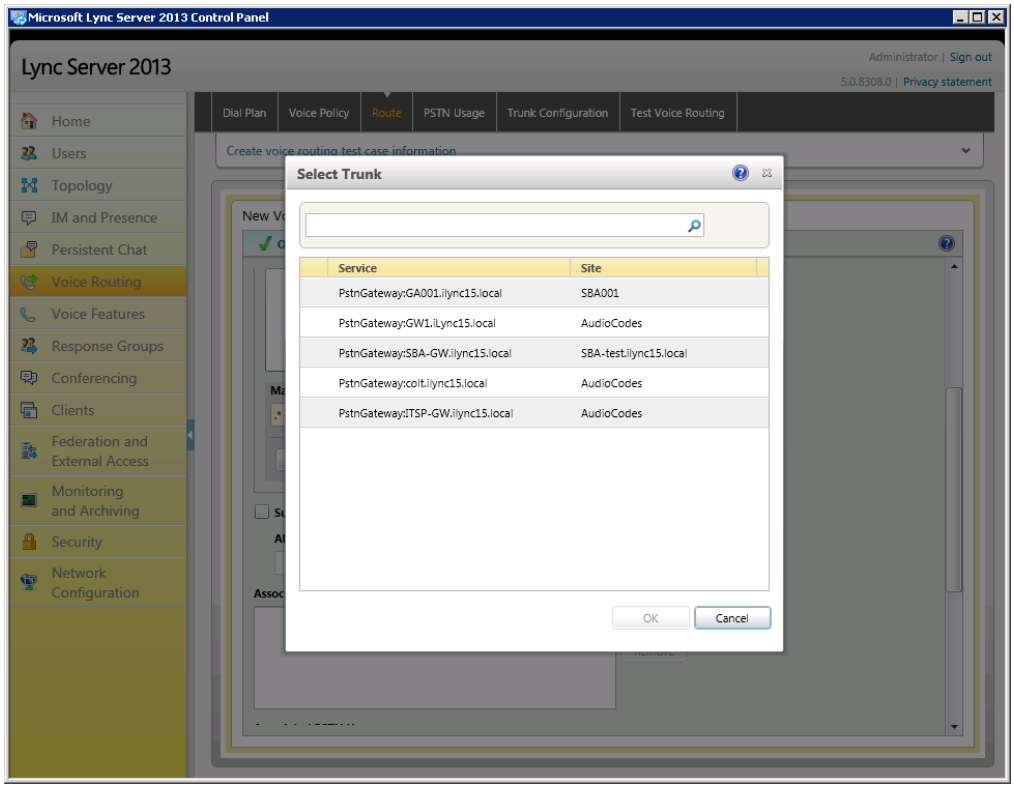
6. In the 'Name' field, enter a name for this route (e.g., **SIP Trunk Route**).
7. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.

Figure 3-20: Adding New Trunk



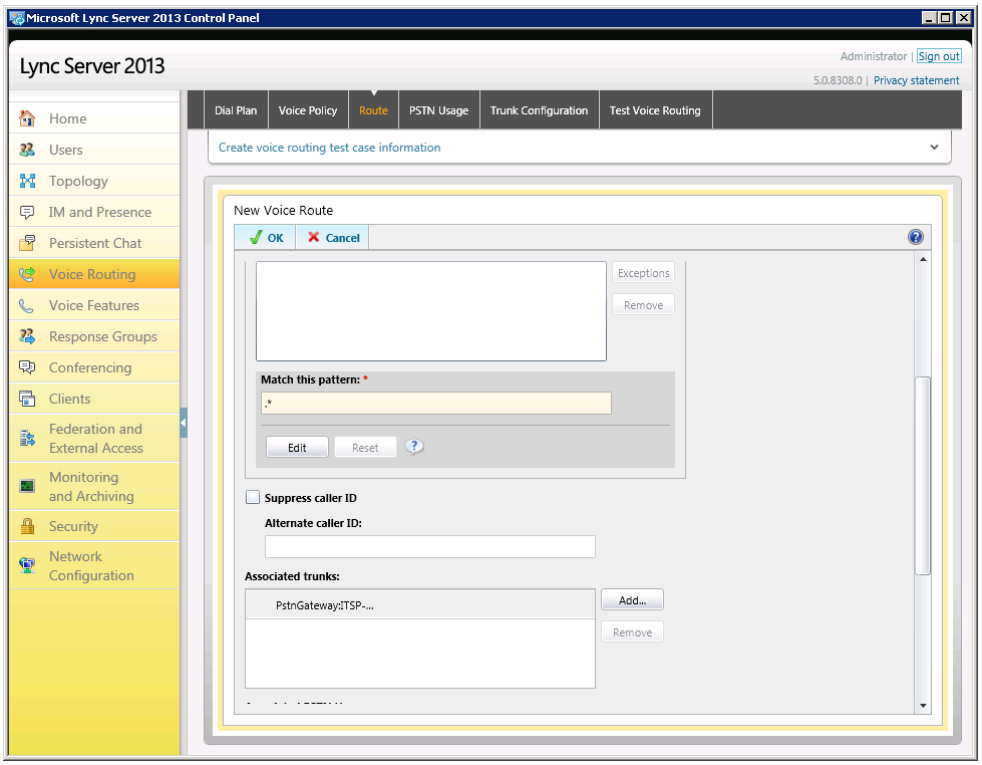
8. Associate the route with the E-SBC Trunk that you created:
   a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



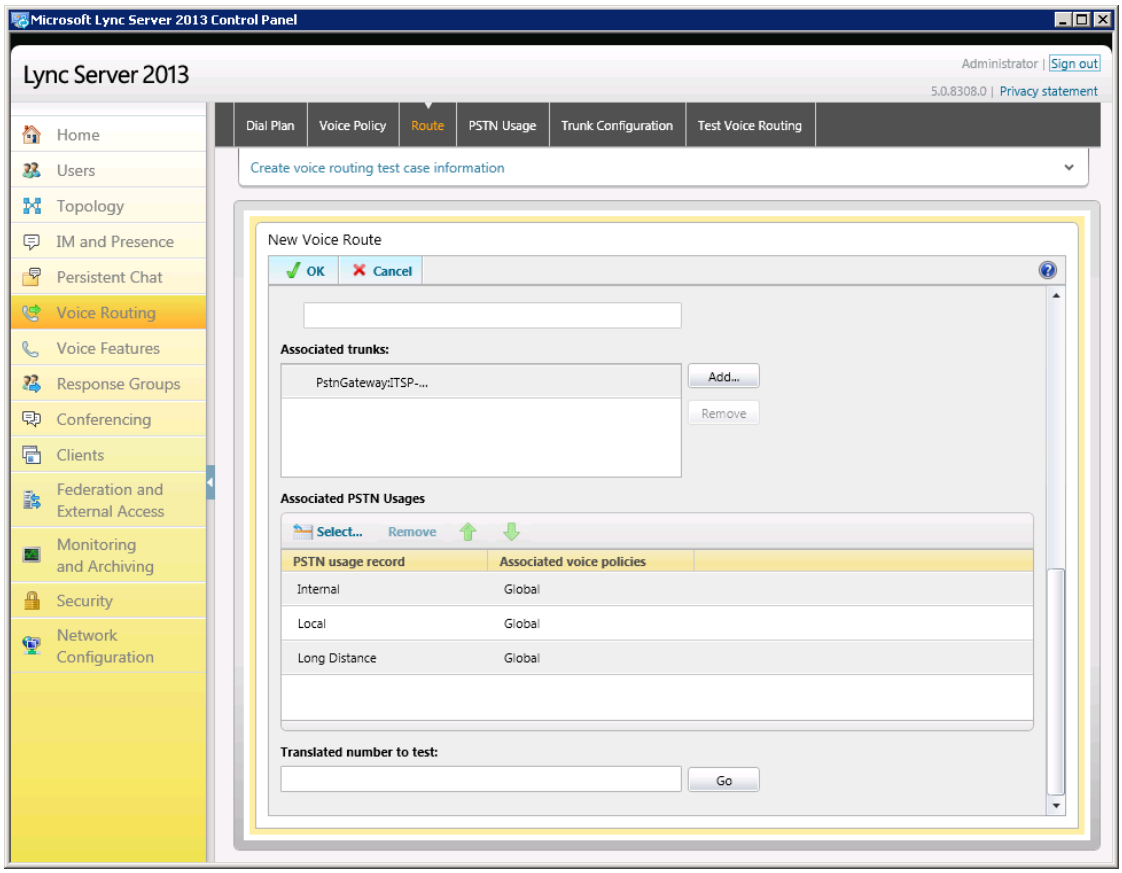
   b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



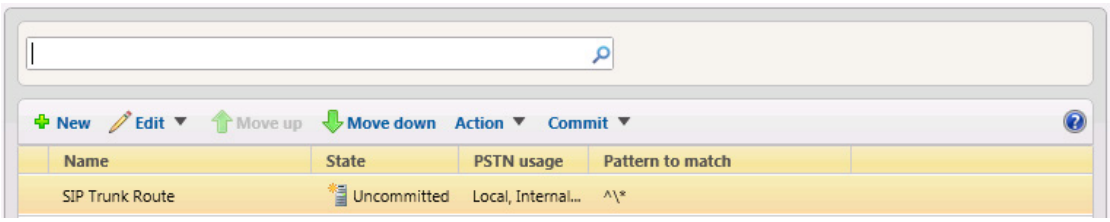
9. Associate a PSTN Usage to this route. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



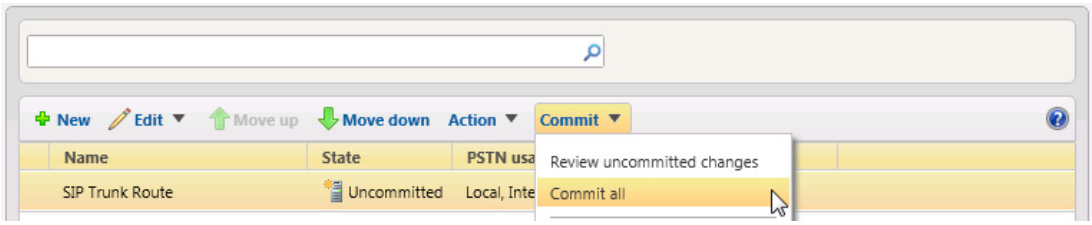
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



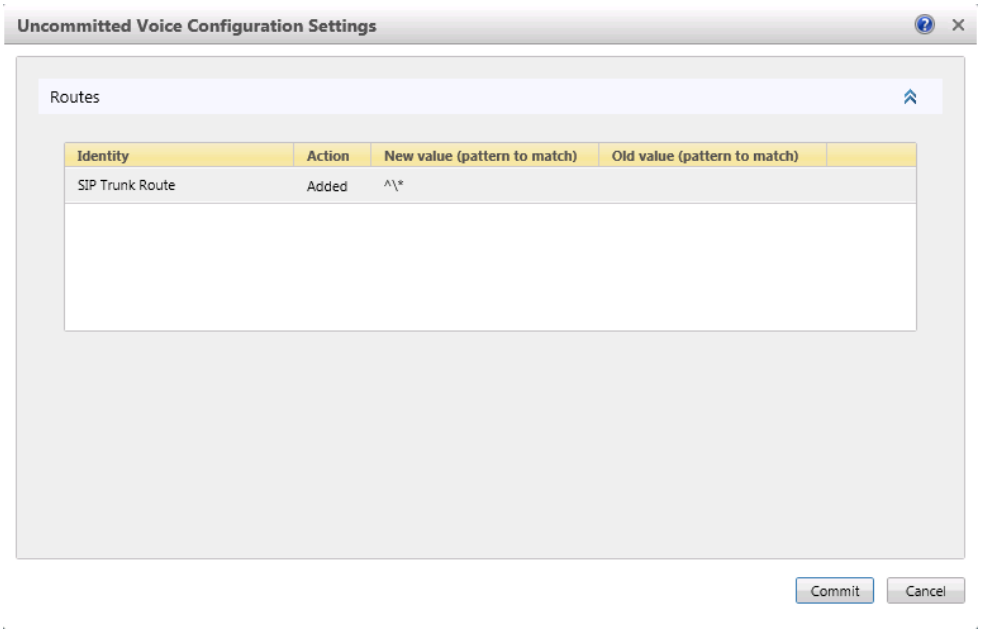
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



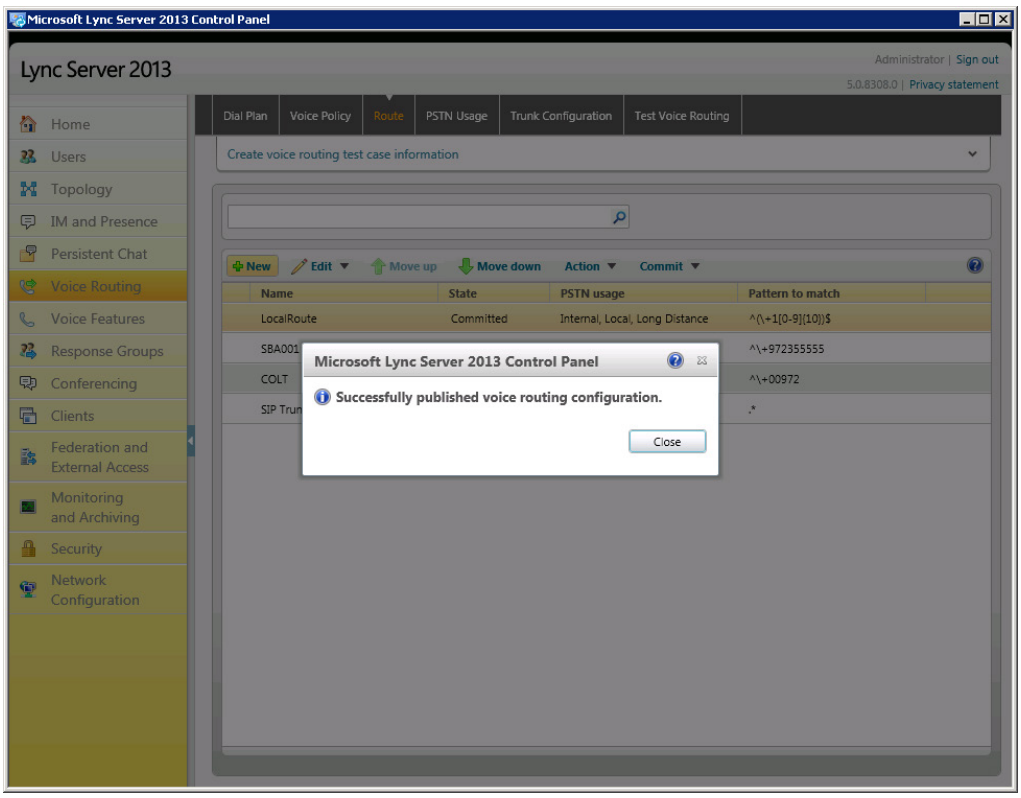
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



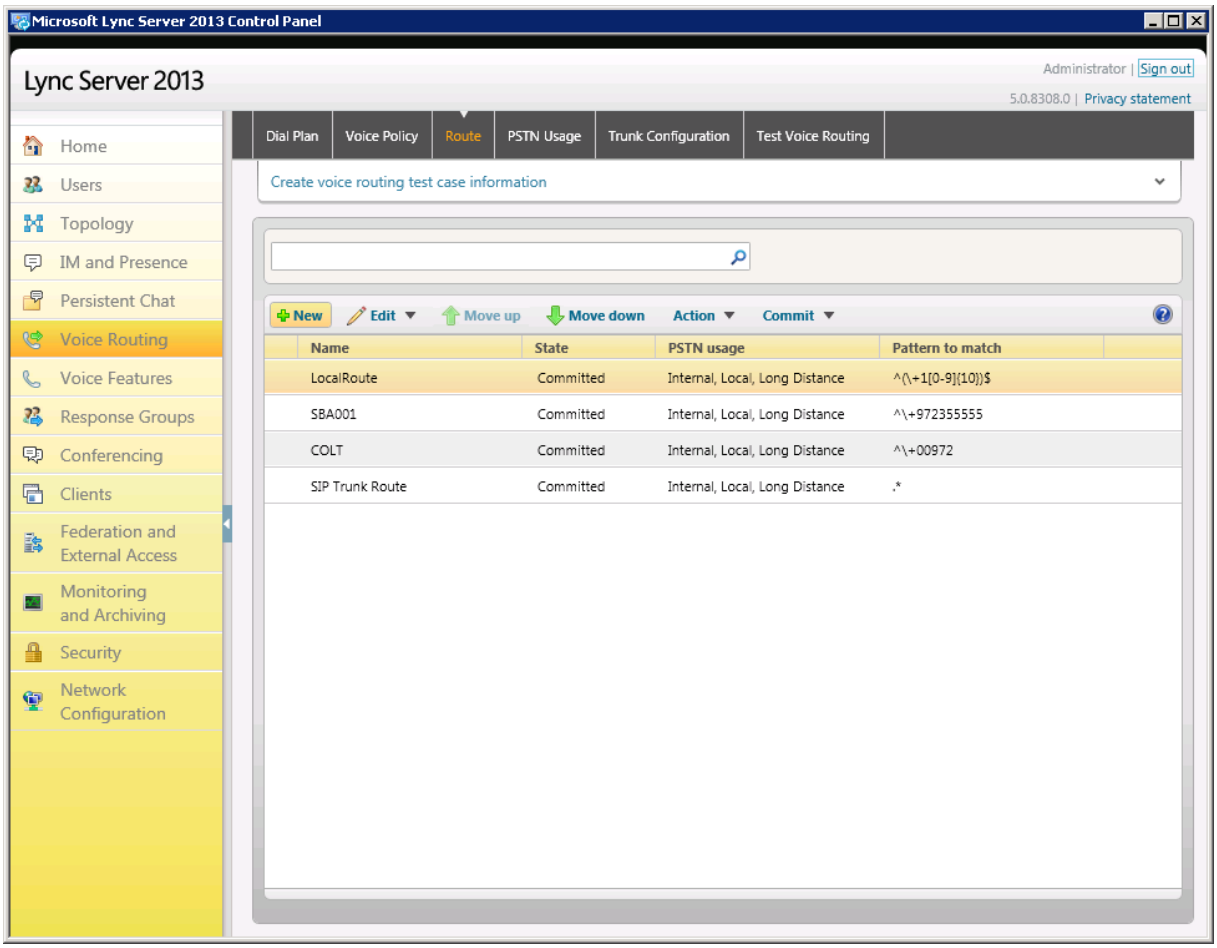
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirmation of Successful Voice Routing Configuration



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

Figure 3-28: Voice Routing Screen Displaying Committed Routes

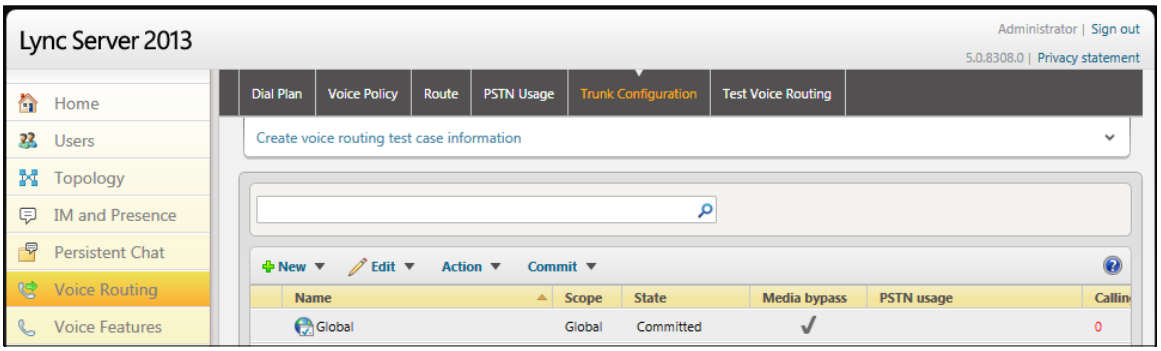


14. For ITSPs that implement a call identifier, continue with the following steps:

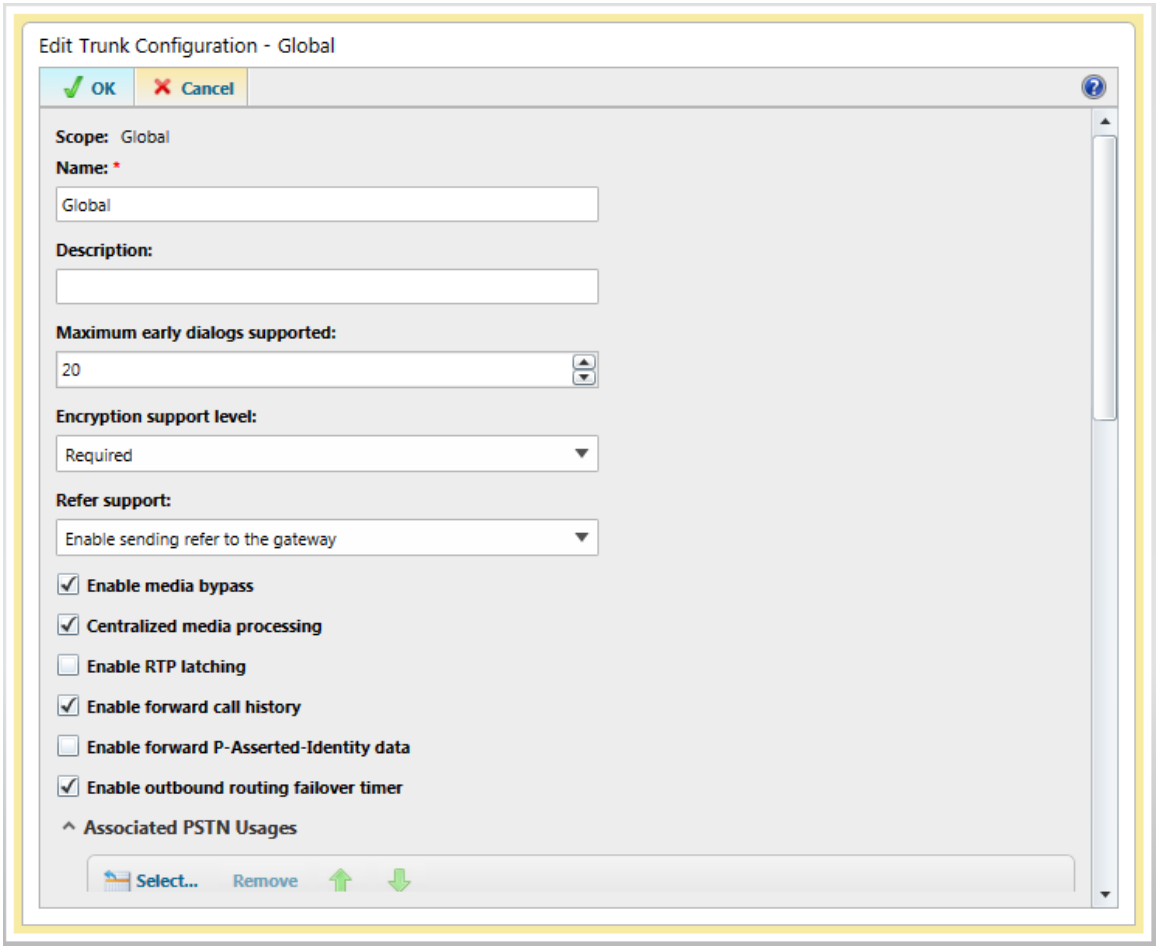
Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Lync user number). This ID is required by BluIP SIP Trunk in the P-Asserted-Identity header. Using a Message Manipulation rule (see Section 4.13 on page 82), the device adds this ID to the P-Asserted-Identity header in the sent INVITE message.

a. In the Voice Routing page, select the **Trunk Configuration** tab. Note that you can add and modify trunk configuration by site or by pool.

Figure 3-29: Voice Routing Screen – Trunk Configuration Tab



b. Click **Edit**; the Edit Trunk Configuration page appears:



c. Select the **Enable forward call history** check box, and then click **OK**.

d. Repeat Steps 11 through 12 to commit your settings.

Reader's Notes

4 Configuring AudioCodes E-SBC

This section shows how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the BluIP SIP Trunk. The configuration procedures are based on the interoperability test topology described in Section 2.4 on page 14, and includes the following main areas:

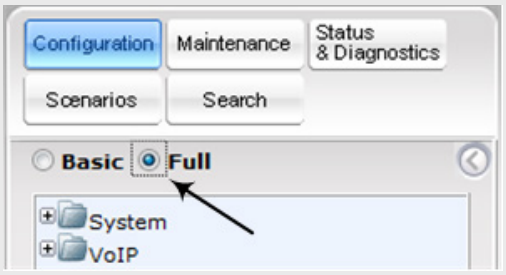
- E-SBC WAN interface - BluIP SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

- To implement Microsoft Lync and BluIP SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

  For more information about the Software License Key, contact your AudioCodes sales representative.
- The scope of this document does **not** cover security aspects for connecting the SIP Trunk to the 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* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in full-menu display mode. To do this, select the **Full** option, as shown below:



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

4.1 Step 1: Configure Network Interfaces

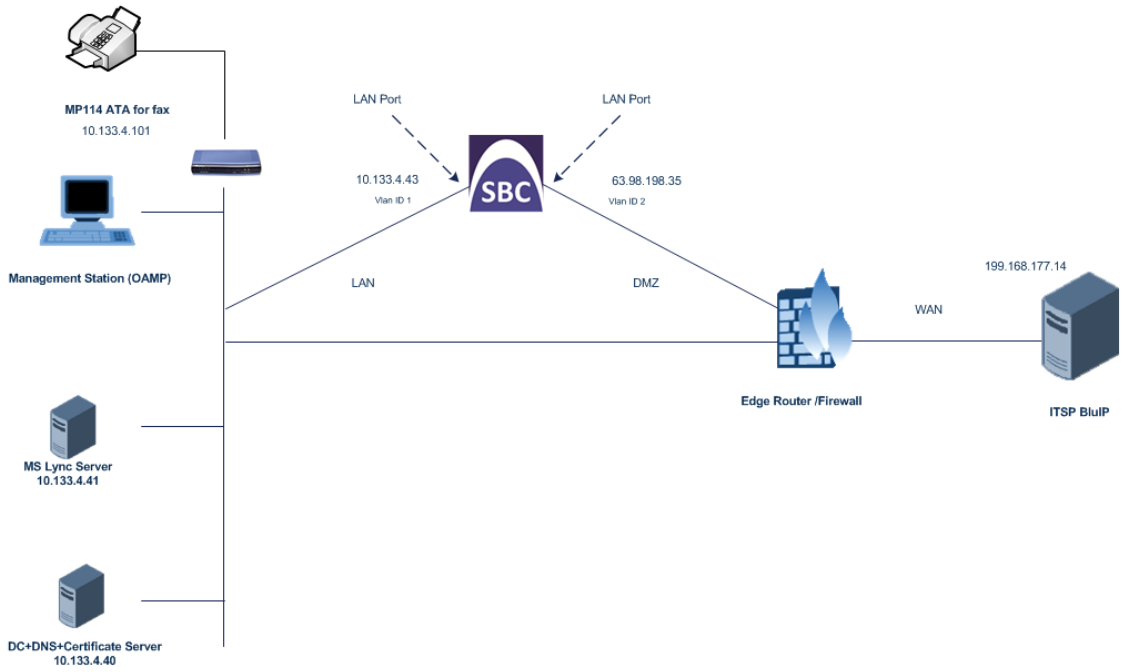
This step shows how to configure the E-SBC's network interfaces. There are several ways to deploy the E-SBC. However, the example scenario in this document uses the following deployment method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the BluIP 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

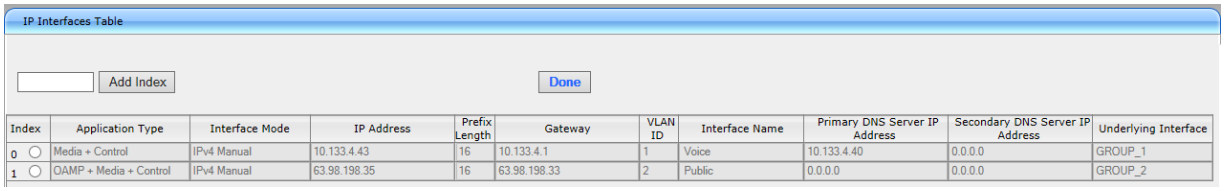
The procedure below shows how to configure the IP network interfaces for each of the following interfaces:

- 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	**10.133.4.43** 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	**10.133.4.40**
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.
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 the 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.

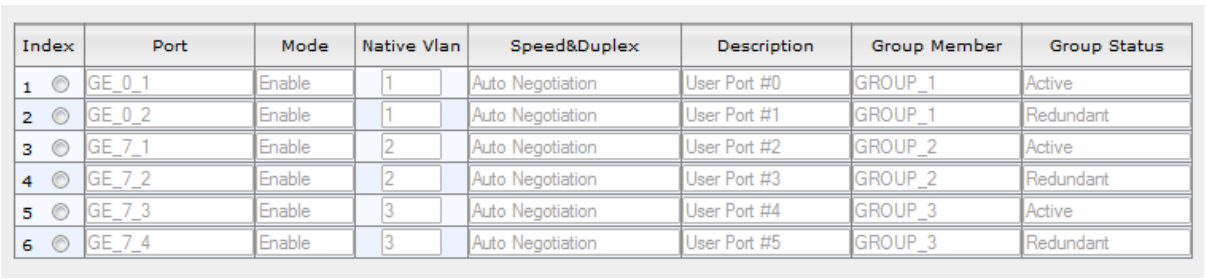
4.1.2 Step 1b: Configure the Native VLAN ID

The procedure below shows 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

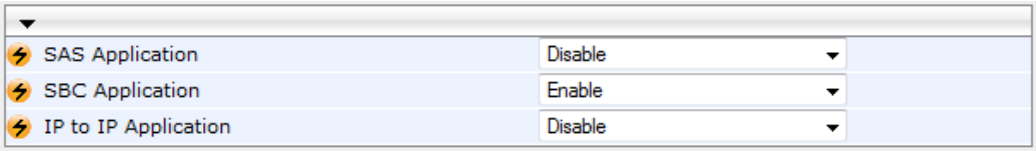
4.2 Step 2: Enable the SBC Application

This step shows 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 4.16 on page 1001).

4.3 Step 3: Signaling Routing Domains

This step shows 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 Media Realms

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

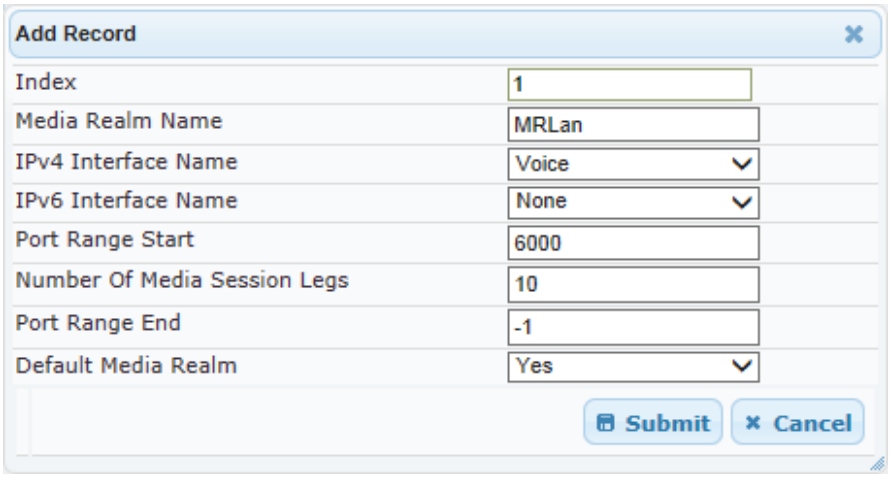
The simplest configuration is to create one Media Realm for internal (LAN) traffic and another for external (WAN) traffic, which is described in the procedure below for our example scenario.

➢ **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	**6000** 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 4-5: Configuring LAN Media Realm

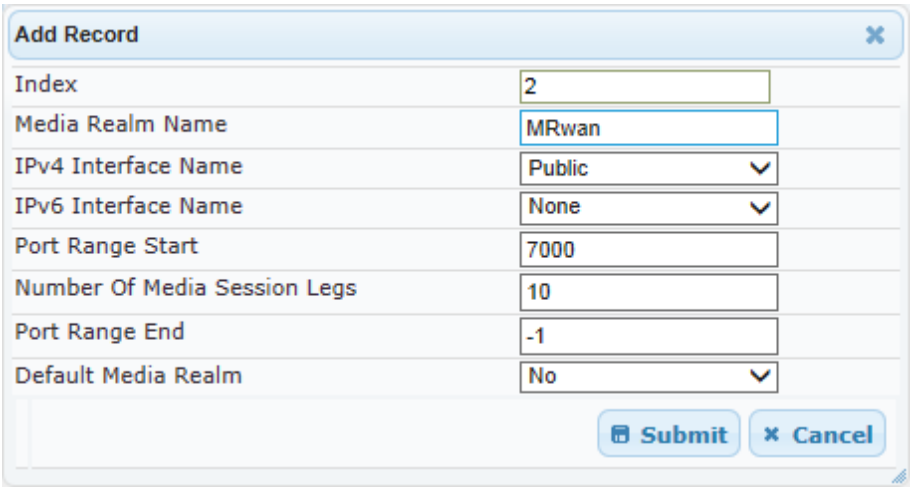


   c. Click **Submit**.

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	**7000** 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.

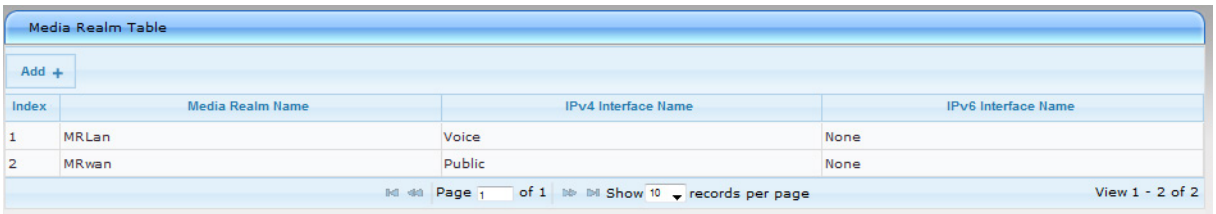
Figure 4-6: Configuring WAN Media Realm



   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-7: Displaying Configured Media Realm



4.3.2 Step 3b: Configure SRDs

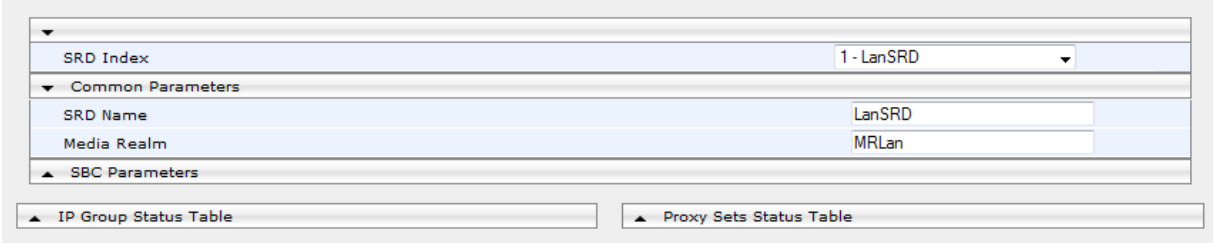
The procedure below shows how to configure the SRDs.

➢ **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.

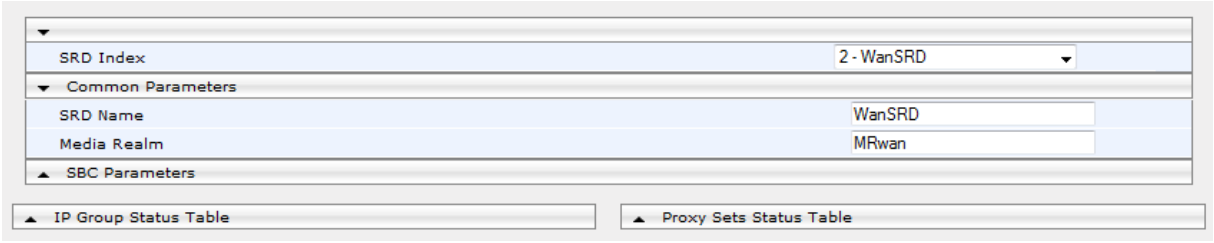
Figure 4-8: Configuring LAN SRDs



   b. Click **Submit**.
3. Add an SRD for the E-SBC's external interface (toward the BluIP 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 4-9: Configuring WAN SRDs



   b. Click **Submit**.

4.3.3 Step 3c: 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 shows 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**

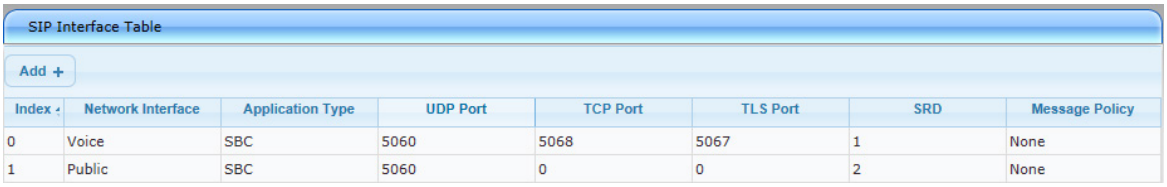
   c. Click **Submit**.
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure the following parameters:

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 4-10: Displaying Configured SIP Interfaces



SIP Interface Table

Add +

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
0	Voice	SBC	5060	5068	5067	1	None
1	Public	SBC	5060	0	0	2	None

4.4 Step 4: Configure Proxy Sets

This step shows 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
- BluIP service
- Fax supporting ATA

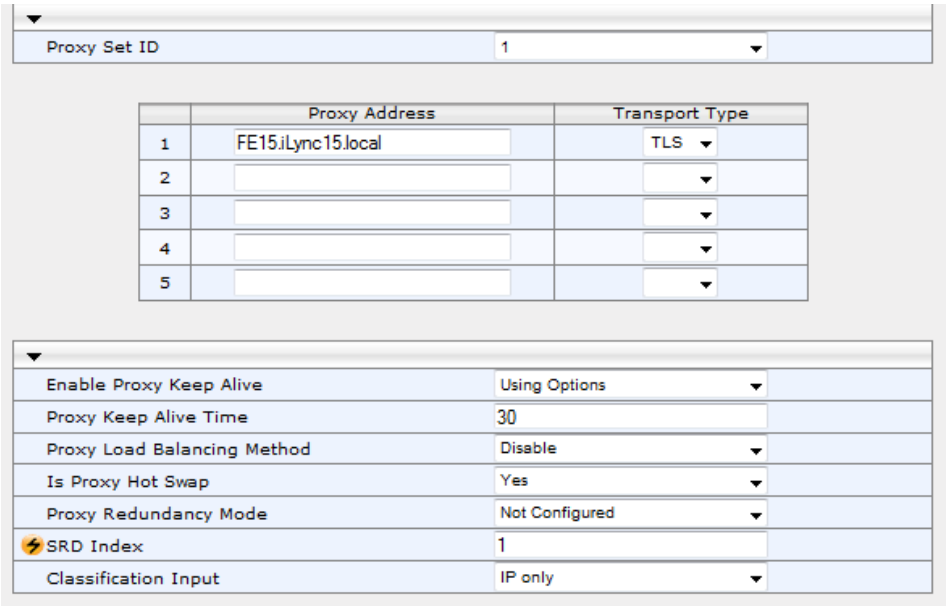
These Proxy Sets will later be associated with IP Groups.

➢ **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 4-11: Configuring Proxy Set for Microsoft Lync Server 2013

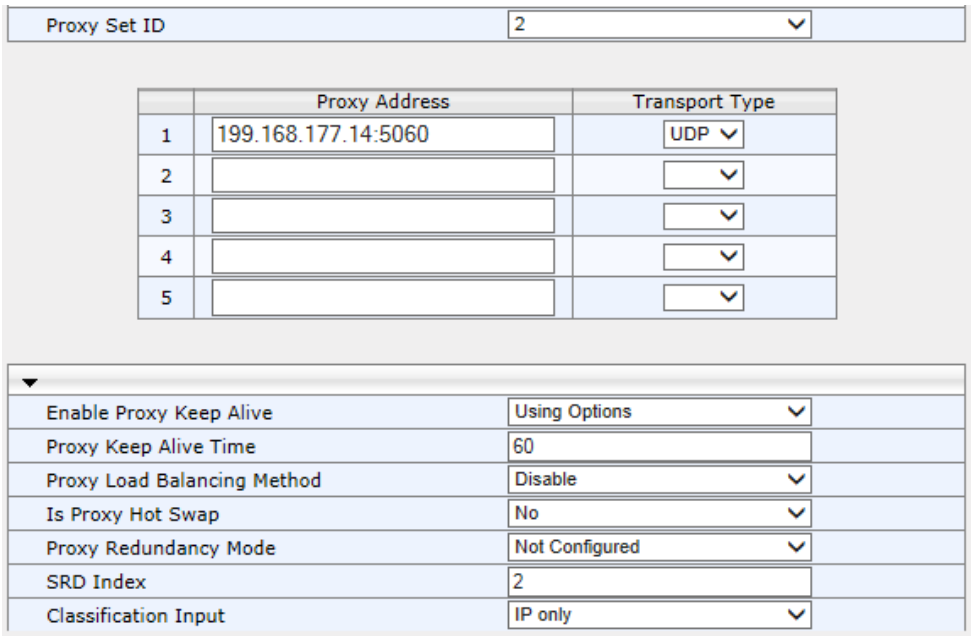


   b. Click **Submit**.

3. Add a Proxy Set for the BluIP service:
   a. Configure the following parameters:

Parameter	Settings
Proxy Set ID	**2**
Proxy Address	**199.168.177.14:5060** BluIP 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 BluIP service.

Figure 4-12: Configuring Proxy Set for BluIP Service

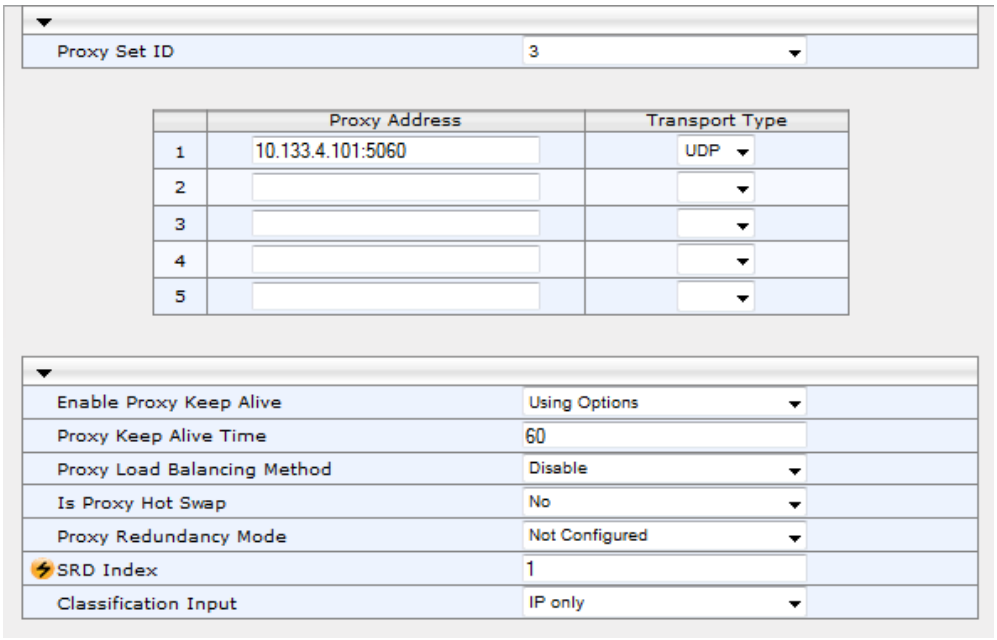


   b. Click **Submit**.

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 4-13: Configuring Proxy Set for Fax Supporting ATA



b. Click **Submit**.

4.5 Step 5: Configure IP Groups

This step shows 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
- BluIP 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	**CorpLab2013**
Proxy Set ID	**1**
SIP Group Name	**audiocodes.com** This is used to ensure the From header has the *audiocodes.com* host name so that the BroadSoft server accepts the call. This is provided by BluIP to the enterprise customer.
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

   c. Click **Submit**.

3. Add an IP Group for the BluIP service:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**2**
Type	**Server**
Description	**BluIP**
Proxy Set ID	**2**
SIP Group Name	**audiocodes.com** This is used to ensure the SIP URL host and the 'To header' have the *audiocodes.com* host name so that the BroadSoft server accepts the call. This is provided by BluIP to the enterprise customer.
SRD	**2**
Media Realm Name	**MRwan**
IP Profile ID	**2**

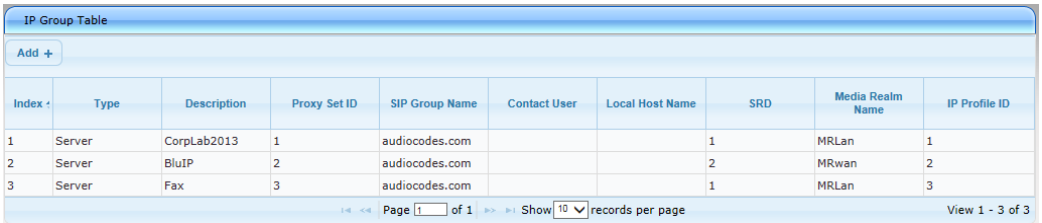
   c. Click **Submit**.
4. Add an IP Group for the BluIP service:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**3**
Type	**Server**
Description	**FAX**
Proxy Set ID	**3**
SIP Group Name	**audiocodes.com**
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**3**
Special Note: SIP Group Name	This is used to ensure the From header has the *audiocodes.com* host name so that the BroadSoft server accepts the call. This is provided by BluIP to the enterprise customer.

   c. Click **Submit**.

The configured IP Group table is shown below:

Figure 4-14: Configuring IP Groups



4.6 Step 6: Configure IP Profiles

This step shows 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 BluIP service. Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 48).

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

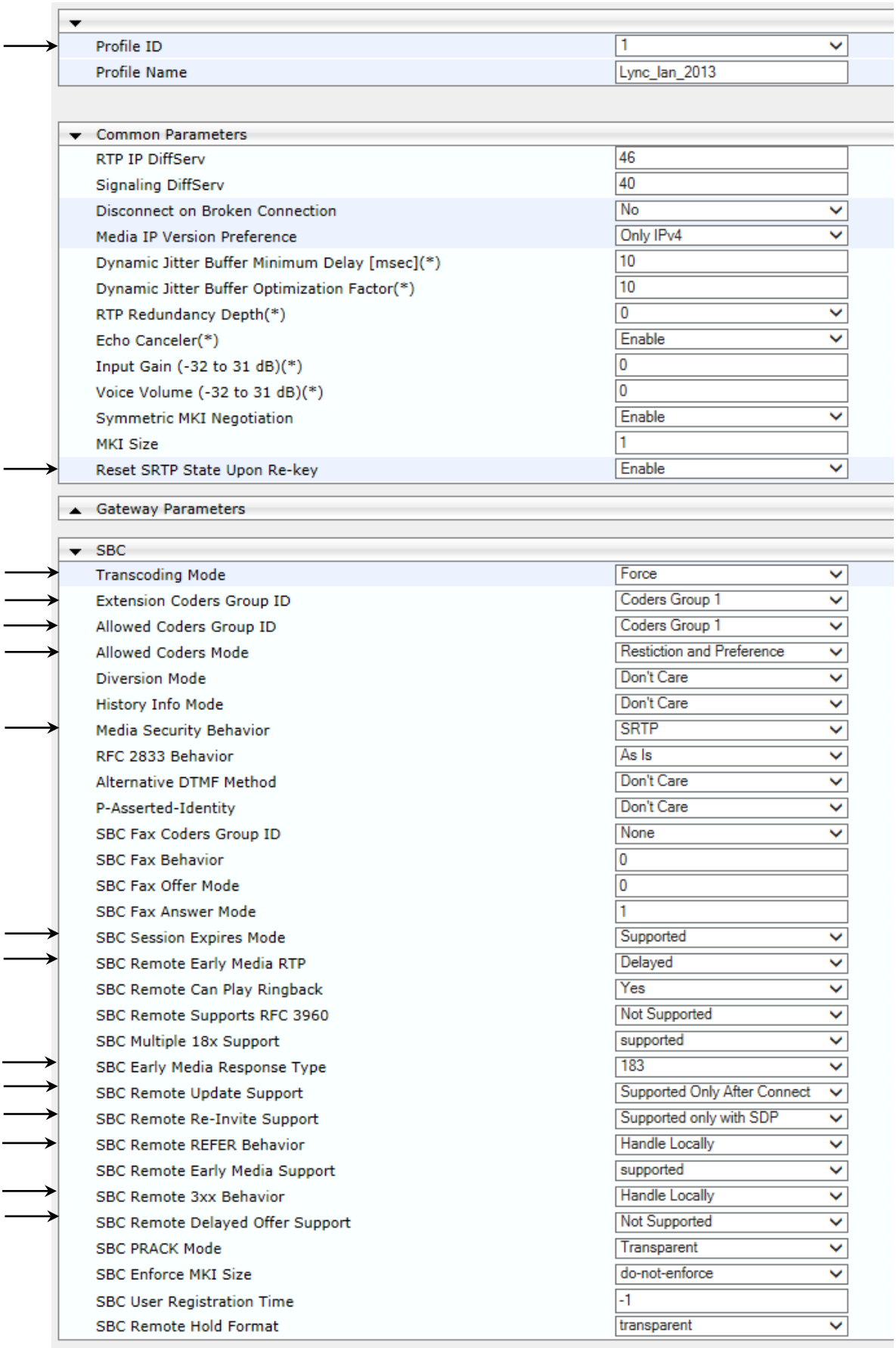
- **Microsoft Lync Server 2013** - to operate in secure mode using SRTP and TLS
- **BluIP Service** - to operate in non-secure mode using RTP and UDP

➢ **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**
Reset SRTP State Upon Re-key	**Enable**
Transcoding Mode	**Force,** this is required to support Music on Hold with RTCP events when calls originate from the PSTN over the SIP trunk.
Extension Coders Group ID	**Coders Group 1**
Allowed Coders Group ID	**Coders Group 1**
Allowed Coders Mode	**Restrict and Preference** This forces the specific preference prioritization
Media Security Behavior	**SRTP**
SBC Session Expires Mode	**Supported** This is required for calls extending beyond 300 seconds while 'on hold' if a client does not have Music on Hold enabled.
SBC Remote Early Media RTP	**Delayed** This is required because when Lync Server 2013 sends a SIP 18x response, it does not immediately send 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 4-15: Configuring IP Profile for Lync Server 2013



b. Click **Submit**.

Notes:
The *GenerateSRTPKeys* parameter currently cannot be configured through the Web-based management tool. You should therefore use the *ini* configuration file as follows:

- After you complete the entire configuration, save it to an *ini* file (see Appendix A on page 101).
- Open the file and search for "IpProfile 1".
- For this IP Profile, set the *IpProfile_GenerateSRTPKeys* parameter to **1**. This value is located at the end of the line for this specific load (i.e., semicolon): "-1, 1, 0, 1, 0, 1, 1;"
- Save the file and load it to the device.

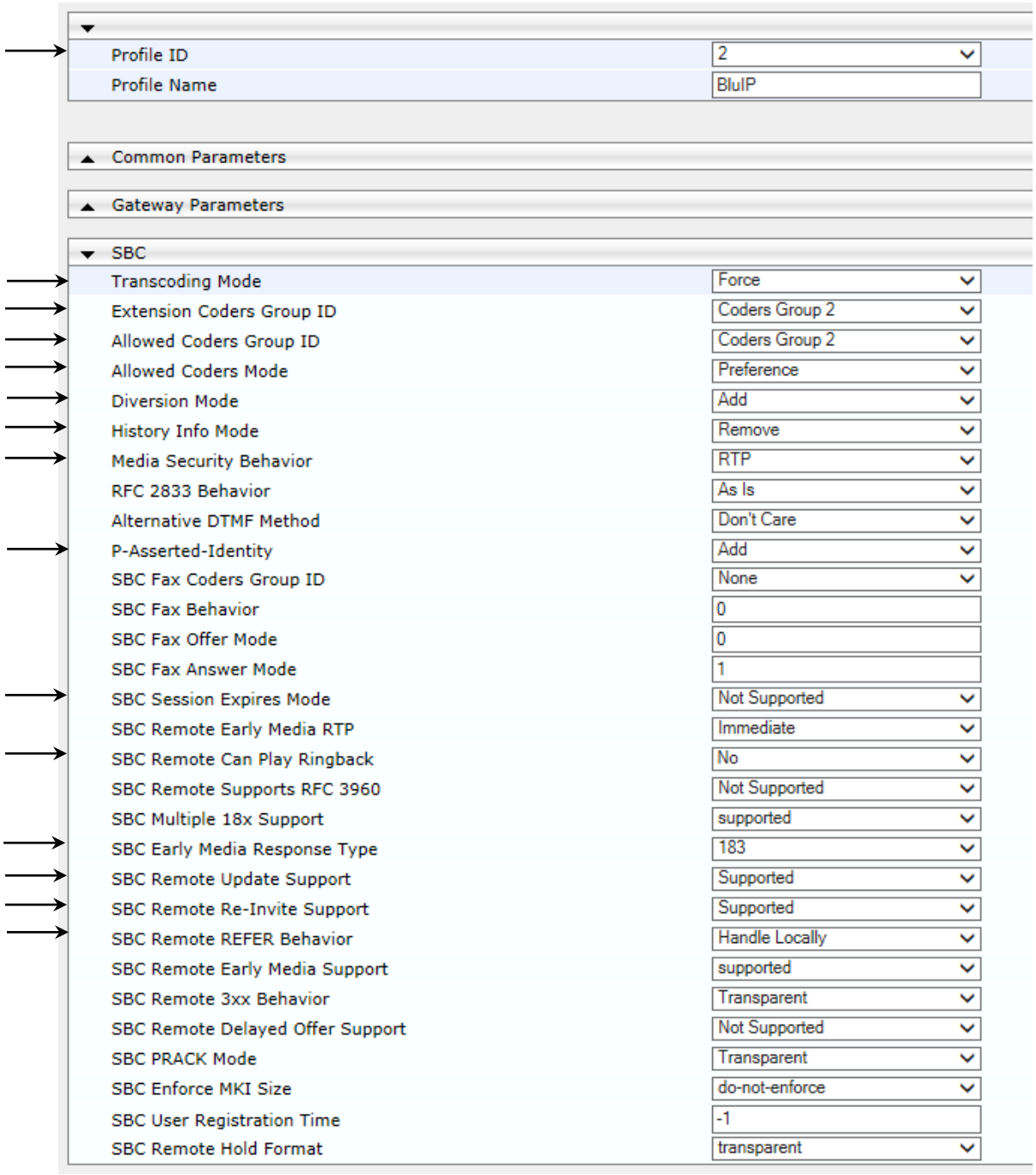
3. Add an IP Profile for the BluIP service:

a. Configure the parameters as follows:

Parameter	Settings
Profile ID	**2**
Transcoding Mode	**Force**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Preference** This enables the received SDP offer to list Allowed coders first.
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 BluIP.
History Info Mode	**Remove** This is utilized on a forward from Lync Server 2013 and is removed when sending to BluIP.
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** This is required for all calls. Additional manipulation is performed to set the main trunk group number within the PAI as required by BluIP.
SBC Session Expires Mode	**Not Supported** BluIP removes Session Timer Header from all messages traversing the network.
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**

Parameter	Settings
SBC Remote Update Support	**Supported** During long calls when the session timer expires and the MS Lync environment initiates a Session Update, the message will transverse the SBC and be sent to the BluIP network which allows the call to stay up. Session timer must be less than 300 ms.
SBC Remote Re-INVITE Support	**Supported**
SBC Remote REFER Behavior	**Handle Locally** E-SBC handles the incoming REFER request itself without forwarding the REFER towards the SIP Trunk.

Figure 4-16: Configuring IP Profile for BluIP Service

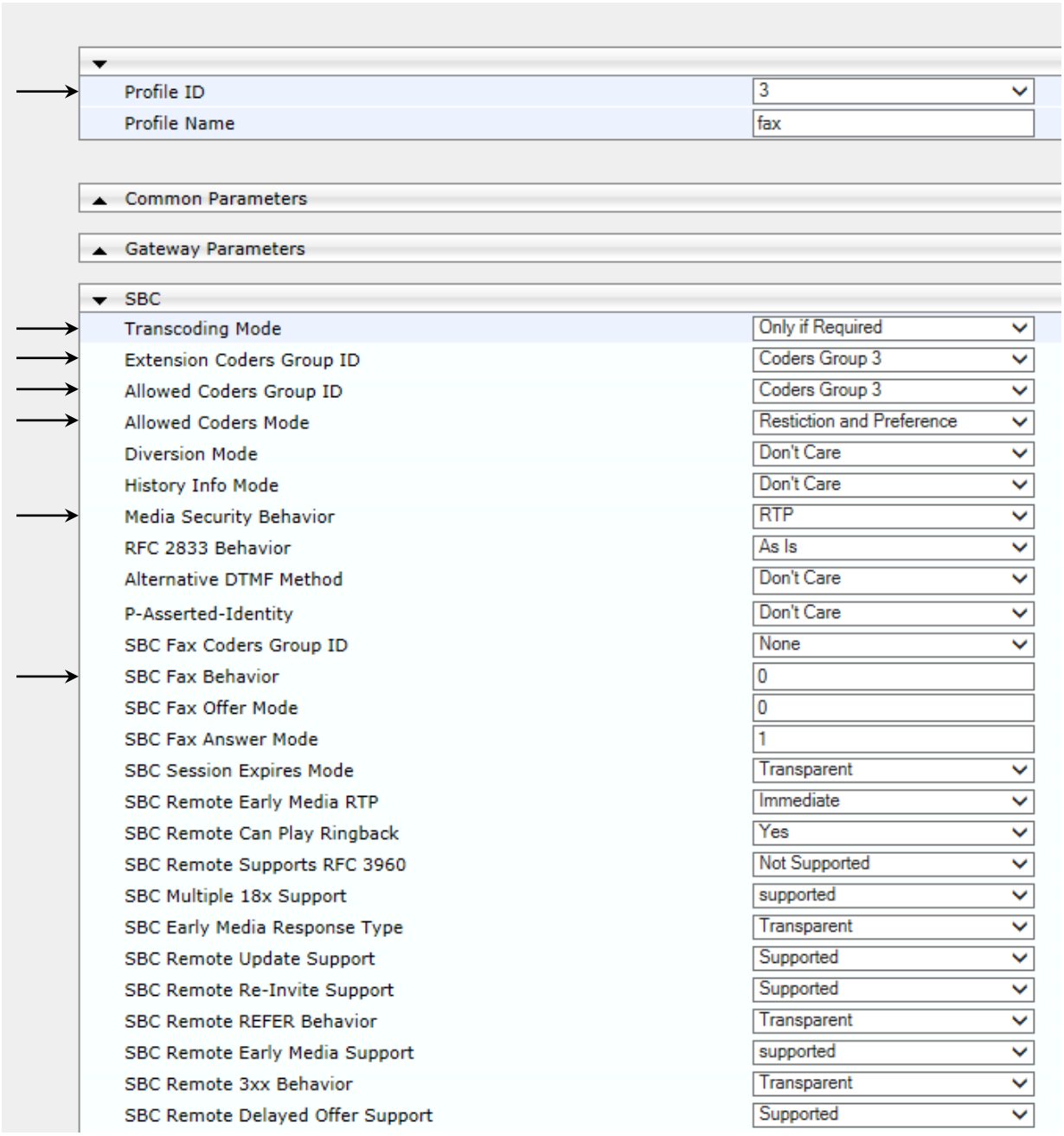


b. Click **Submit**.

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 3**
Allowed Coders Group ID	**Coders Group 3**
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 4-17: Configuring IP Profile for Fax Supporting ATA



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 BluIP 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 BluIP service.

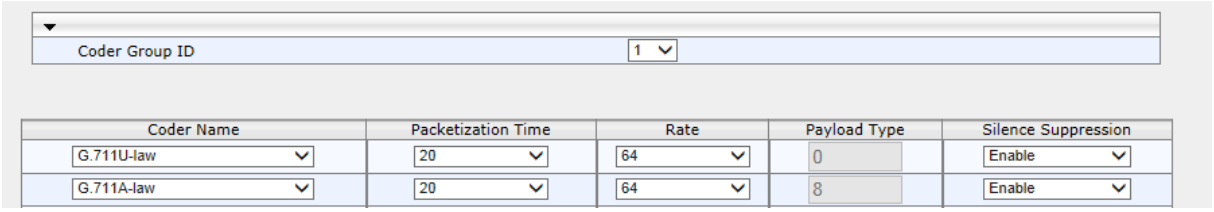
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step.

➢ **To configure coders:**

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

Parameter	Settings
Coder Group ID	**1**
Coder Name	**G.711 U-law**
Coder Name	**G.711 A-law**
Silence Suppression	**Enable**

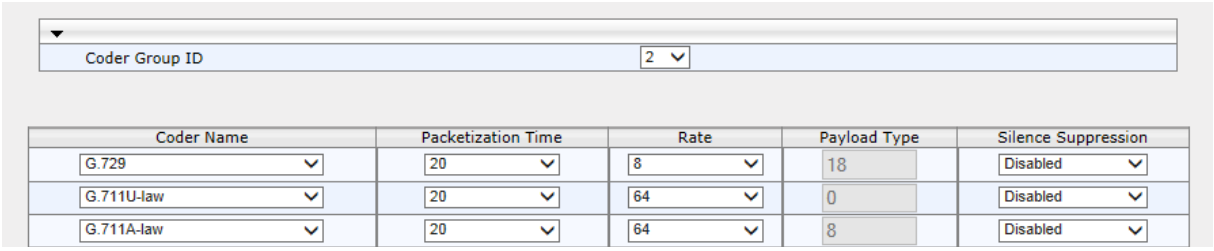
Figure 4-18: Configuring Coders for Lync Server 2013



   b. Click **Submit**.
2. Add a Coder Group for BluIP service:
   a. Configure the parameters as follows:

Parameter	Settings
Coder Group ID	**2**
Coder Name	**G.729**
Coder Name	**G.711 U-law**
Coder Name	**G.711 A-law**
Silence Suppression	**Disabled**

Figure 4-19: Configuring Coders for BluIP Service

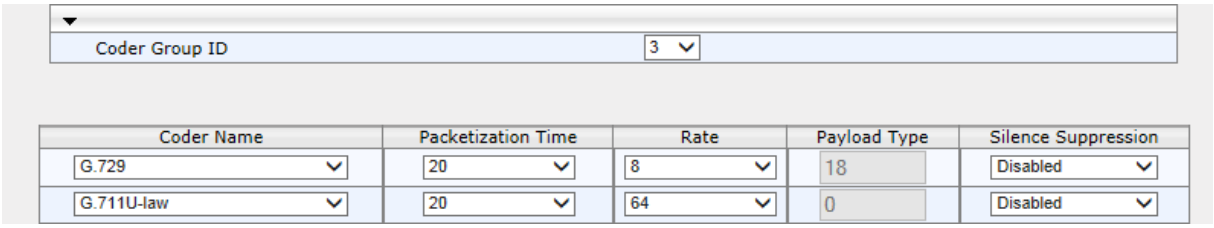


   b. Click **Submit**.

3. Add a Coder Group for FAX ATA device:
   a. Configure the parameters as follows:

Parameter	Settings
Coder Group ID	**3**
Coder Name	**G.729**
Coder Name	**G.711 U-law**
Silence Suppression	**Disabled**

Figure 4-20: Configuring Coders for Fax ATA Device



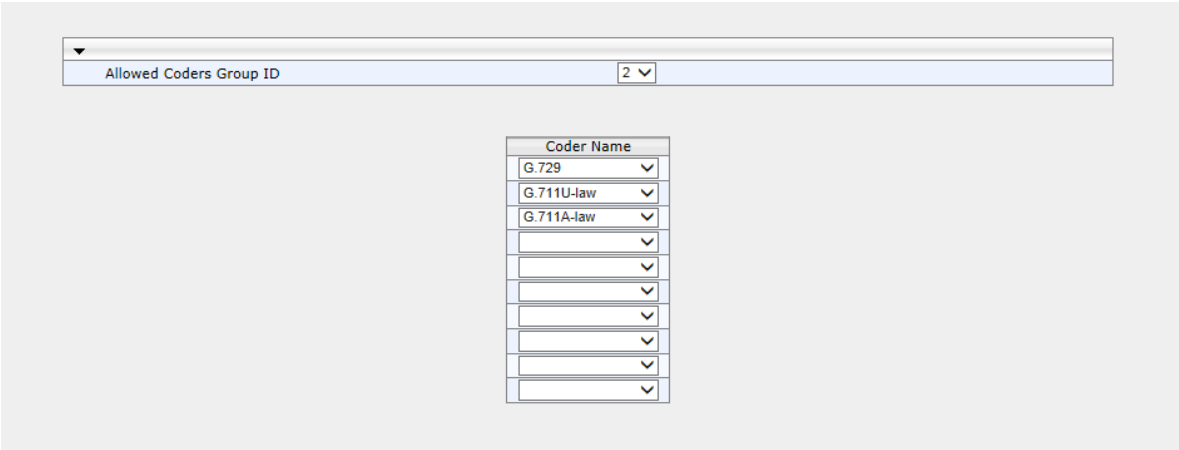
   b. Click **Submit**.

The procedure below adds an Allowed Coders Group to ensure that voice sent to the BluIP 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 BluIP service in the previous step.

➢ **To set a preferred coder for the BluIP service:**

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

Figure 4-21: Setting Preferred Coder for BluIP Service

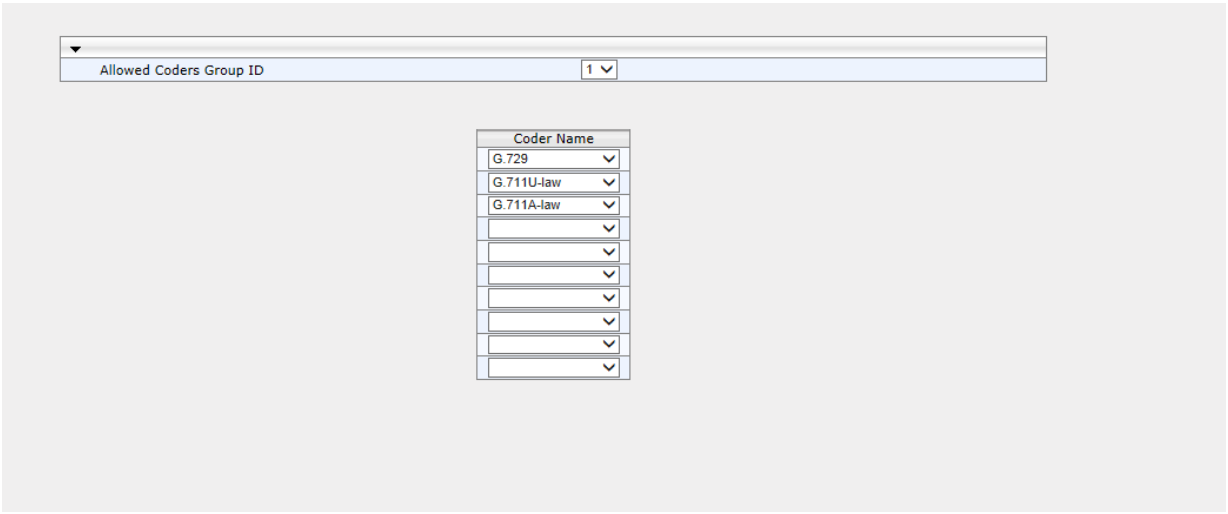


2. From the 'Allowed Coders Group ID' drop-down list, select **2**.
3. From the 'Coder Name' drop-down list, select **G.729**.
4. From the 'Coder Name' drop-down list, select **G.711 U-Law**.
5. From the 'Coder Name' drop-down list, select **G.711 A-Law**.
6. Click **Submit**.

➢ **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

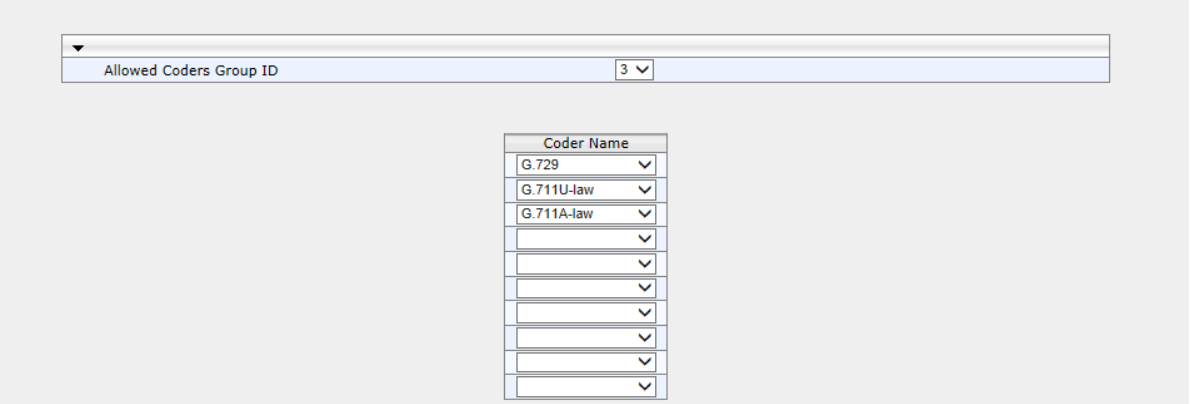


2. From the 'Allowed Coders Group ID' drop-down list, select **1**.
3. From the 'Coder Name' drop-down list, select **G.729, G.711 U-law, and G711 A-law**.
4. Click **Submit**.

➢ **To set a preferred coder for the Fax ATA device:**

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

Figure 4-23: Setting Preferred Coder for Fax ATA device



2. From the 'Allowed Coders Group ID' drop-down list, select **3**.
3. From the 'Coder Name' drop-down list, select **G.729**, **G.711 U-law**, and **G711 A-law**.
4. Click **Submit**.

4.8 Step 8: SIP TLS Connection Configuration

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

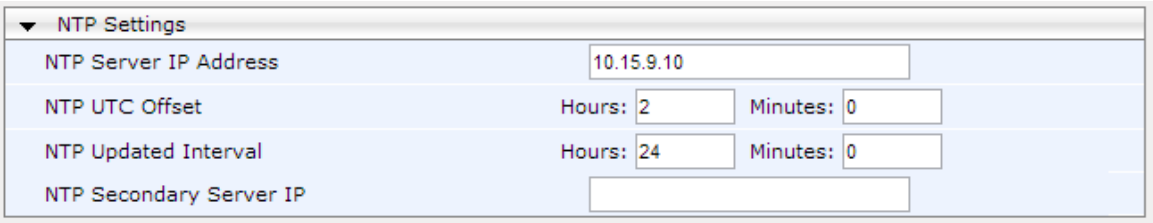
4.8.1 Step 8a: Configure the NTP Server Address

This step shows 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**).

Figure 4-24: 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 shows 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.

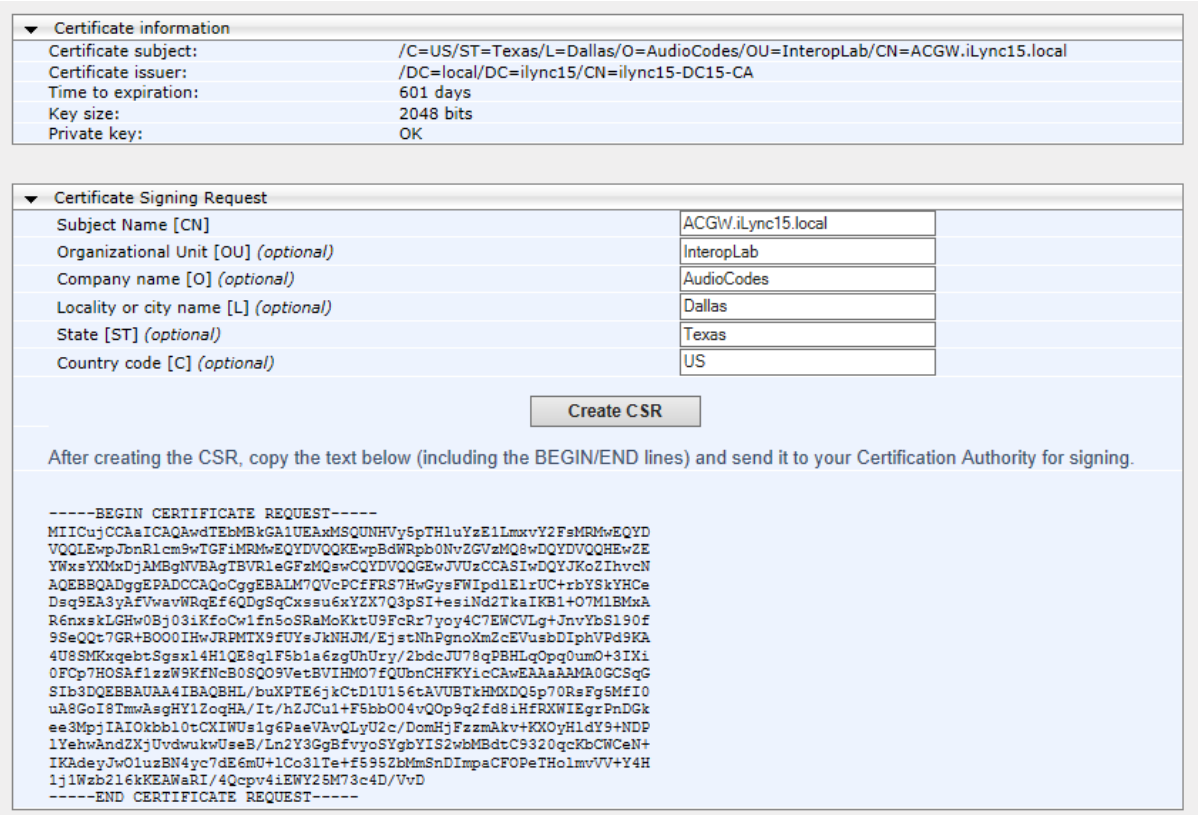
It consists of the following steps:

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**).

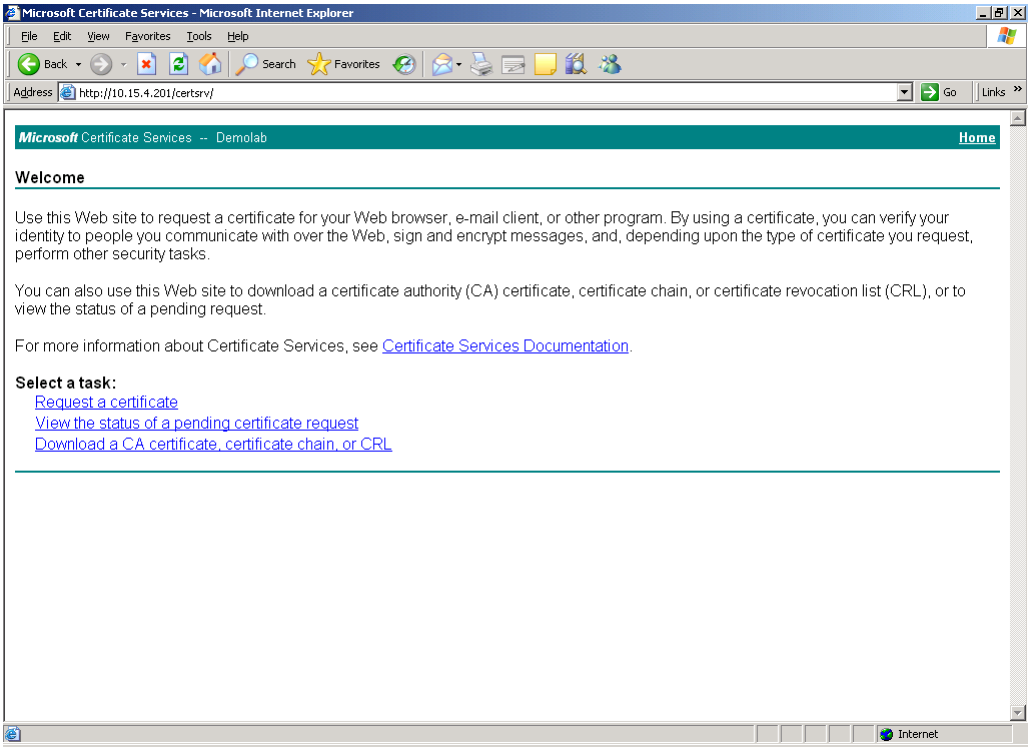
Figure 4-25: Configuring Certificates



2. In the 'Subject Name' field, enter the media gateway name (e.g., **ACGW.iLync15.local**). This name must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 17).
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*.

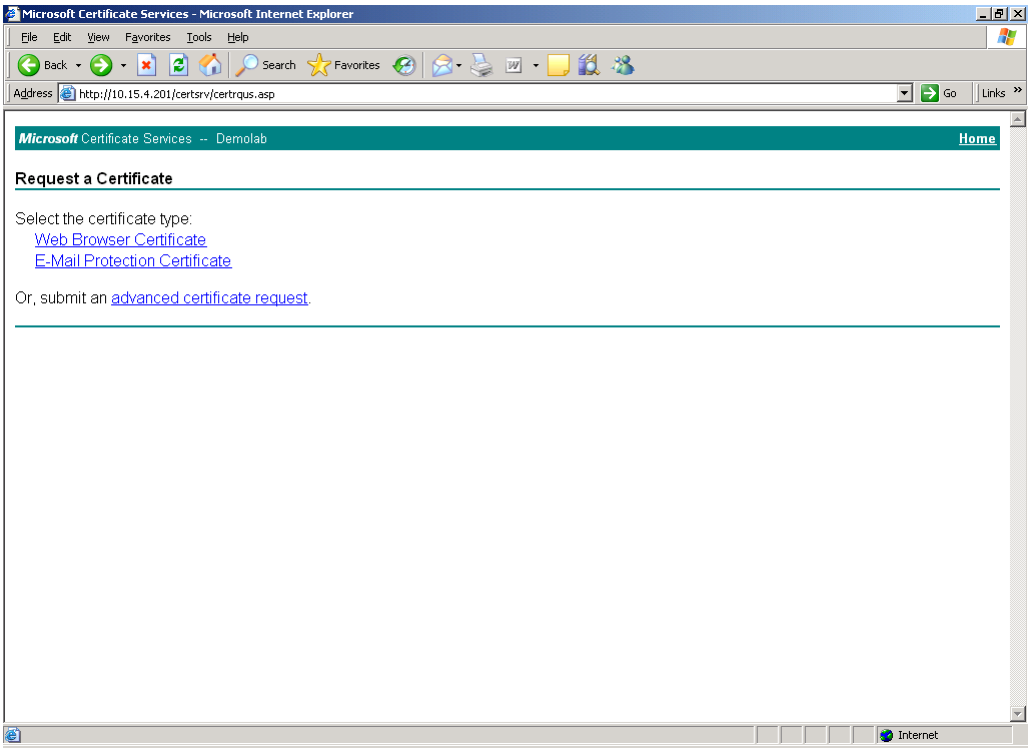
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-26: Navigating to Microsoft Certificate Services Web Site



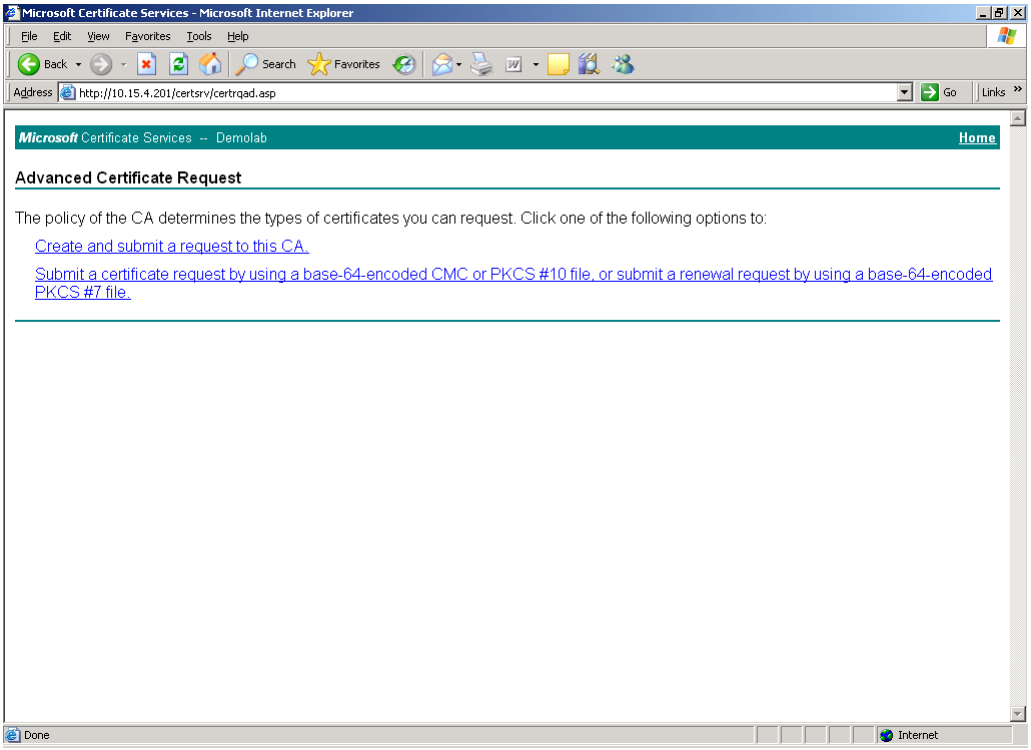
6. Click **Request a certificate**.

Figure 4-27: Requesting a Certificate



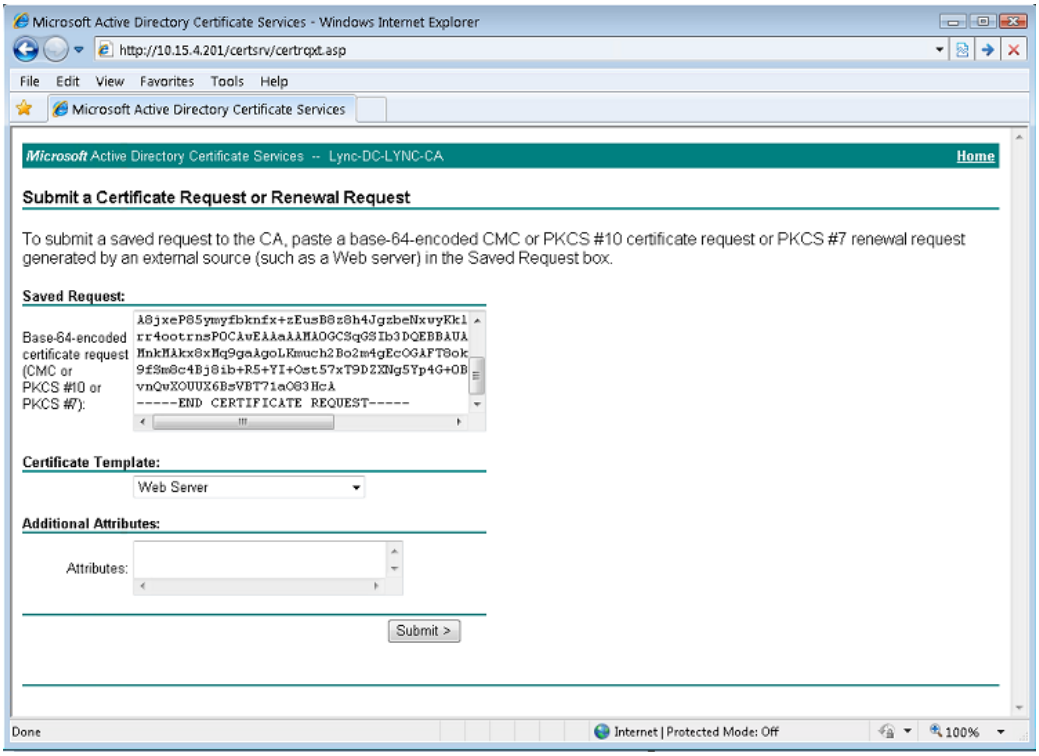
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-28: Selecting Advanced Certificate Request



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

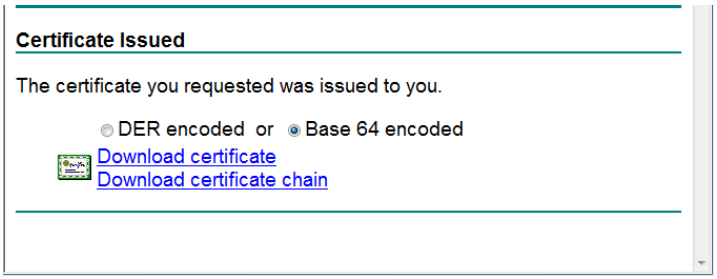
Figure 4-29: Submitting a Certificate Request



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.

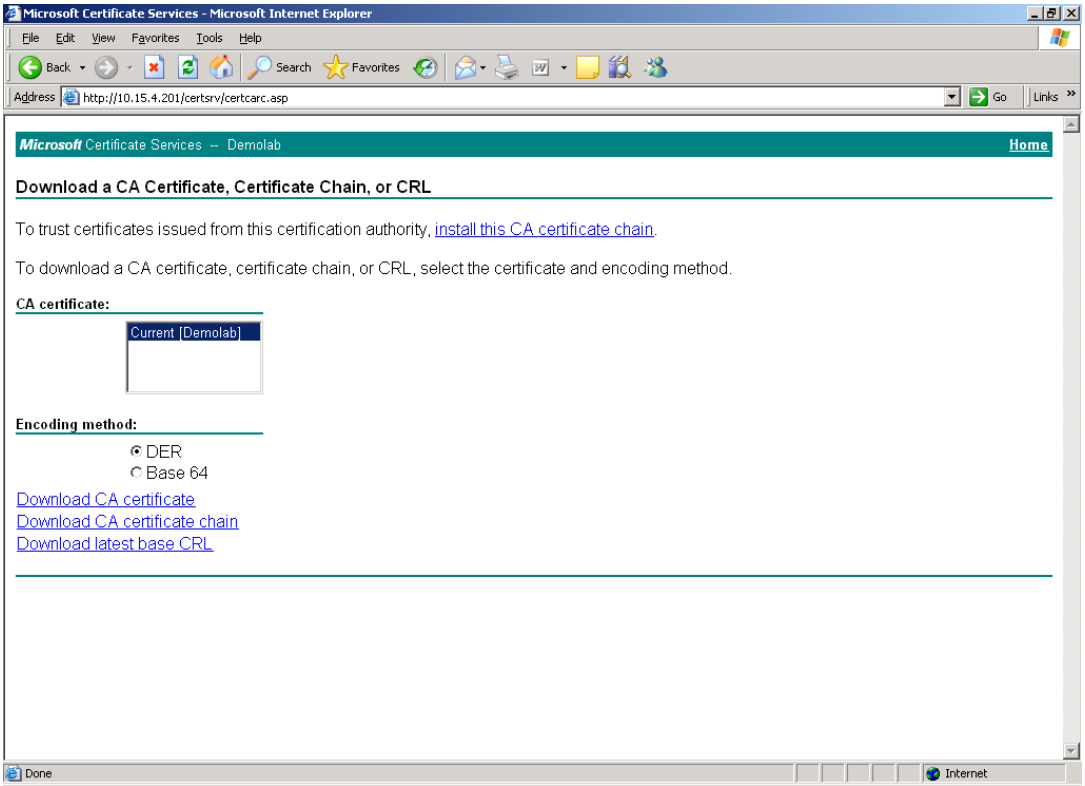
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-30: 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 4-31: 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 4-32: Uploading Certificate

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 1 on page 100).

4.9 Step 9: Configure SRTP

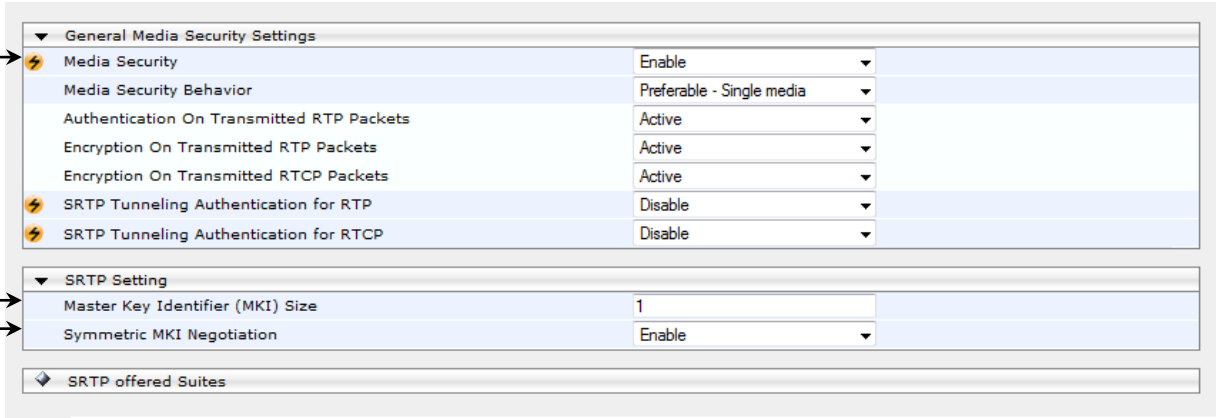
This step shows how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), you need to configure the E-SBC to operate in the same manner.

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 50).

➢ **To configure media security:**

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

Figure 4-33: 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 4.16 1 on page 100).

4.10 Step 10: Configure Number of Media Channels

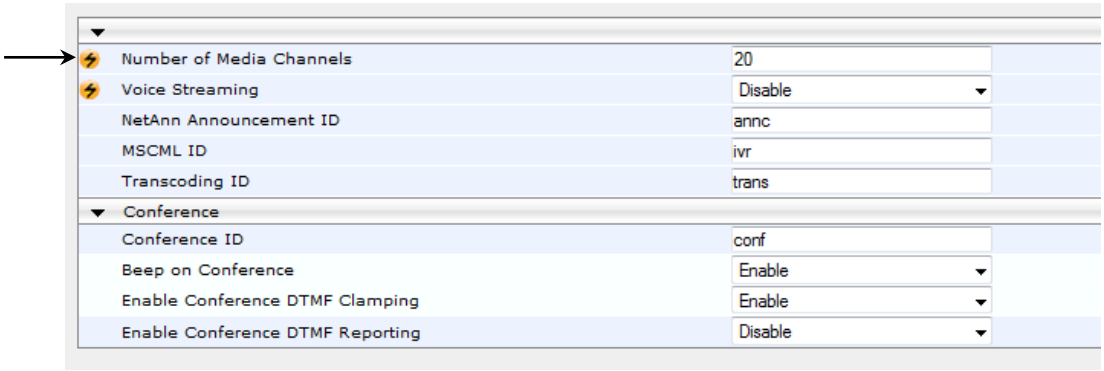
This step shows how to configure the number of media channels for IP-based media. To perform coder transcoding, define digital signaling processors (DSP) channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to sessions.

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 4-34: 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 shows how to configure IP-to-IP call routing rules (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 the example scenario, you need to add the following IP-to-IP routing rules to route calls between Lync Server 2013 (LAN) and BluIP 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
- Calls from LAN to WAN.
- Calls from WAN to Fax supporting LAN ATA.
- Calls from WAN to LAN.
- Calls from LAN ATA to WAN.

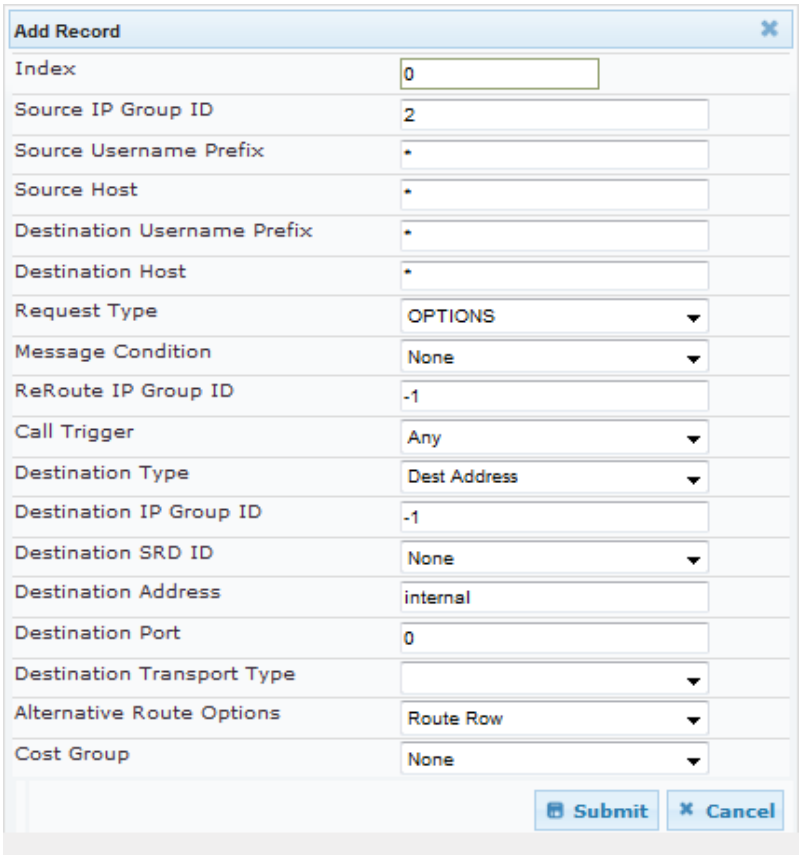
The routing rules use IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 48, IP Group ID 1 was assigned to Lync Server 2013, IP Group ID 2 to BluIP service, and IP Group ID 3 to the Fax supporting ATA.

➢ **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**

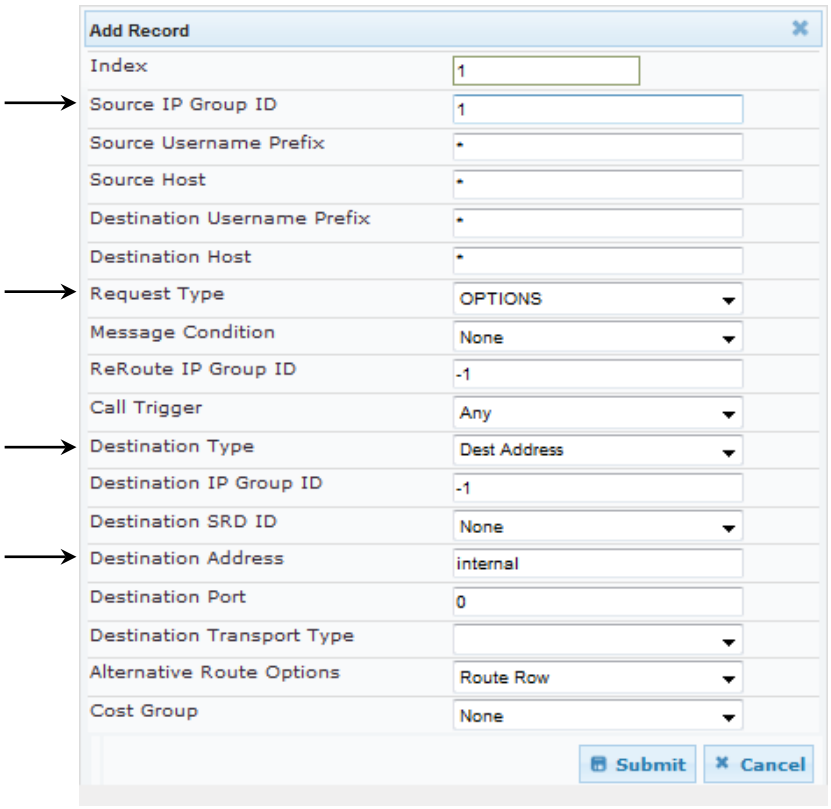
Figure 4-35: Configuring IP-to-IP Routing Rules



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**

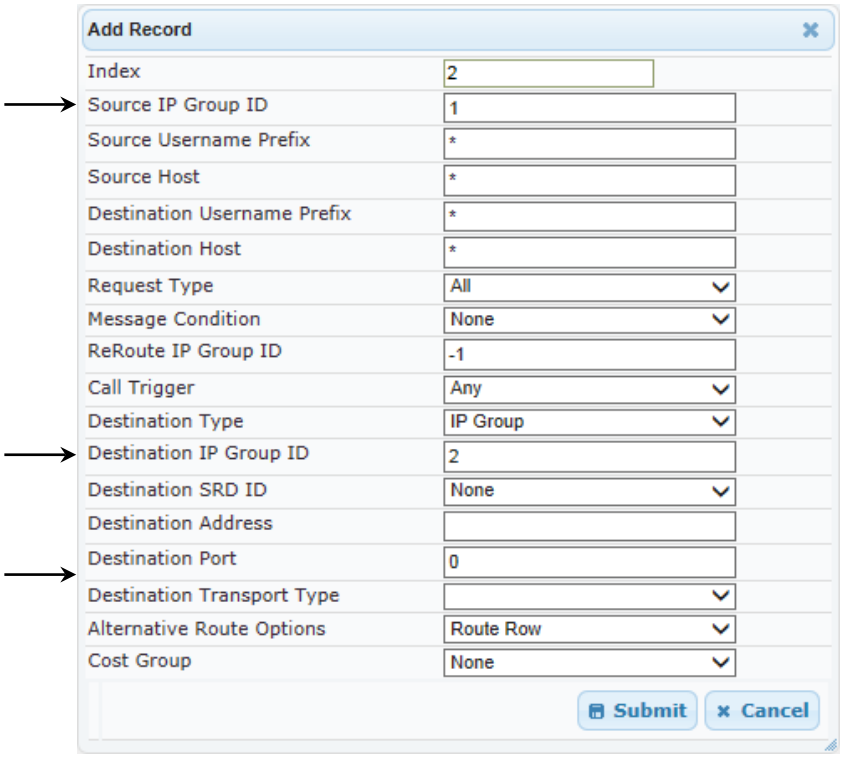
Figure 4-36: Adding Rule to Terminate SIP Options from LAN



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

Parameter	Settings
Index	**2**
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

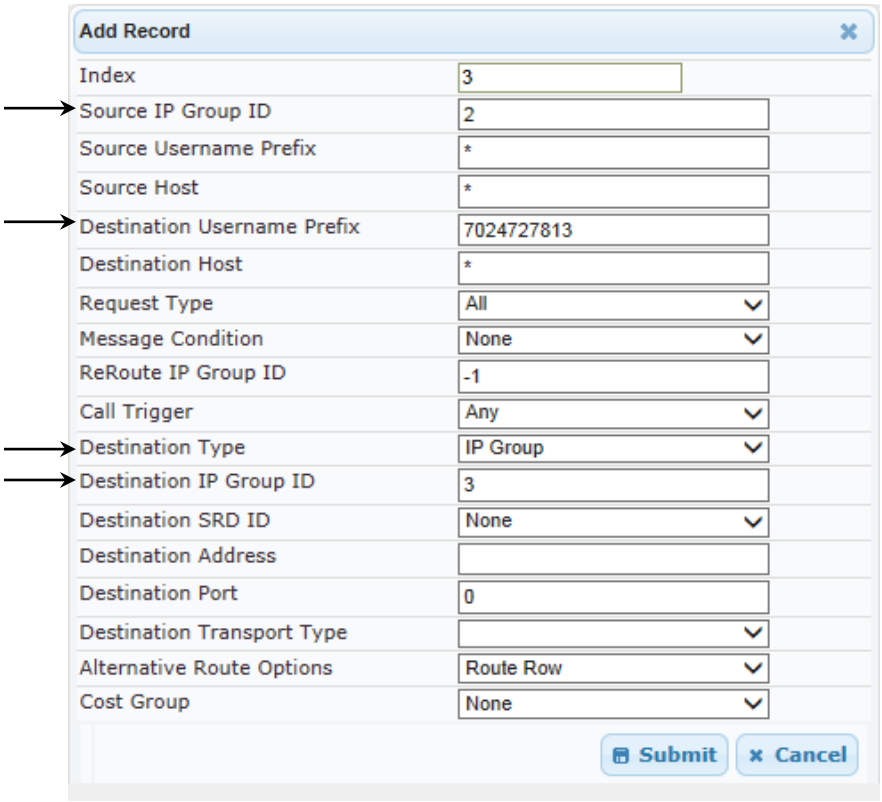


   c. Click **Submit**.

5. 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	**3**
Source IP Group ID	**2**
Destination Username Prefix	**7024727813** (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

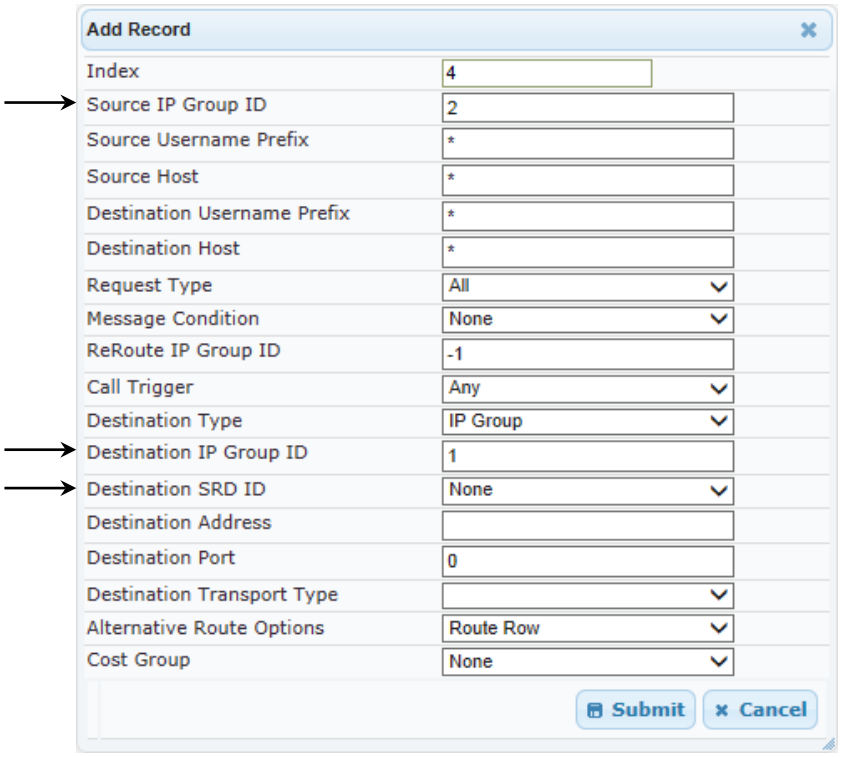


   c. Click **Submit**.

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

Parameter	Settings
Index	**4**
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

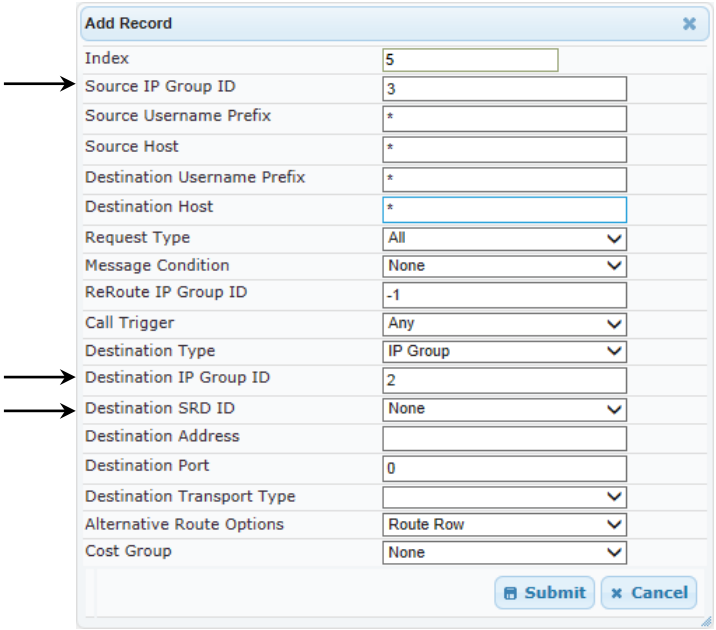


   c. Click **Submit**.

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

Parameter	Settings
Index	**5**
Source IP Group ID	**3**
Destination Type	**IP Group**
Destination IP Group ID	**2**

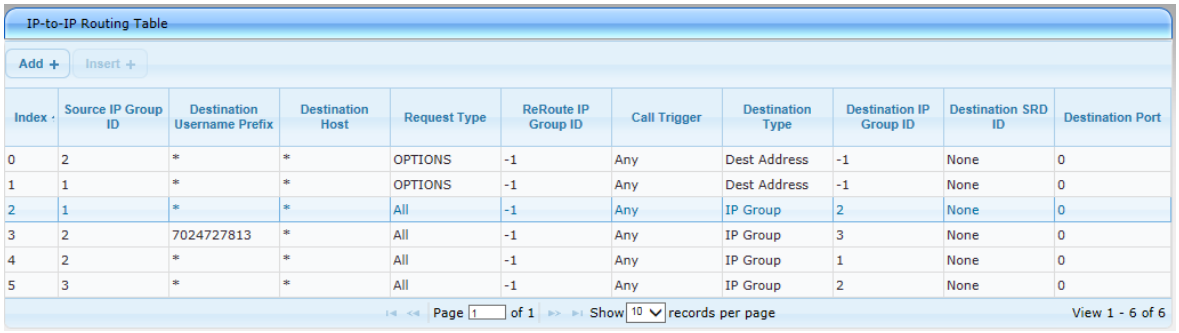
Figure 4-40: Configuring IP-to-IP Routing Rule for WAN to LAN



   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	1	*	*	All	-1	Any	IP Group	2	None	0
3	2	7024727813	*	All	-1	Any	IP Group	3	None	0
4	2	*	*	All	-1	Any	IP Group	1	None	0
5	3	*	*	All	-1	Any	IP Group	2	None	0

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

4.12 Step 12: Configure IP-to-IP Manipulation

This step shows 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 48, IP Group ID 1 was assigned to Lync Server 2013, IP Group ID 2 to the BluIP service, and IP Group ID 3 to the Fax supporting ATA.

Note: Adapt the manipulation table according to your 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.

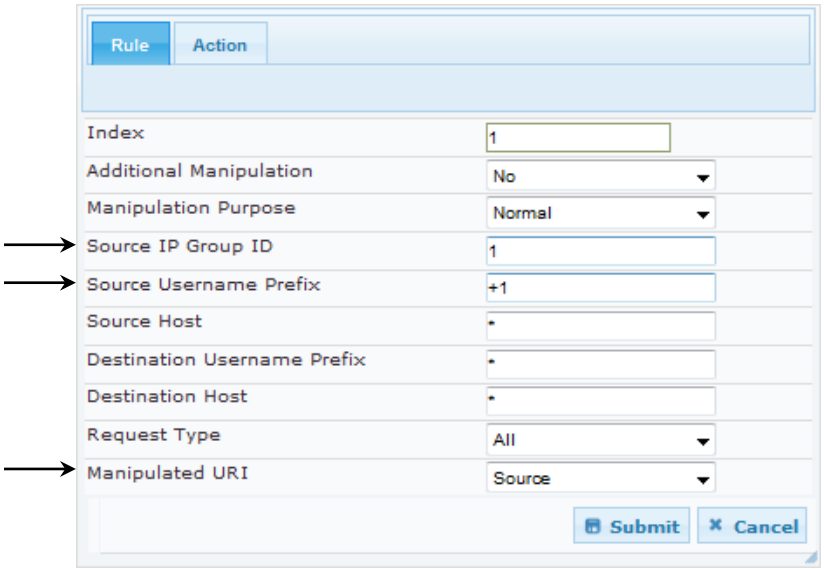
The procedure below provides an example of configuring a manipulation rule that adds the plus "+1" to the destination number for calls from IP Group 2 (BluIP service) destined to IP Group 1 (i.e., Lync Server 2013).

➢ **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**

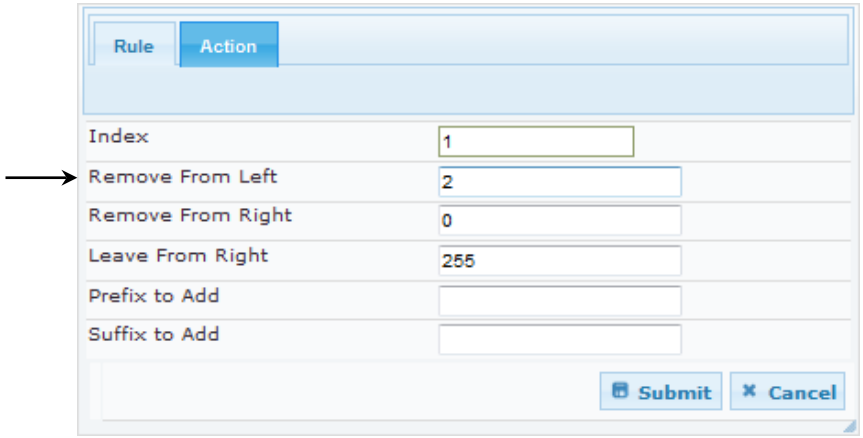
Figure 4-42: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Remove from Left	**2**

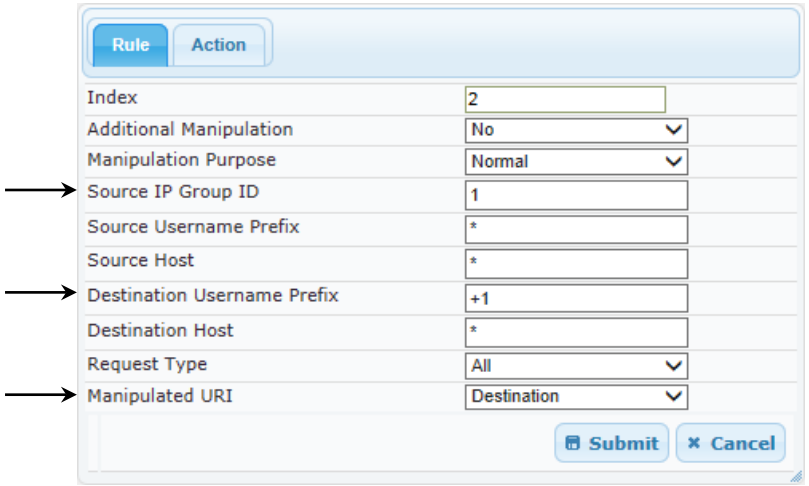
Figure 4-43: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



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	**1**
Destination Username Prefix	**+1**
Manipulated URI	**Destination**

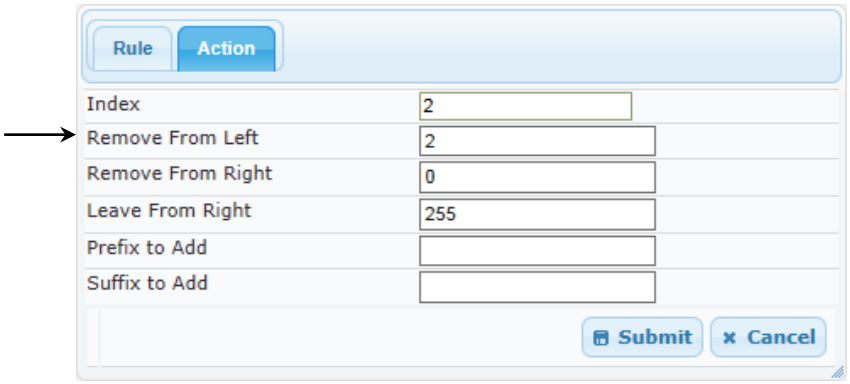
Figure 4-44: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Remove From Left	**2**

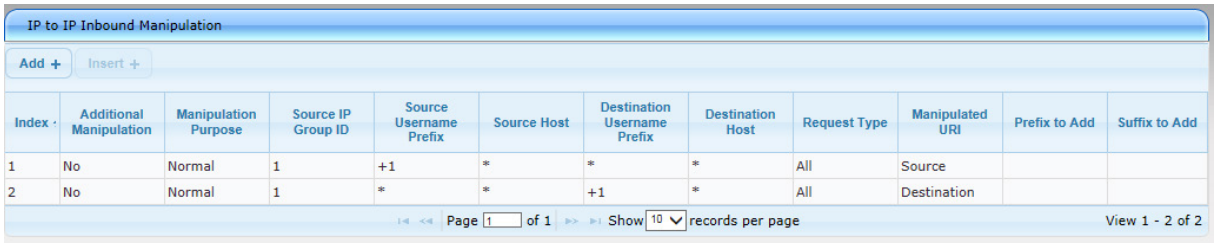
Figure 4-45: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



9. 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., BluIP service):

Figure 4-46: 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 1 that have a prefix destination number of "+1", remove "+1" from this prefix.

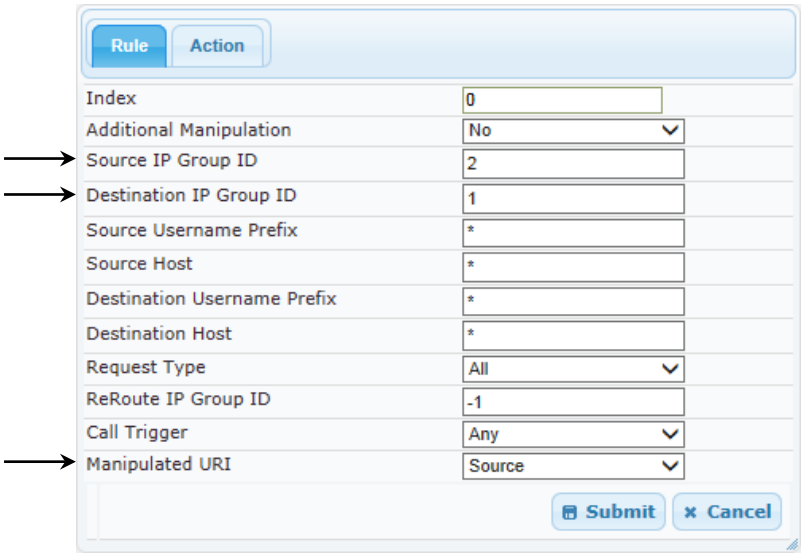
The procedure below provides an example of configuring a manipulation rule that adds the plus "+1" to the destination number for calls from IP Group 2 (BluIP service) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number ("*").

➢ **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	**0**
Source IP Group ID	**2**
Destination IP Group ID	**1**
Manipulated URI	**Source**

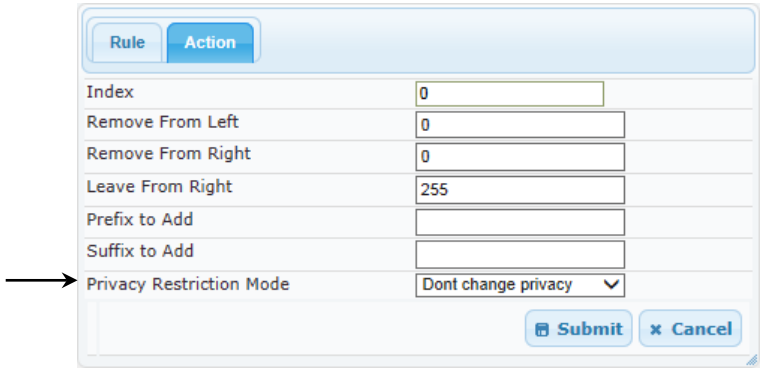
Figure 4-47: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Privacy Restriction Mode	**Don't change privacy.** This is done for normalization handling. Presentation Restricted calls are presented to the Lync 2013 environment in the "Anonymous" manner. See User Manual for further details.

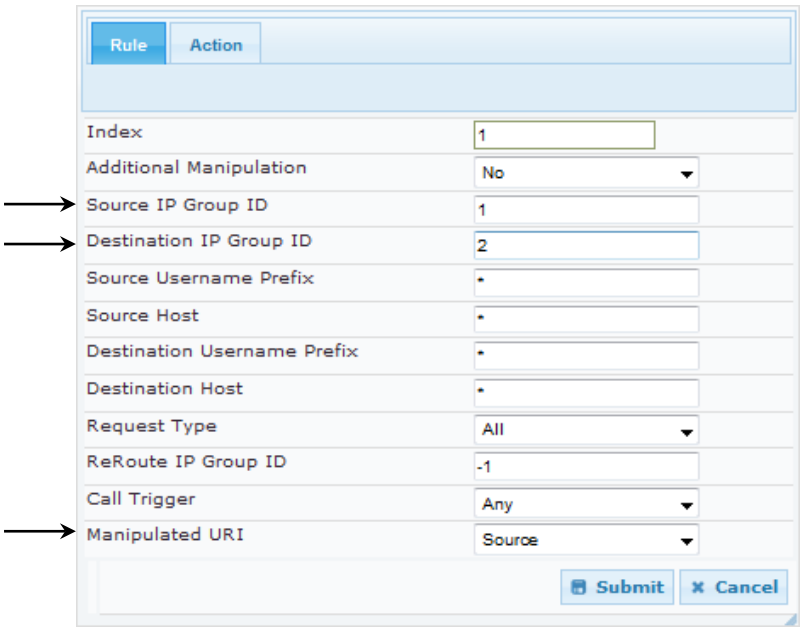
Figure 4-48: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



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

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

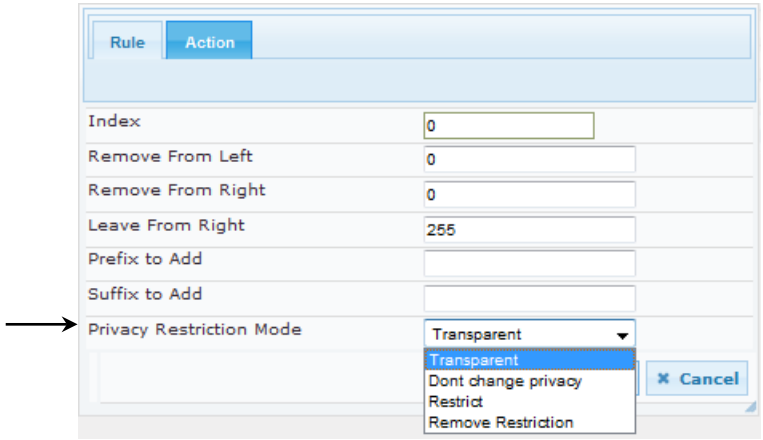
Figure 4-49: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Privacy Restriction Mode	**Transparent**, **Restrict** or **Remove Restriction**. Select **Remove Restriction** for unrestricted presentation. Select **Transparent** as presented by Lync 2013.

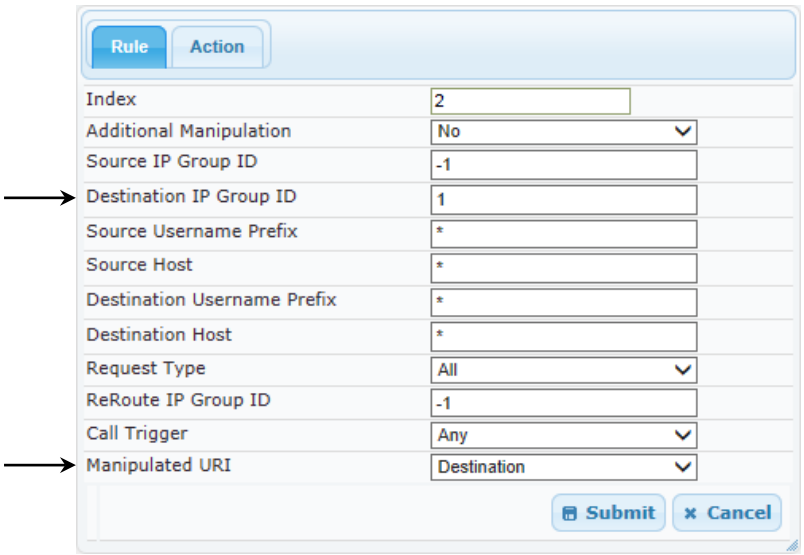
Figure 4-50: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



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

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

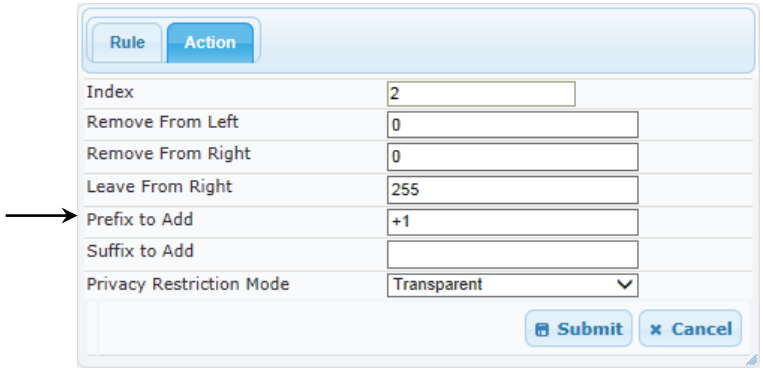
Figure 4-51: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Settings
Prefix to Add	**+1**

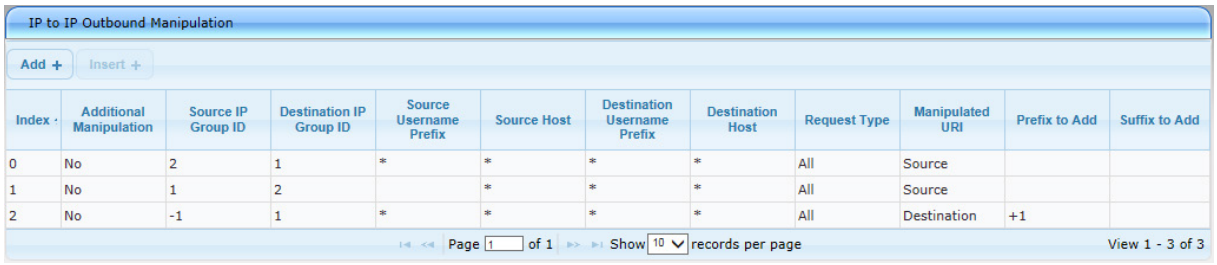
Figure 4-52: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



11. 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., BluIP service):

Figure 4-53: Configuring IP to IP Outbound Manipulation Rules



Rule Index	Description
0	The privacy settings for calls received from BluIP (IP Group 2) and sent to Lync 2013, are not changed (the user identity remains the same as in the incoming SIP dialog). If a restricted call scenario exists, the restricted presentation is normalized as follows: • From URL header: *anonymous@anonymous.invalid* • If a P-Asserted-Identity header exists (either in the incoming SIP dialog or added by the device), a Privacy header is added with the value "id"
1	Calls received from IP Group 1 with a destination of IP Group 2, manipulate the Privacy Restriction Mode. This example can apply to all source numbers but may be refined to reflect a specific DID. See the *User's Manual* for further details.
2	Calls with a destination of IP Group 1, manipulate the Destination to add a prefix of '+1". This example can apply to all destination numbers but may be refined to reflect a specific DID or a range of DIDs. See the *User's Manual* for further details.

4.13 Step 13: Configure SIP Message Manipulation Rules

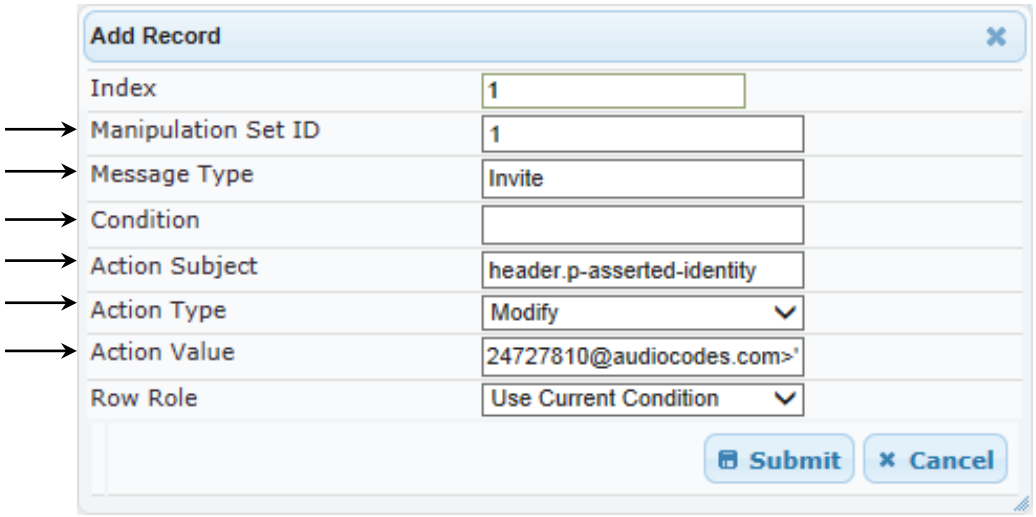
This step shows how to configure SIP message manipulation rules in the Message Manipulations table. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. After configuring the SIP message 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.

➢ **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 1:

Rule Index	Setting
Index	**1**
Manipulation Set ID	**1**
Message Type	**Invite**
Condition	
Action Subject	**header.p-asserted-identity**
Action Type	**Modify**
Action Value	**'<sip:7024727810@audiocodes.com>'**

Figure 4-54: Configuring SIP Message Manipulation – Index 1

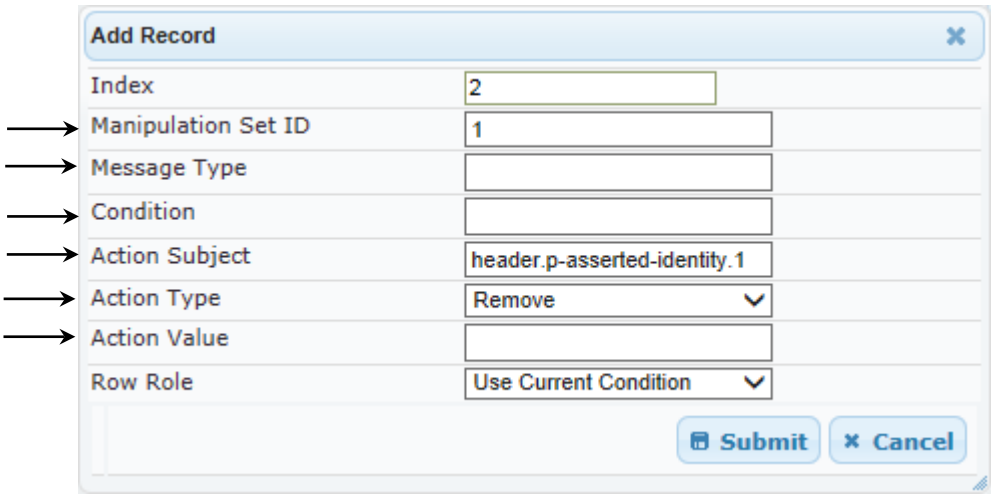


➢ **To configure SIP message manipulation rule for Index 2:**

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 1:

Rule Index	Setting
Index	**2**
Manipulation Set ID	**1**
Message Type	
Condition	
Action Subject	**header.p-asserted-identity.1**
Action Type	**Remove**
Action Value	

Figure 4-55: Configuring SIP Message Manipulation – Index 2

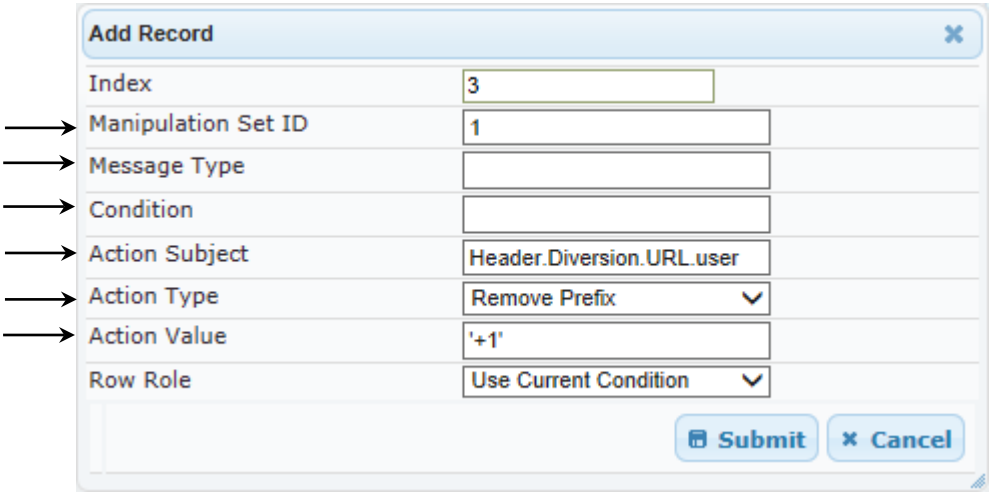


➢ **To configure SIP message manipulation rule for Index 3:**

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 1:

Rule Index	Setting
Index	**3**
Manipulation Set ID	**1**
Message Type	
Condition	
Action Subject	**Header.Diversion.URL.user**
Action Type	**Remove Prefix**
Action Value	**'+1'**
Row Role	**Use Current Condition**

Figure 4-56: Configuring SIP Message Manipulation – Index 3

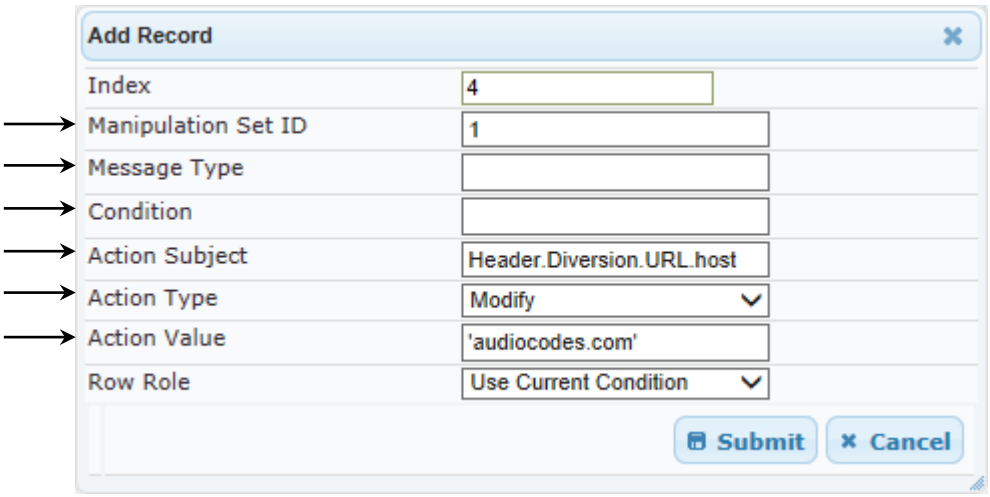


➢ **To configure SIP message manipulation rules for Index 4:**

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 1:

Rule Index	Setting
Index	**4**
Manipulation Set ID	**1**
Message Type	
Condition	
Action Subject	**Header.Diversion.URL.host**
Action Type	**Modify**
Action Value	**'audiocodes.com'**

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

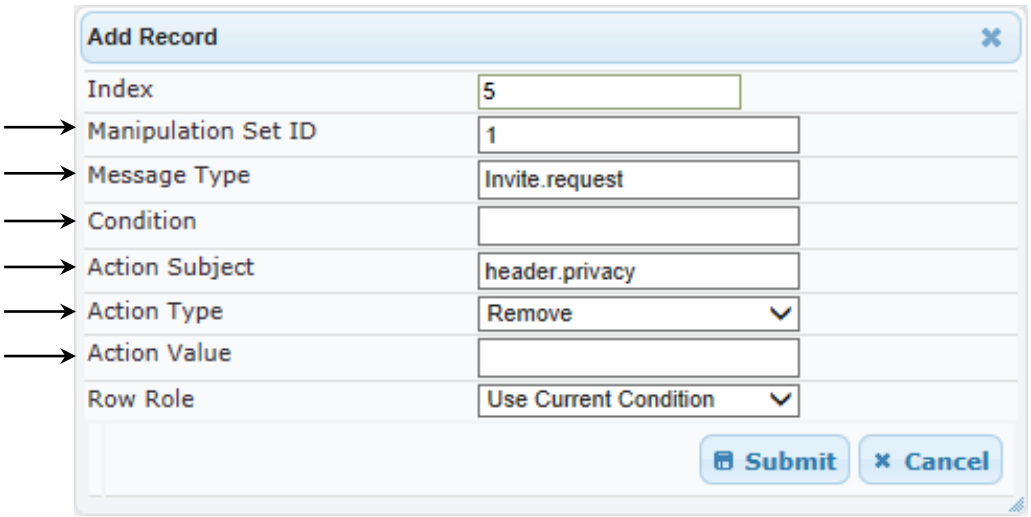


➢ **To configure SIP message manipulation rule for Index 5:**

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 1:

Rule Index	Setting
Index	**5**
Manipulation Set ID	**1**
Message Type	**Invite.request**
Condition	
Action Subject	**header.privacy**
Action Type	**Remove**
Action Value	

Figure 4-58: Configuring SIP Message Manipulation – Index 5

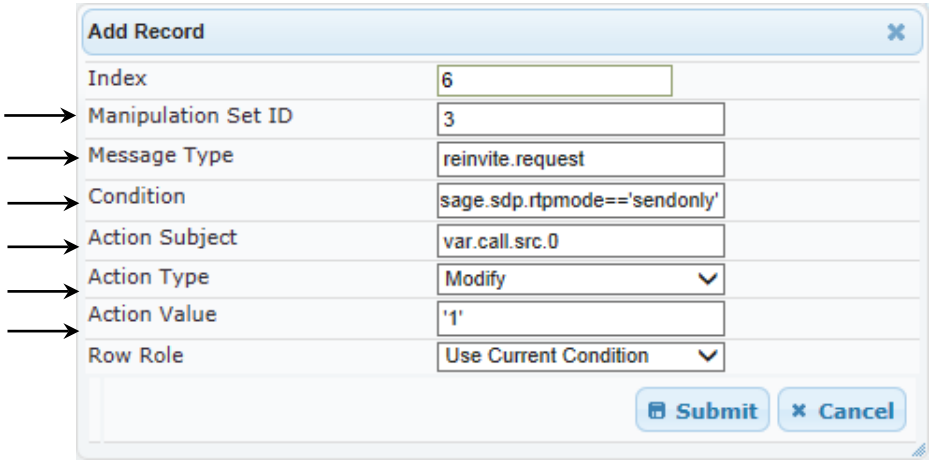


➢ **To configure SIP message manipulation rules for Index 6:**

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 3:

Rule Index	Setting
Index	**6**
Manipulation Set ID	**3**
Message Type	**reinvite.request**
Condition	**param.message.sdp.rtpmode=='sendonly'**
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'1'**
Row Role	**Use Current Condition**

Figure 4-59: Configuring SIP Message Manipulation – Index 6

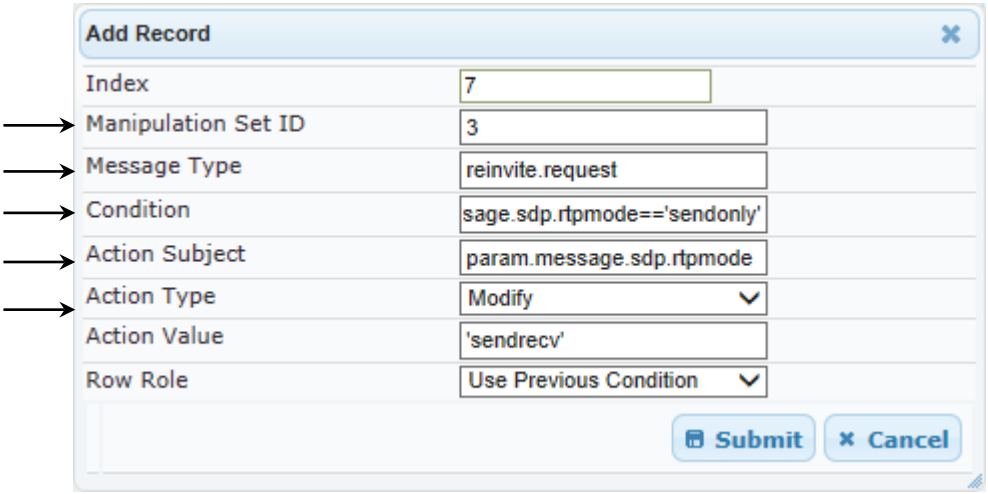


➢ **To configure SIP message manipulation rule for Index 7:**

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 3:

Rule Index	Setting
Index	**7**
Manipulation Set ID	**3**
Message Type	**reinvite.request**
Condition	**param.message.sdp.rtpmode=='sendonly'**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**'sendrecv'**
Row Rule	**Use Previous Condition**

Figure 4-60: Configuring SIP Message Manipulation – Index 7

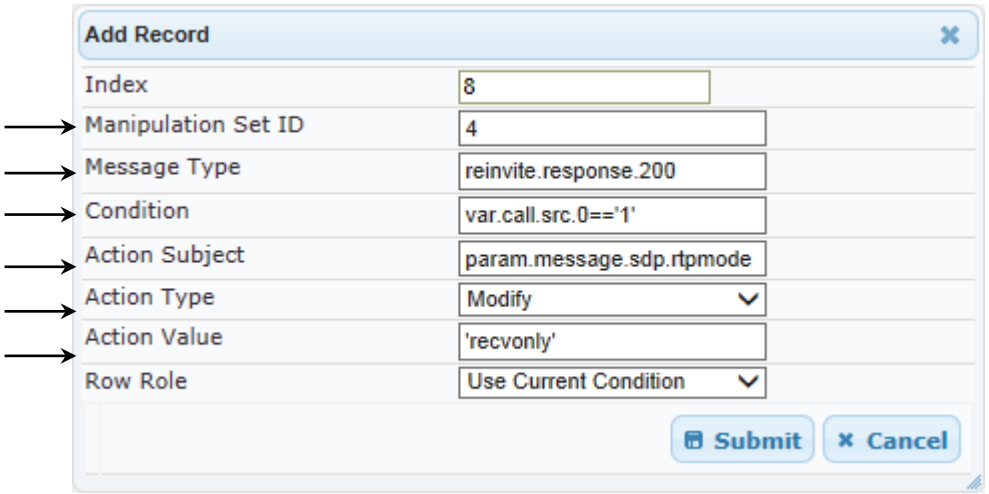


➢ **To configure SIP message manipulation rule for Index 8:**

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 4:

Rule Index	Setting
Index	**8**
Manipulation Set ID	**4**
Message Type	**reinvite.response.200**
Condition	**var.call.src.0=='1'**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**'recvonly'**
Row Role	**Use Current Condition**

Figure 4-61: Configuring SIP Message Manipulation – Index 8

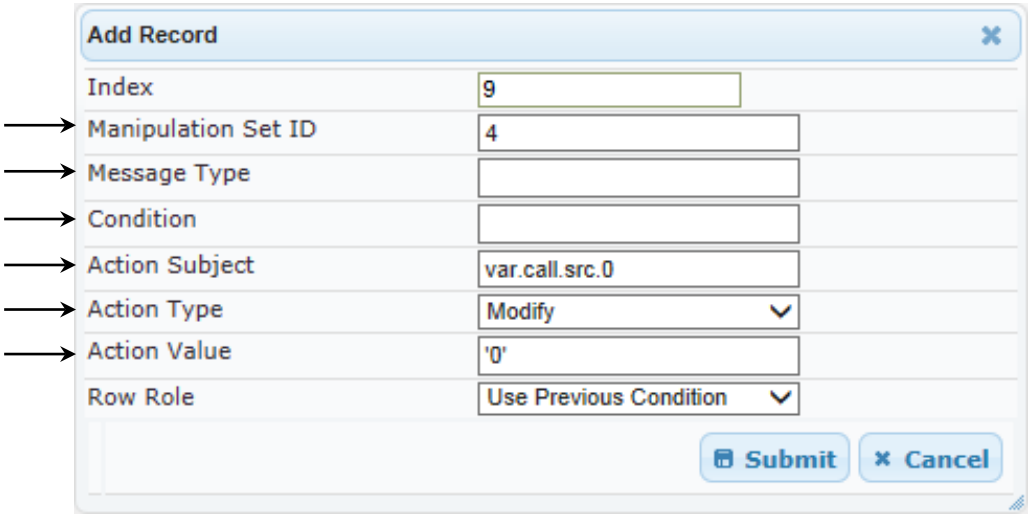


➢ **To configure SIP message manipulation rule for Index 9:**

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 4:

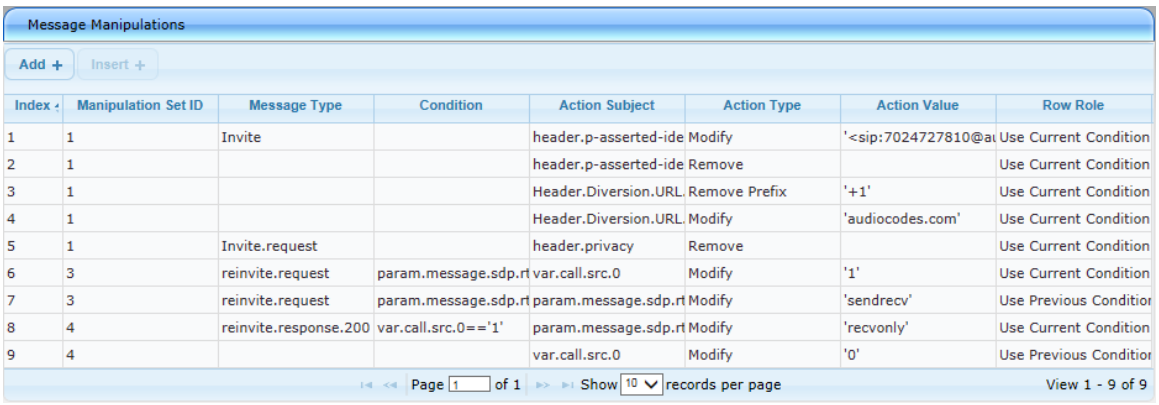
Rule Index	Setting
Index	**9**
Manipulation Set ID	**4**
Message Type	
Condition	
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'0'**
Row Rule	**Use Previous Condition**

Figure 4-62: Configuring SIP Message Manipulation – Index 10



The table displayed below includes SIP message manipulation rules bound together by common Manipulation Set IDs (Manipulation Set IDs 1, 3, and 4) executed for messages sent to and from the BluIP 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 items are dependent or related to the deployment while others are specifically required to enable correct interworking between BluIP service and Lync Server 2013. Some show specific interworking linkage which must be performed in specific order (Rule 7 is dependent on Rule 6 and Rule 9 is dependent on Rule 8). The specific items are needed to support Music on Hold, proper P-Asserted Identity header, and Host URL presentation. See the *User's Manual* for details on the full capabilities of header manipulation. The Manipulation Set IDs are indexed and utilized from within the IP Group table.

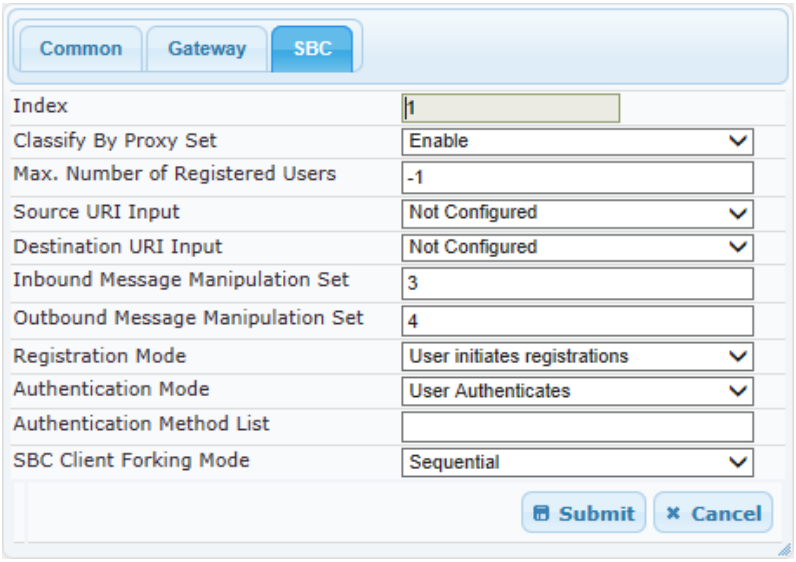
Figure 4-63: Configuring SIP Message Manipulation – Example



Rule Index	Description
1	SIP INVITE messages have the P-Asserted-Identity header modified to reflect the DID associated with the SIP trunk. This is required of BluIP. The user and the host must be associated with the SIP trunk. All calls must reflect the usage of the main line associated with the service.
2	A SIP INVITE message is received from Microsoft Lync 2013 and has the second P-Asserted Identity header removed prior to delivery to BluIP service. The original header is broken into two headers and the second portion is removed.
3	On all messages with a Diversion header present, remove the URL user prefix of '+1'.
4	On all messages with a Diversion header present, modify the URL host to reflect 'audiocodes.com'.
5	On all SIP INVITE messages which have the Privacy ID set for Restricted calls, remove the Privacy header. This is to support interworking in the manner in which BluIP utilizes their BroadSoft application server.
6	SIP re-INVITE messages that contain an RTP mode, within the SDP, that is set to "sendonly" (Microsoft Lync initiated Hold), creates a variable and sets it to "1". This manages the call process handling for the state of the call during the Music on Hold feature interworking.
7	If the manipulation rule Index 6 (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".
8	A SIP re-INVITE response, while the current call state has a variable set to "1", sets within the SDP, an RTP mode of "recvdonly" (as a proper response from BluIP to the Microsoft Lync initiated Hold attempt, is to normalize the call processing state back to Microsoft Lync as the proper reply to the initially received true "sendonly").
9	If the manipulation rule Index 8 (above) is executed, then the following rule is also executed. It modifies the variable for its current state. The variable is now set 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. The call can be retrieved and the normal talk path restored without any unique interworking. If any specific call is placed on hold and retrieved repeatedly, then rules 6 through 9 will ensure the sanity of the call state without limiting the feature capabilities of MS Lync or BluIP.

3. Assign the Manipulation Set IDs 3 and 4 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 **3**.
   e. Set the 'Outbound Message Manipulation Set' field to **4**.

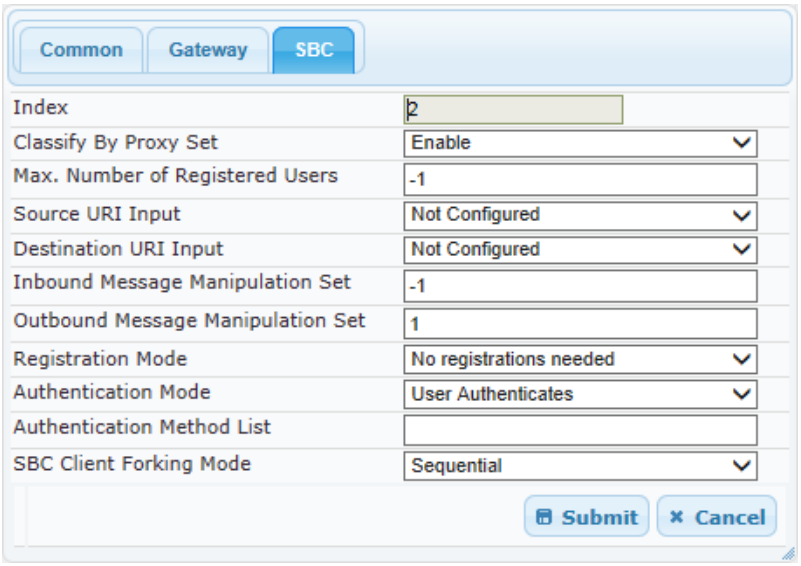
Figure 4-64: Assigning Manipulation Rule to IP Group 1



   f. Click **Submit**.

4. Assign the Manipulation Set ID 1 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. Leave the 'Inbound Message Manipulation Set' field to **-1**.
   e. Set the 'Outbound Message Manipulation Set' field to **1**.

Figure 4-65: Assigning Manipulation Rule to IP Group 2



   f. Click **Submit**.

4.14 Step 14: Miscellaneous Configuration

This step shows miscellaneous E-SBC configuration.

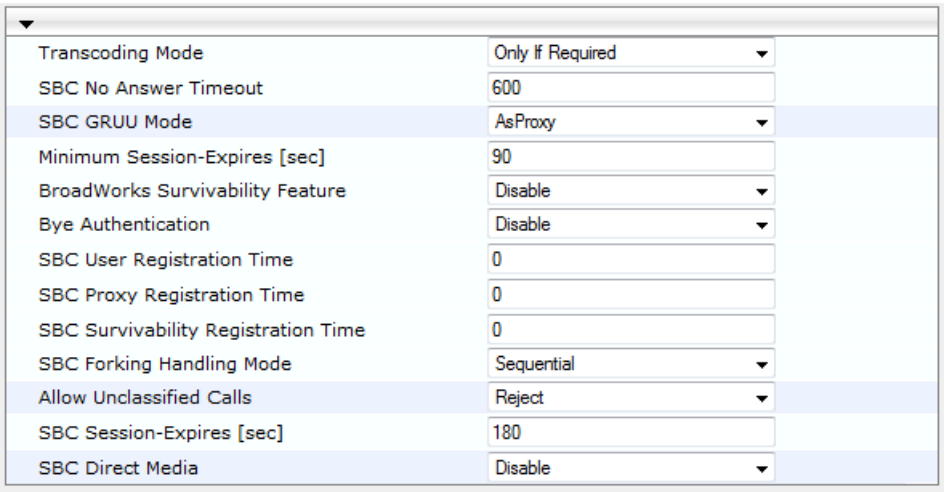
4.14.1 Step 14a: Configure Forking Mode

This step shows how to configure the E-SBC's handling of SIP 18x responses received due to call forking of an INVITE. In the 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 4-66: Configuring Forking Mode



3. Click **Submit**.

4.14.2 Step 14b: Configure SBC Preference Mode

This step shows how to configure the E-SBC's handling of SBC Extension Coders Group settings. This parameter determines the order of the Extension coders (coders added if there are no common coders between SDP offered coders and Allowed coders) and Allowed coders (defined in the Allowed Coders Group table) in the outgoing SIP message (in the SDP). This is used to ensure the preference usage of G.729 when processing calls to and from BluIP. This table parameter is used in conjunction with Extension Coders Group and Allowed Coders Group settings within the IP profile settings.

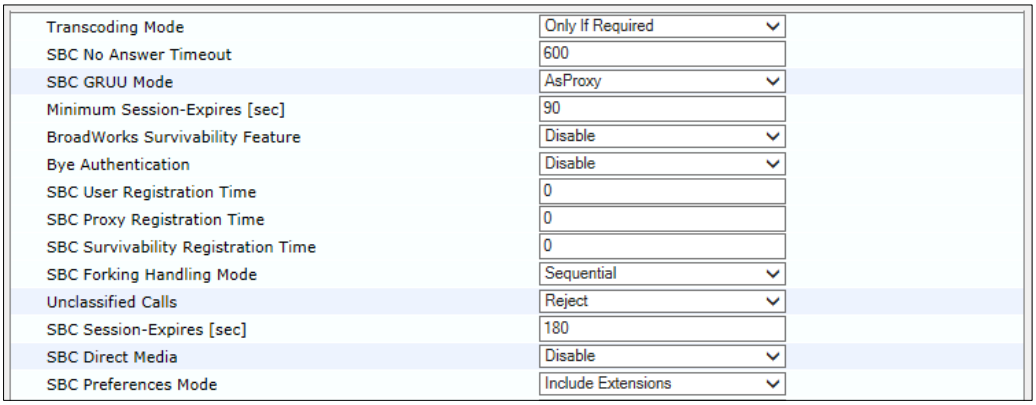
- **[0] Doesn't Include Extensions:** (Default) Extension coders are added at the end of the coder list.
- **[1] Include Extensions:** Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Coders Group table.

Note: If the *SBCExtensionCodersGroupID* parameter of the IP Profile table is set to **None**, this parameter is not applicable.

➢ **To configure SBC Preference Mode:**

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

Figure 4-67: Configuring SBC Preferences Mode



3. Click **Submit**.

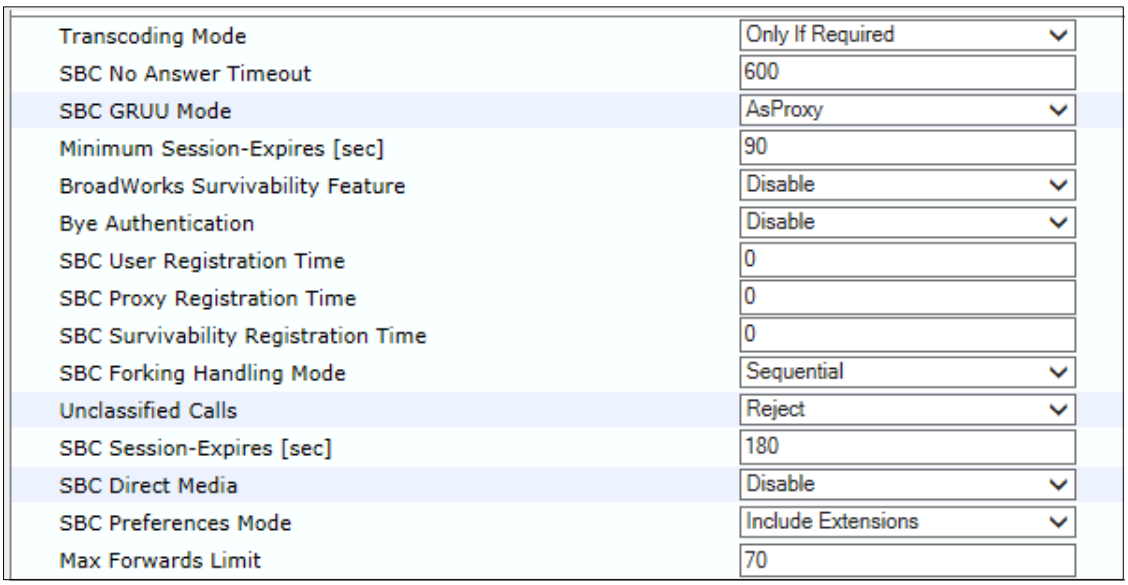
4.14.3 Step 14c: Configure Max Forwards Limit and Session-Expires

This step shows how to configure SBC Max Forward Limit and Session-Expires.

➢ **To configure SBC Max Forwards Limit and Session-Expires:**

1. Open the General Settings page (**Configuration** tab > **VoIP** > **SBC** > **General Settings**).
2. From the 'Max Forwards Limit' drop-down list, select **70**.
3. From the 'SBC Session-Expires (sec)' drop-down list, select **180**.
   Although this is the default value, this must be less than 300 seconds to help support the 'long Hold' feature call scenarios so that the SIP trunk does not de-allocate during a long duration Hold, when a given client does not have Music on Hold enabled.

Figure 4-68: Configuring Max Forwards Limit and Session-Expires



4. Click **Submit**.

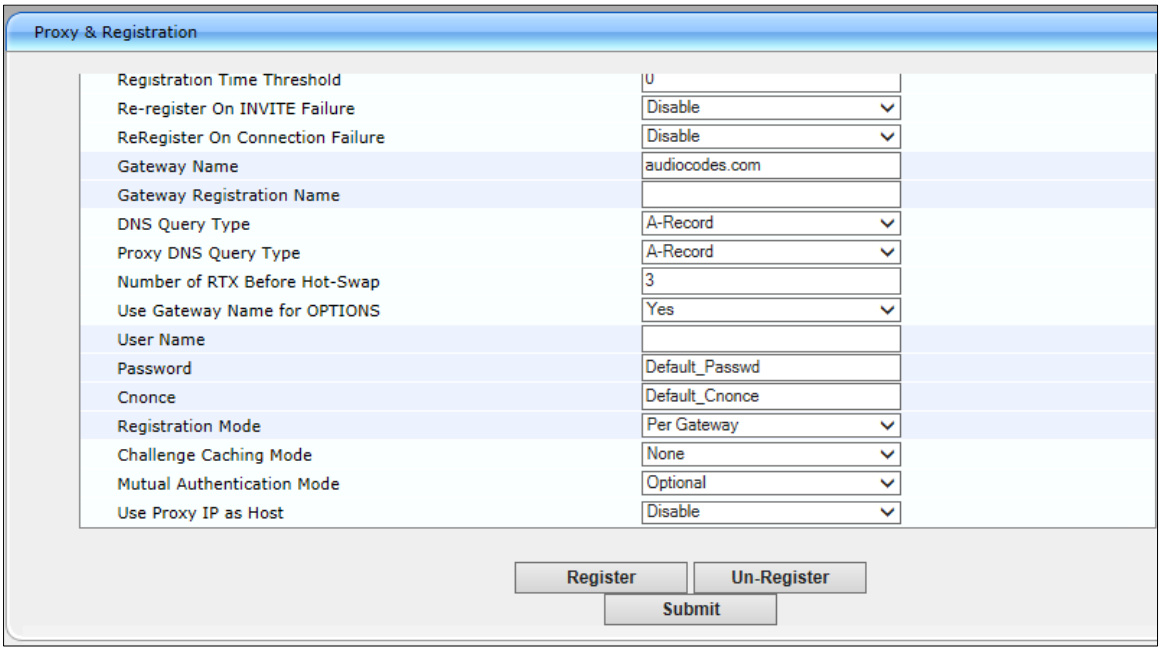
4.14.4 Step 14d: Configure Gateway Name utilization within OPTIONS

This step shows how to configure Gateway Name for usage within Options messages..

➢ **To configure Gateway Name for usage in Options messages:**

1. Open the Proxy and Registration page (**Configuration** tab > **VoIP** > **Sip Definitions** > **Proxy and Registration**).
2. From the 'Gateway Name' drop-down list, select the <domain name> provided by BluIP for the enterprise (e.g.,audiocodes.com).
3. From the 'Use Gateway Name for OPTIONS' drop-down list, select **Yes**. This must be set to properly interwork with the BluIP SIP trunk.

Figure 4-69: Configuring Gateway Name to be used in Options Messages



4. Click **Submit**.

4.15 Step 15: Configure Registration Accounts

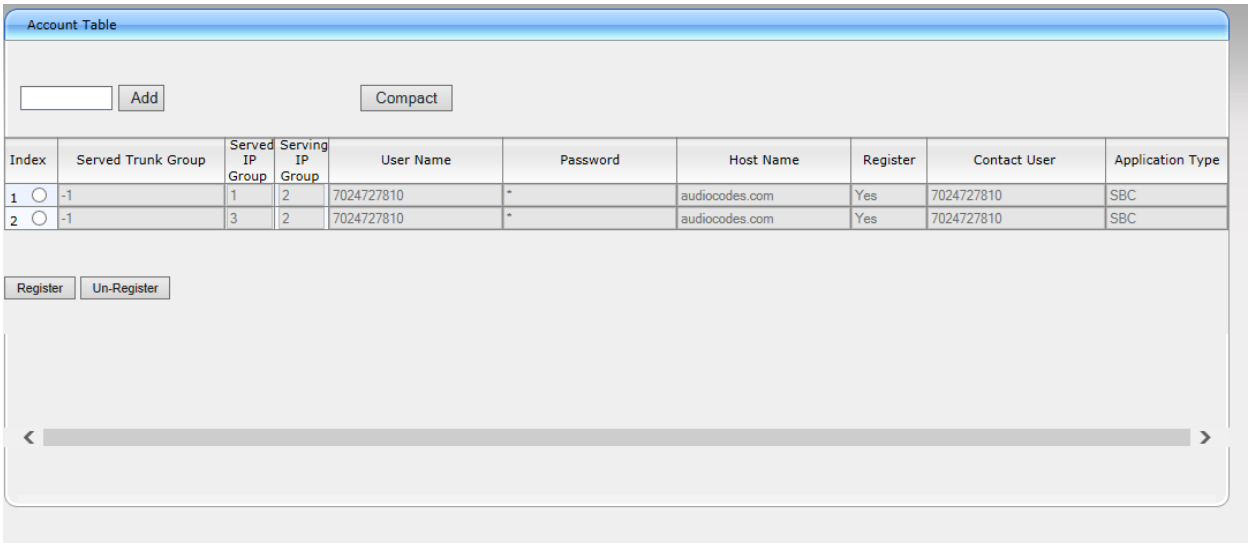
This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the BluIP SIP Trunk on behalf of Lync Server 2013. The BluIP SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Lync Server 2013 (IP Group 1) and the Serving IP Group is BluIP SIP Trunk (IP Group 2). Also do the same for the FAX supporting ATA (IP Group 3).

➢ **To configure a registration account:**

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

Figure 4-72: Configuring SIP Registration Account



2. Enter an index number (e.g., "1"), and then click **Add**.
3. Configure the account according to the provided information from BluIP, for example:

Parameter	Value
Served IP Group	**1** (Lync Server 2013)
Serving IP Group	**2** (BluIP SIP Trunk)
Username	As provided by BluIP
Password	As provided by BluIP
Host Name	**audiocodes.com**
Register	**Yes**
Contact User	**7024727810** (trunk main line)
Application Type	**SBC**

4. Click **Apply**.
5. Enter an index number (e.g., "2"), and then click **Add**.

6. Configure the account according to the provided information from BluIP, for example:

Parameter	Value
Served IP Group	**3** (Fax supporting ATA)
Serving IP Group	**2** (BluIP SIP Trunk)
Username	As provided by BluIP
Password	As provided by BluIP
Host Name	**audiocodes.com**
Register	**Yes**
Contact User	**7024727810** (trunk main line)
Application Type	**SBC**

7. Click **Apply**.

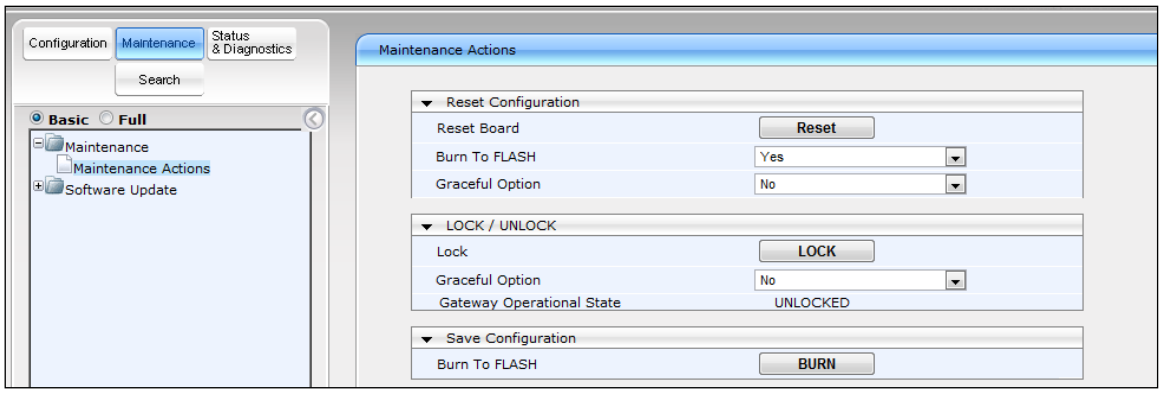
4.16 Step 16: Reset the E-SBC

After you complete the E-SBC configuration as shown 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 4-73: Resetting the E-SBC



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

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 35, is shown below:

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

;Board: Mediant 1000
;HW Board Type: 47  FK Board Type: 71
;Serial Number: 2967088
;Slot Number: 1
;Software Version: 6.60A.241.010
;DSP Software Version: 624AE3 => 660.10
;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

[Analog Params]


[ControlProtocols Params]

RTCPInterval = 5000




[Voice Engine Params]

ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'


[SIP Params]

MEDIACHANNELS = 20
SIPDESTINATIONPORT = 5067
GWDEBUGLEVEL = 5
SIPGATEWAYNAME = 'audiocodes.com'
PROXYREDUNDANCYMODE = 1
USEGATEWAYNAMEFOROPTIONS = 1
SIPTRANSPORTTYPE = 2
TCPLOCALSIPPORT = 5068
TLSLOCALSIPPORT = 5067
MEDIASECURITYBEHAVIOUR = 3
ENABLESBCAPPLICATION = 1
SBCMAXFORWARDSLIMIT = 70
ENABLESYMMETRICMKI = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 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, 10.133.4.43, 16, 10.133.4.1, 1, "Voice",
10.133.4.40, 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, , 6000, 10, 6090, 1;
CpMediaRealm 2 = "MRwan", Public, , 7000, 10, 7090, 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 ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE15.ilync15.local", 2, 1;
ProxyIp 1 = "199.168.177.14:5060", 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_AmdMode,
IpProfile_SBCReliableHeldToneSource, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_GenerateSRTPKeys;
IpProfile 1 = "Lync_lan_2013", 1, 1, 0, 10, 10, 46, 40, 0, 0, 0,
0, 2, 0, 0, 0, 1, -1, 1, 0, 1, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0,
1, 1, 2, 1, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3,
1, 1, 0, 3, 2, 1, 2, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, -1, 1, 0, 1, 0,
0, 1;
IpProfile 2 = "BluIP", 2, 2, 0, 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, "", 2, 0, 1, 2, 1,
2, 0, 0, 1, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 2, 2, 2, 0,
3, 0, 1, 2, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, -1, 0, 0, 1, 0, 0, 0;
IpProfile 3 = "fax", 1, 3, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 3, 0, 0, 3, 1, 0,
0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0,
0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 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, 60, 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, "CorpLab2013", 1, "audiocodes.com", "", 0, -1, -1,
0, -1, 1, "MRLan", 1, 1, -1, 3, 4, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "BluIP", 2, "audiocodes.com", "", 0, -1, -1, 0, -1,
2, "MRwan", 1, 2, -1, -1, 1, 0, 0, "", 0, -1, -1, "";
IPGroup 3 = 0, "Fax", 3, "audiocodes.com", "", 0, -1, -1, 0, -1,
1, "MRLan", 1, 3, -1, -1, -1, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroup, Account_ServingIPGroup, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 1 = -1, 1, 2, "7024727810", *, "audiocodes.com", 1,
"7024727810", 2;
Account 2 = -1, 3, 2, "7024727810", *, "audiocodes.com", 1,
"7024727810", 2;


[ \Account ]


[ 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 = 1, "*", "*", "*", "*", 0, , -1, 0, 0, 2, , "", 0,
-1, 0, ;
IP2IPRouting 3 = 2, "*", "*", "7024727813", "*", 0, , -1, 0, 0, 3,
, "", 0, -1, 0, ;
IP2IPRouting 4 = 2, "*", "*", "*", "*", 0, , -1, 0, 0, 1, , "", 0,
-1, 0, ;
IP2IPRouting 5 = 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, 0, 0, 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, 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 0 = 0, 2, 1, "*", "*", "*", "*", 0, -1, 0,
0, 0, 0, 255, "", "", 1;
IPOutboundManipulation 1 = 0, 1, 2, "", "*", "*", "*", 0, -1, 0,
0, 0, 0, 255, "", "", 3;
IPOutboundManipulation 2 = 0, -1, 1, "*", "*", "*", "*", 0, -1, 0,
1, 0, 0, 255, "+1", "", 0;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

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

[ \CodersGroup0 ]


[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 1;
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 1;

[ \CodersGroup1 ]


[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = "g729", 20, 0, -1, 0;
CodersGroup2 1 = "g711Ulaw64k", 20, 0, -1, 0;
CodersGroup2 2 = "g711Alaw64k", 20, 0, -1, 0;
```

```
[ \CodersGroup2 ]


[ CodersGroup3 ]

FORMAT CodersGroup3_Index = CodersGroup3_Name, CodersGroup3_pTime,
CodersGroup3_rate, CodersGroup3_PayloadType, CodersGroup3_Sce;
CodersGroup3 0 = "g729", 20, 0, -1, 0;
CodersGroup3 1 = "g711Ulaw64k", 20, 0, -1, 0;

[ \CodersGroup3 ]


[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g729";
AllowedCodersGroup1 1 = "g711Ulaw64k";
AllowedCodersGroup1 2 = "g711Alaw64k";

[ \AllowedCodersGroup1 ]


[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
AllowedCodersGroup2 1 = "g711Ulaw64k";
AllowedCodersGroup2 2 = "g711Alaw64k";

[ \AllowedCodersGroup2 ]


[ AllowedCodersGroup3 ]

FORMAT AllowedCodersGroup3_Index = AllowedCodersGroup3_Name;
AllowedCodersGroup3 0 = "g729";
AllowedCodersGroup3 1 = "g711Ulaw64k";
AllowedCodersGroup3 2 = "g711Alaw64k";

[ \AllowedCodersGroup3 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 1 = 1, "Invite", "", "header.p-asserted-
identity", 2, "'<sip:7024727810@audiocodes.com>'", 0;
MessageManipulations 2 = 1, "", "", "header.p-asserted-
identity.1", 1, "", 0;
```

```
MessageManipulations 3 = 1, "", "", "Header.Diversion.URL.user",
6, "'+1'", 0;
MessageManipulations 4 = 1, "", "", "Header.Diversion.URL.host",
2, "'audiocodes.com'", 0;
MessageManipulations 5 = 1, "Invite.request", "",
"header.privacy", 1, "", 0;
MessageManipulations 6 = 3, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2,
"'1'", 0;
MessageManipulations 7 = 3, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'",
"param.message.sdp.rtpmode", 2, "'sendrecv'", 1;
MessageManipulations 8 = 4, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2,
"'recvonly'", 0;
MessageManipulations 9 = 4, "", "", "var.call.src.0", 2, "'0'", 1;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]
```

B Configuring Analog Devices (ATAs)

This section shows how to configure the analog device entity to route its calls to 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 shown 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

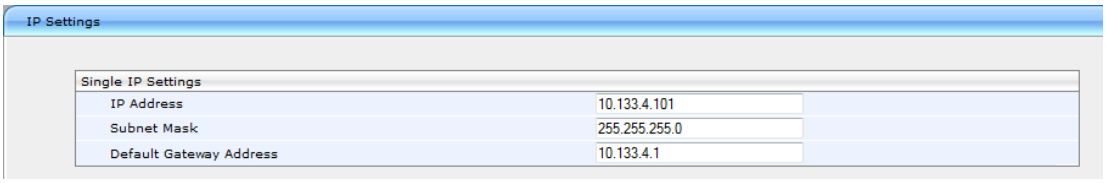
This step shows how to configure the IP address settings of the MP-11x. Refer to the *Installation Manual* for details.

➢ **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 the *Installation Manual* for detailed instructions.

Figure 4-70: Configuring IP Address of the MP-11x



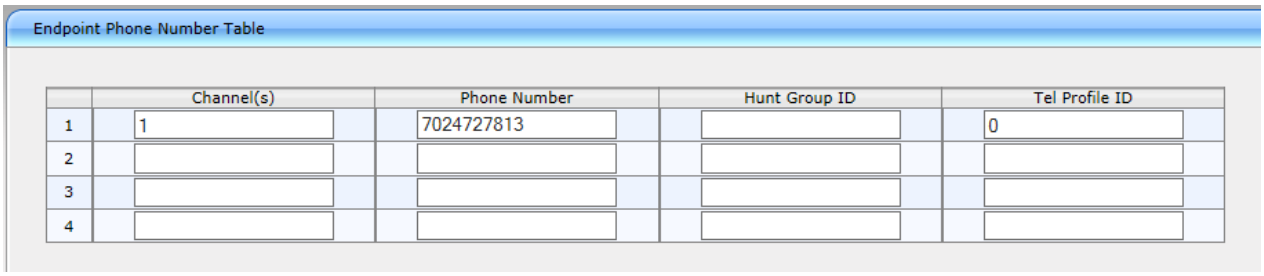
B.2 Step 2: Configure Endpoint Phone Numbers

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 **7024727813.**

➢ **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 4-71: Configuring Endpoint Phone Numbers



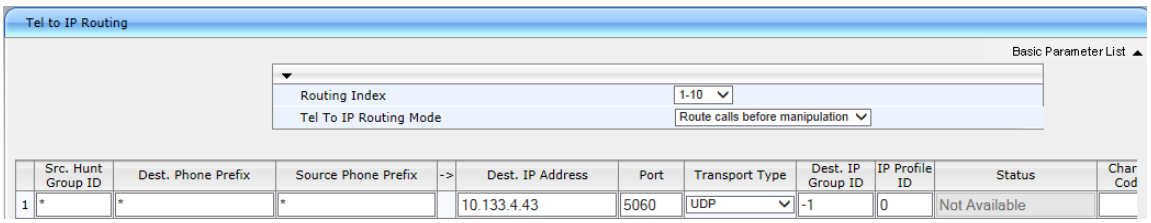
B.3 Step 3: Configure Tel-to-IP Routing Rules

This step shows how to configure the Tel-to-IP routing rules to ensure that the MP-11x device sends all calls to AudioCodes' centralized E-SBC device to be sent onwards to the BluIP service. All Tel-to-IP calls from the FAX supporting analog device (IP address 10.133.4.101) are routed directly to the AudioCodes' E-SBC (10.133.4.43).

➢ **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 4-72: Configuring Tel-to-IP Routing Rules



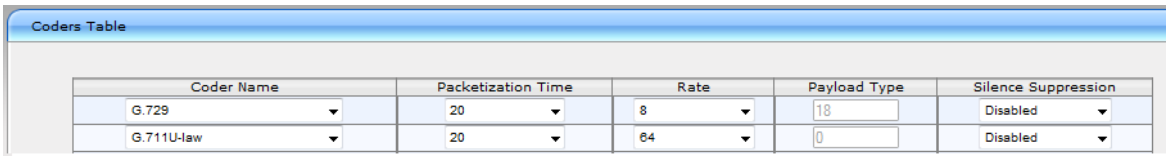
B.4 Step 4: Configure Coders for MP-11x

This step shows how to configure the coders for the MP-11x. Note that the first choice is **G.729**. Even though the device will be used exclusively for Fax support, the BluIP network must first see the originating attempt displayed as **G.729**. After the call is answered on the other side of the BluIP network, the infrastructure can then support the transition to T.38 support. This is a unique interworking caveat of BluIP.

➢ **To configure coders for MP-11x:**

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

Figure 4-73: Configuring Coders for MP-11x



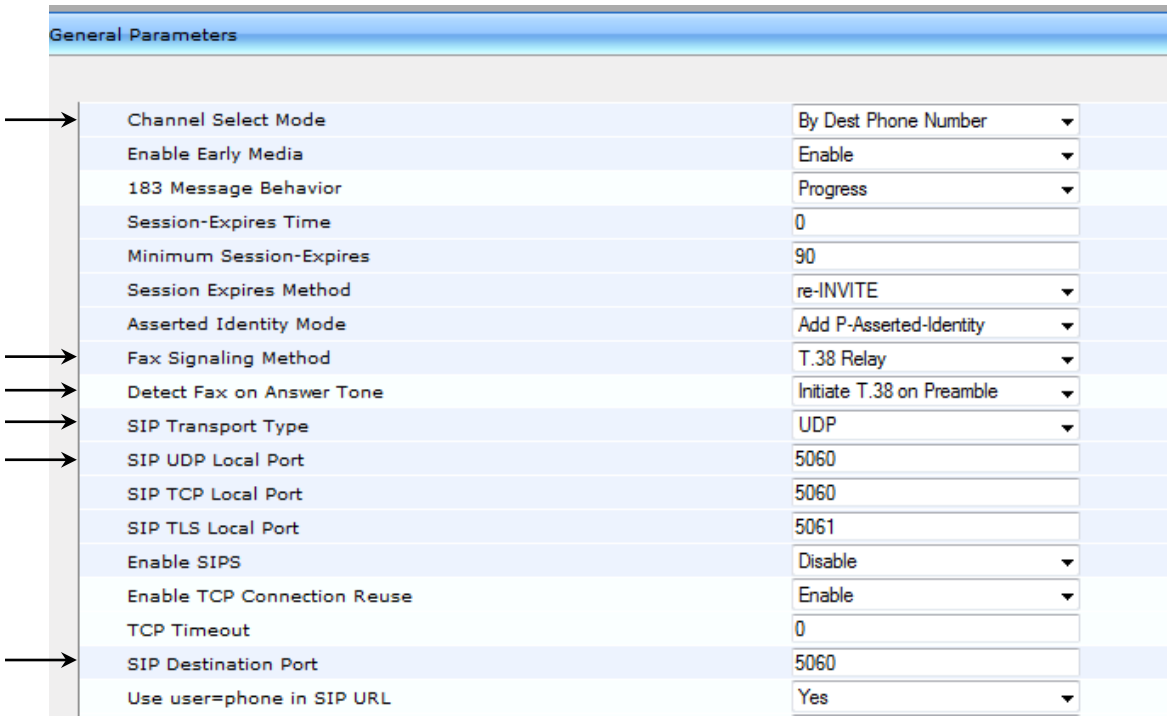
B.5 Step 5: Configure SIP UDP Transport Type and Fax Signaling Method

This step shows 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 4-74: 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' field, enter **5060** (corresponding to the Centralized E-SBC UDP listening port configuration).

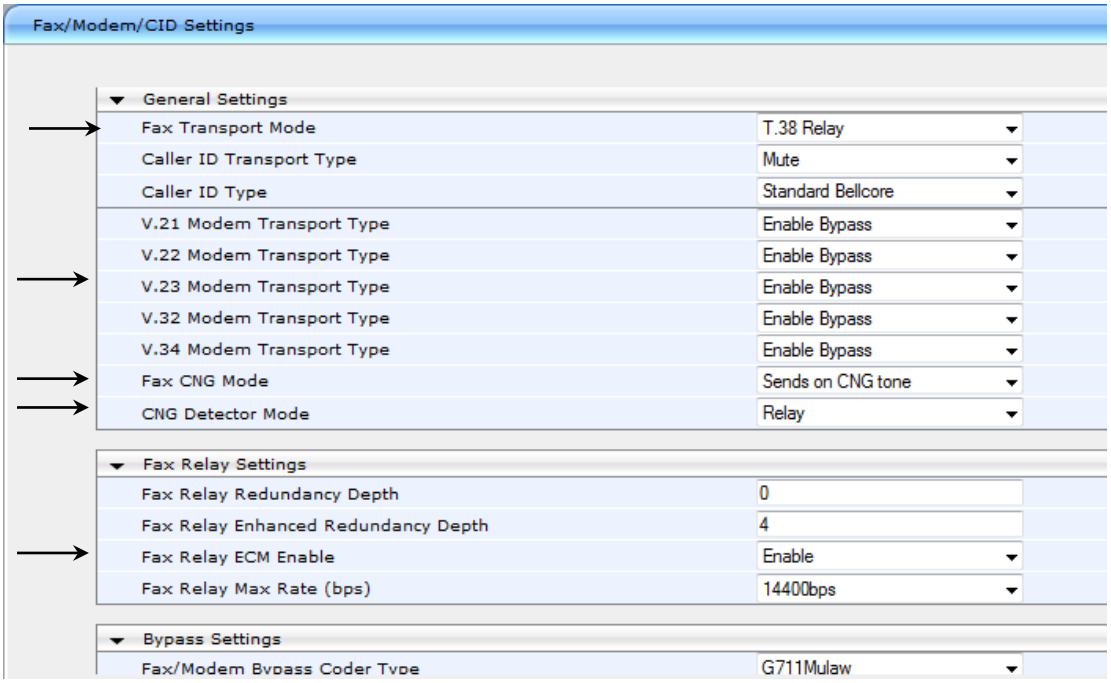
B.6 Step 6: Configure Base Media Fax Settings

This step shows 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 4-75: 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 list, select **Send on CNG tone**.
5. From the 'CNG Detector Mode' drop-down list, select **Relay**.
6. From the 'Fax Relay ECM Enable' drop-down list, select **Enable**.

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com