AudioCodes™ Mediant™ Series

Enterprise Session Border Controller (E-SBC)

Interoperability Laboratory

Configuration Note

Connecting Microsoft® Lync™ Server 2013 with ITSP SIP Trunk using AudioCodes E-SBC

SBC

Microsoft Partner
Gold Communications

Lync

AudioCodes

Version 6.6

December 2013

Document #: LTRT-54006

Table of Contents

List of Figures

Reader's Notes

Notice

This Configuration Note shows how to connect Microsoft Lync Server 2013 and a SIP Trunk using AudioCodes Mediant E-SBC product series.

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

Date Published: December-8-2013

Trademarks

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

WEEE EU Directive

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

Customer Support

Customer technical support and 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.

Reader's Notes

1 Introduction

This Configuration Note shows how to configure AudioCodes' Enterprise Session Border Controller (E-SBC) for interworking between an ITSP (Internet Telephony Service Provider's) SIP (Session Initiation Protocol) Trunking service and Microsoft's Lync communication platform (Lync Server 2013).

The Note shows how to connect Microsoft Lync Server 2013 and a SIP Trunk using AudioCodes Mediant E-SBC product series, which includes the Mediant 1000B Gateway & E-SBC, Mediant 800 Gateway & E-SBC, Mediant 2600 E-SBC, Mediant 4000 E-SBC and Mediant 3000 Gateway & E-SBC.

1.1 Intended Audience

The Configuration Note is intended for engineers or AudioCodes and Partners who are responsible for installing and configuring SIP Trunking and Microsoft's Lync communication platform for enabling VoIP calls using AudioCodes' E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between an enterprise's VoIP network and the ITSP's VoIP network.

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

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.60A or later
Protocol	▪ SIP/UDP (to the ITSP's SIP Trunk) ▪ SIP/TCP or TLS (to the Lync Front End Server)
Additional Notes	None

2.2 Microsoft Lync Server 2013 Version

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

2.3 Deploying the E-SBC

2.3.1 Example Environment

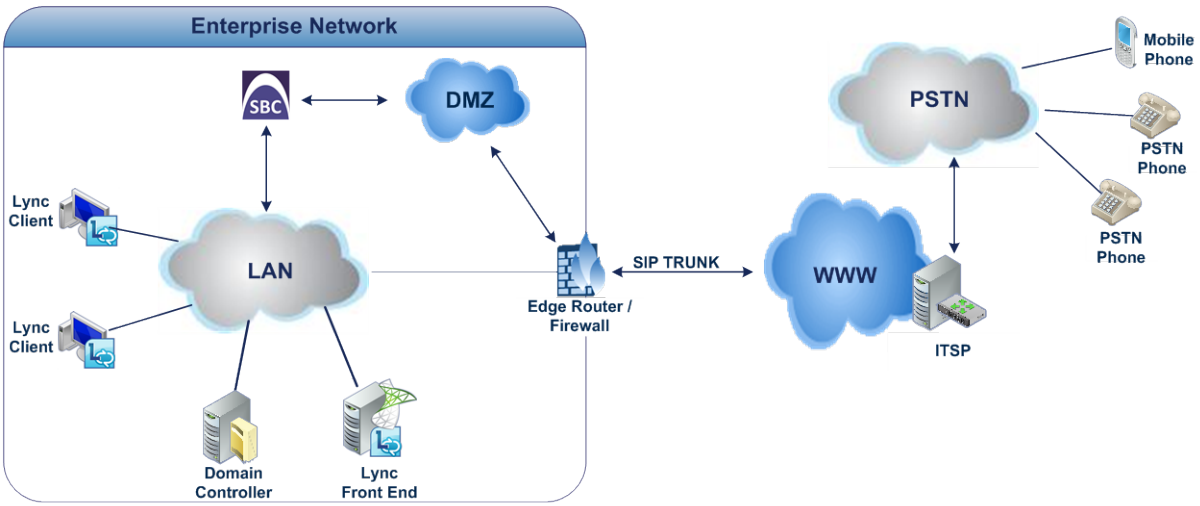
The example scenario below is referred to throughout this document in order to show how to deploy the E-SBC.

In the example environment:

- Microsoft Lync Server 2013 is deployed in an enterprise's private network for enhanced communication within the enterprise.
- The enterprise wants to offer its employees enterprise-voice capabilities and to connect the enterprise to the PSTN network using a SIP Trunking service provided by the enterprise's ITSP.
- AudioCodes' E-SBC is implemented to interconnect between the enterprise's LAN and the SIP Trunk.
  - Session: Real-time voice session using IP-based SIP
  - Border: IP-to-IP network border between Lync Server 2013 network in the enterprise LAN and the SIP Trunk located in the public network.

The figure below illustrates AudioCodes' E-SBC interworking between Microsoft Lync Server 2013 and an ITSP's SIP Trunking site.

Figure 2-1: E-SBC Interworking Lync 2013 and a SIP Trunk in an Example Environment



2.3.2 Environment Setup

The example scenario includes the following environment setup:

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

Reader's Notes

3 Configuring Microsoft Lync Server 2013

This section shows 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.

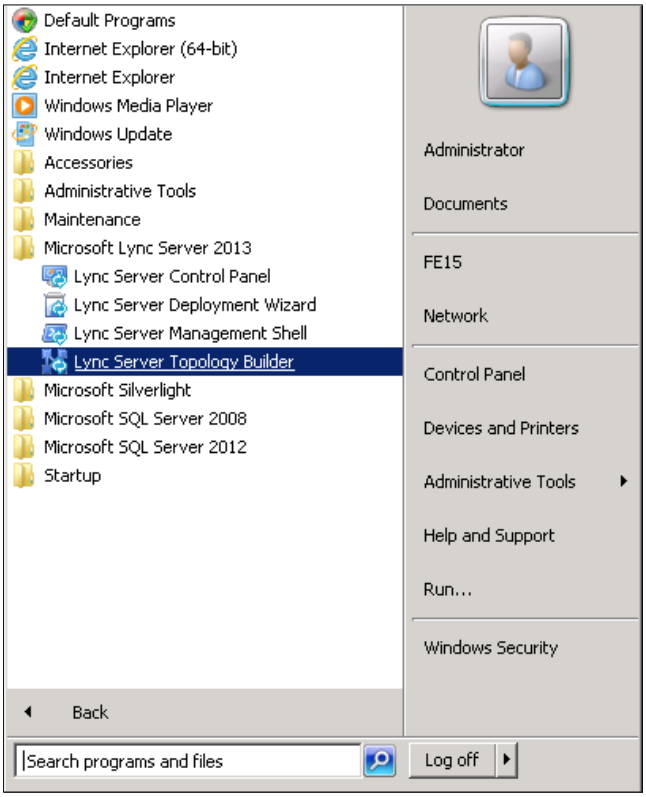
3.1 Configuring the E-SBC as an IP / PSTN Gateway

This section shows how to configure the E-SBC as an IP / PSTN Gateway.

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

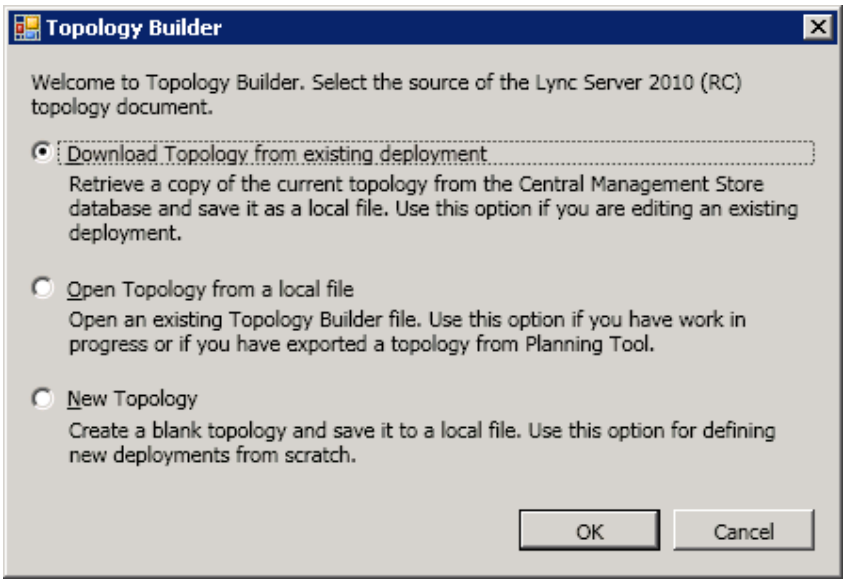
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder: Click the Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**.

Figure 3-1: Starting the Lync Server Topology Builder



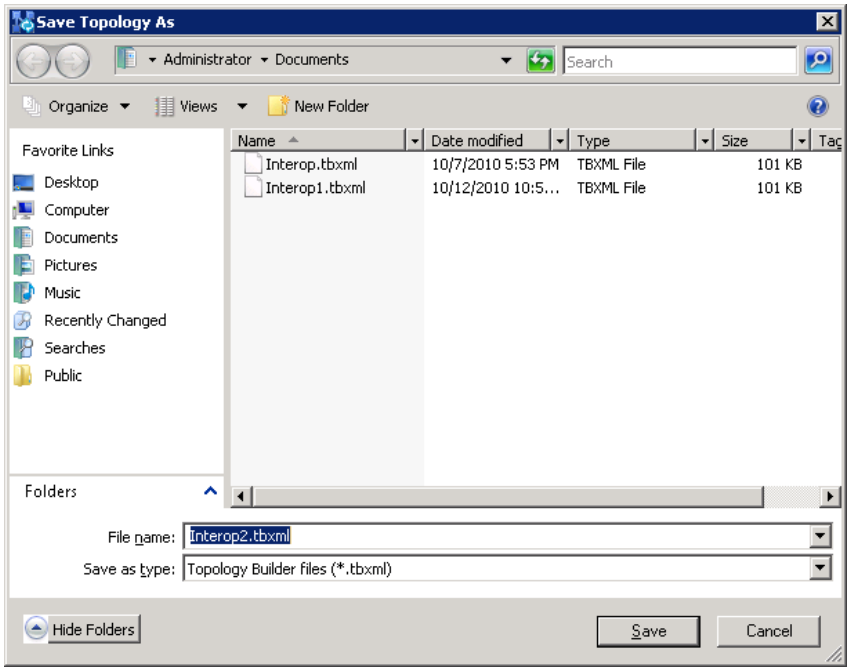
This screen is displayed:

Figure 3-2: Topology Builder Options



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

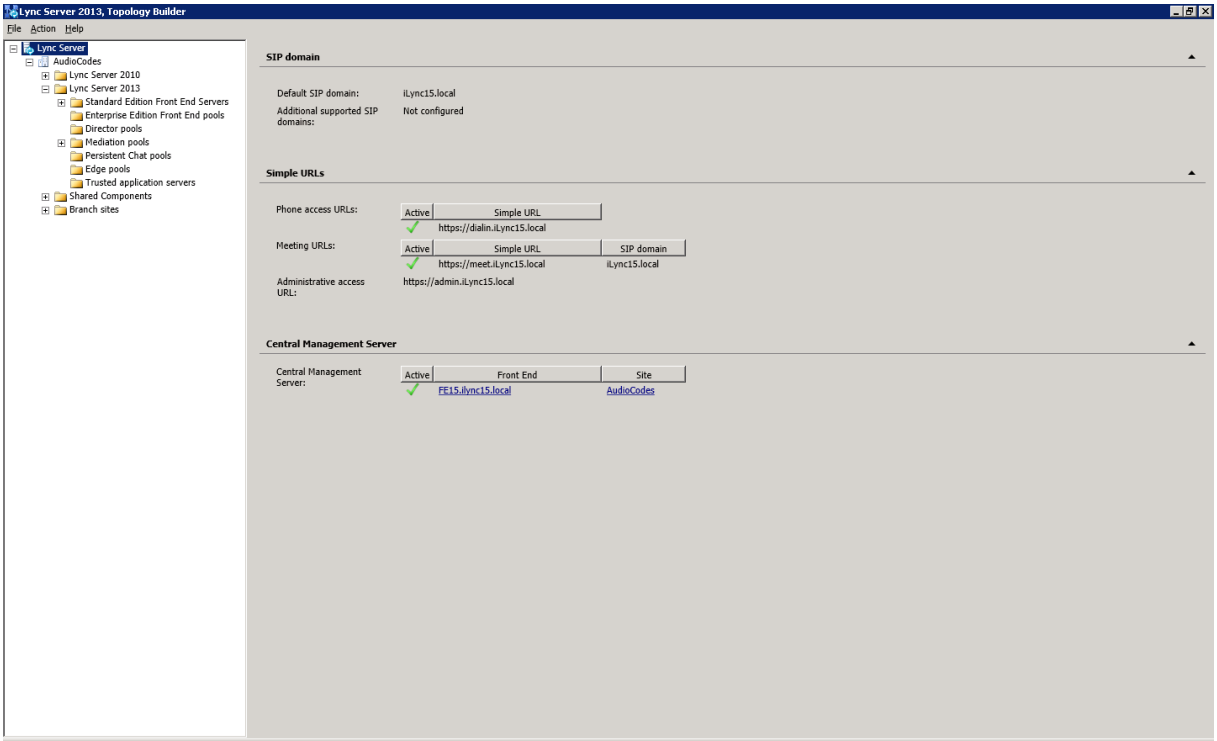
Figure 3-3: Save Topology



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

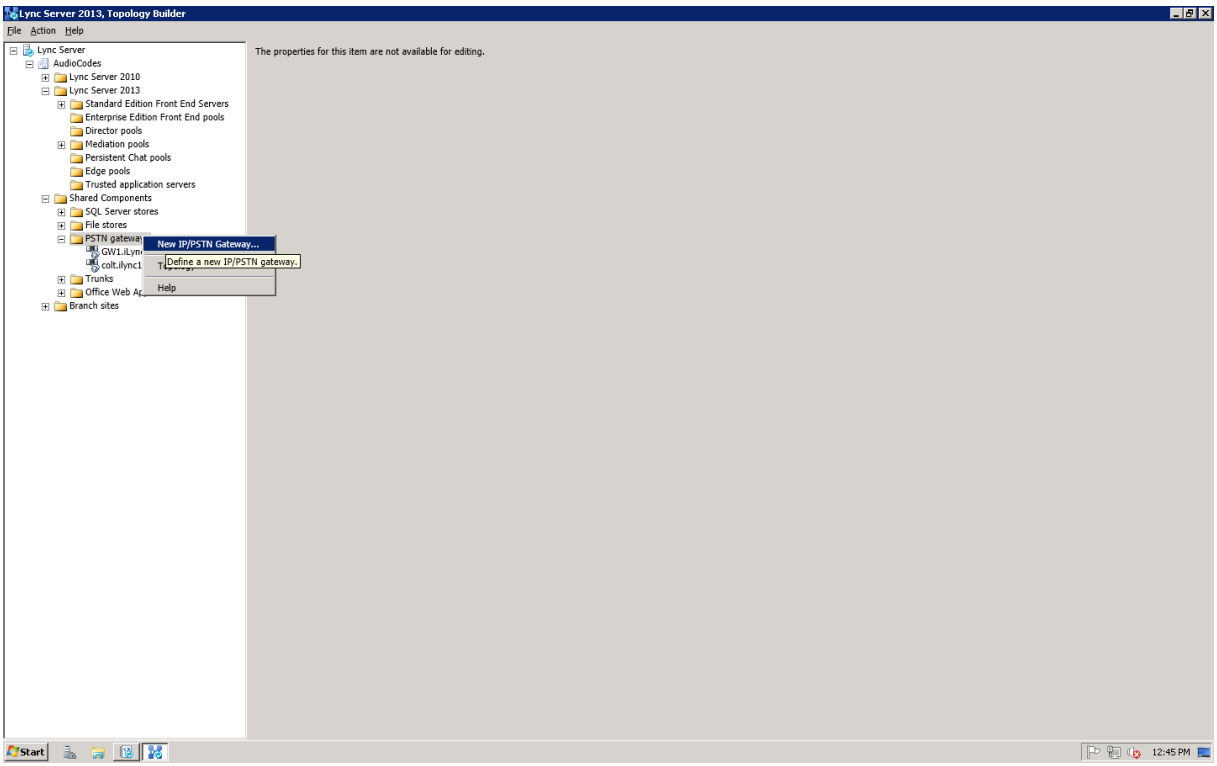
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Topology Builder Displaying Downloaded Topology



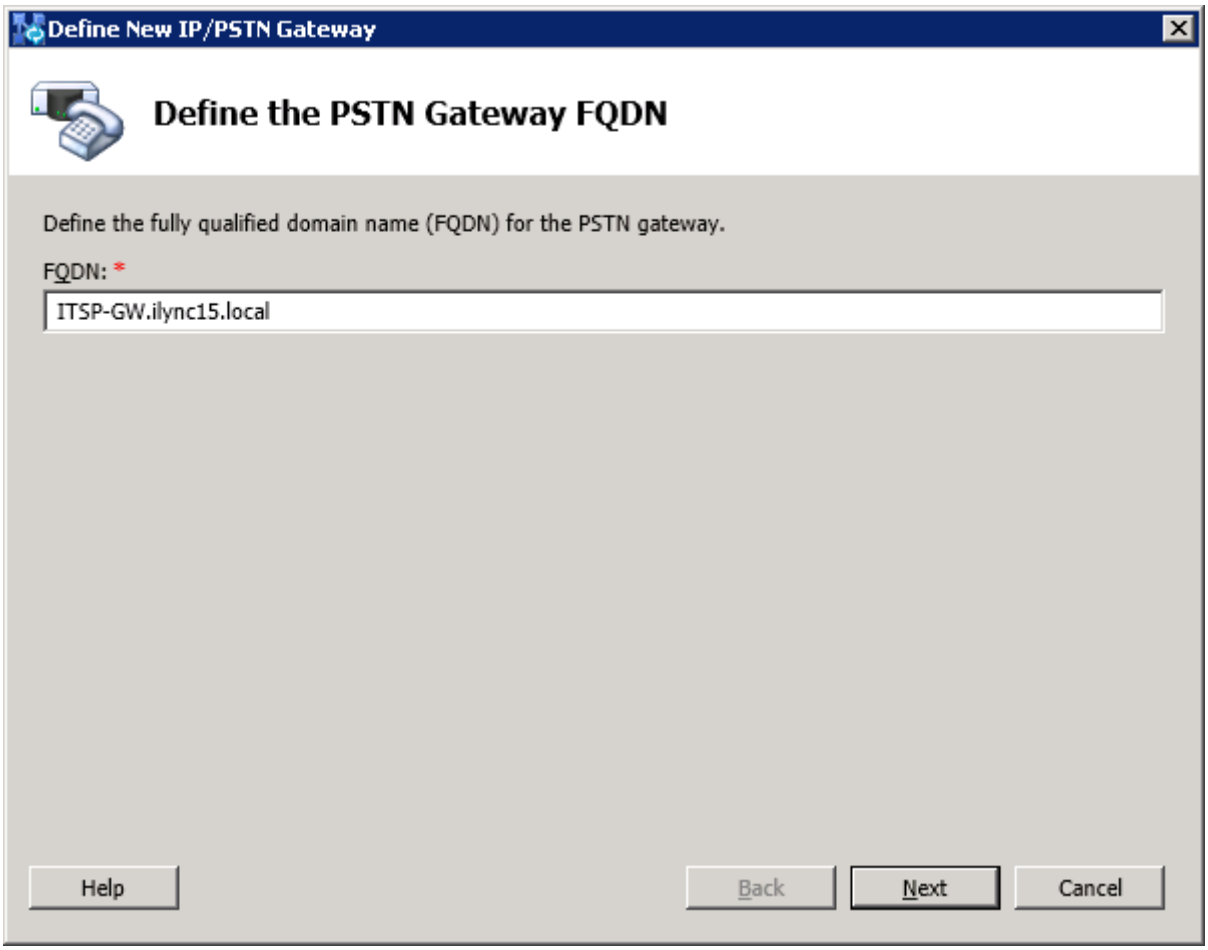
4. In the tree, expand Lync Server 2013 > your site name > Shared Components.
5. Right-click the **PSTN Gateways** folder and select **New IP/PSTN Gateway** from the popup menu:

Figure 3-5: Selecting New IP/PSTN Gateway



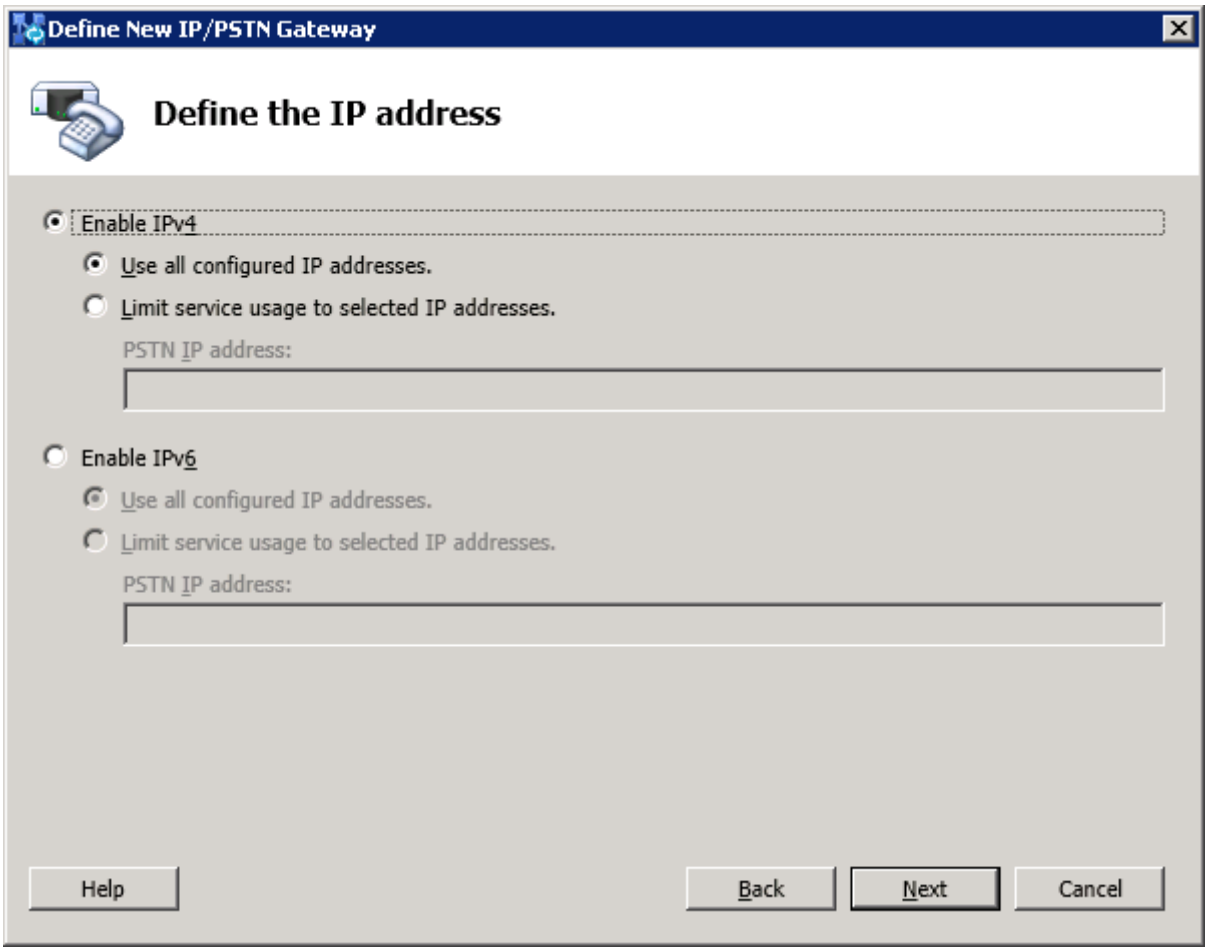
This dialog opens:

Figure 3-6: Define New IP/PSTN Gateway



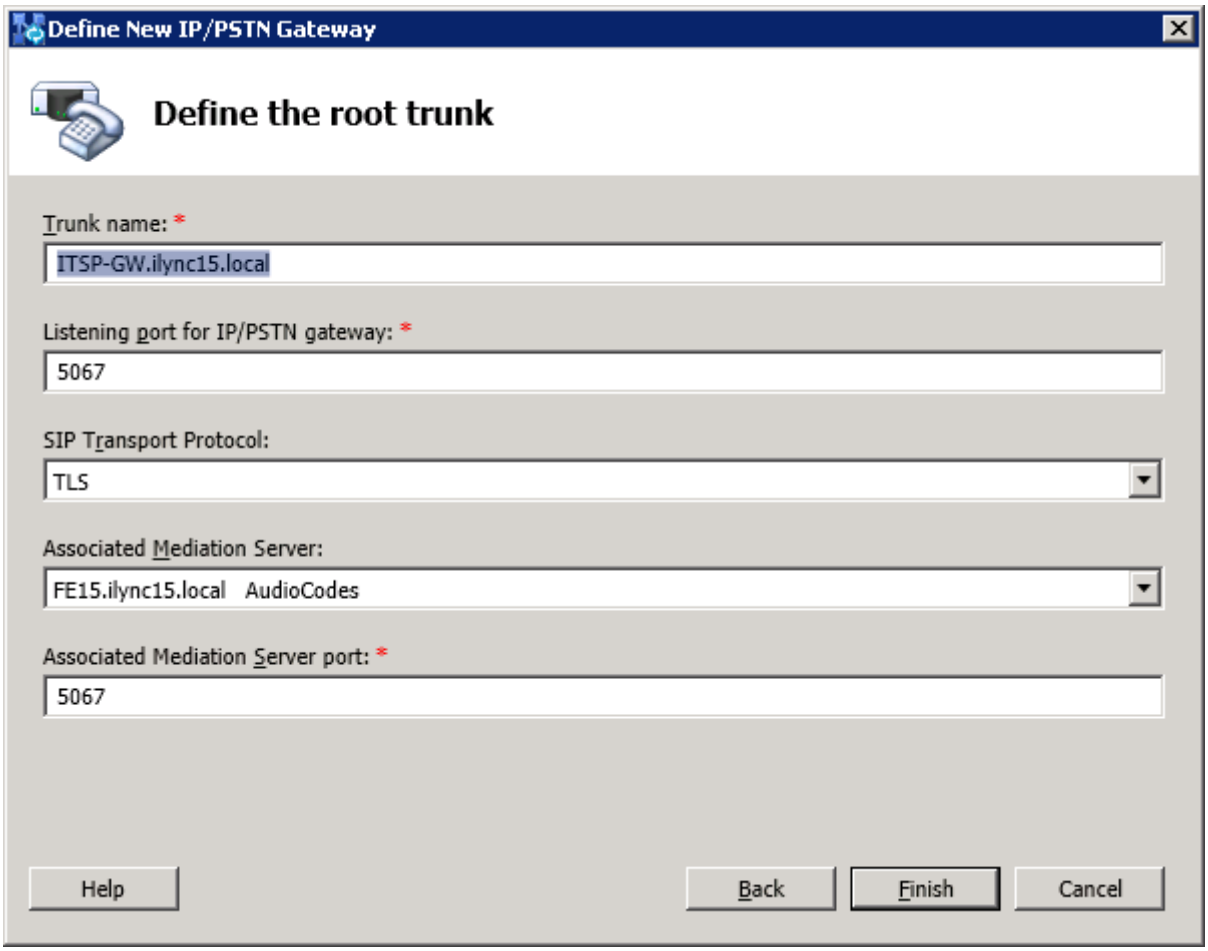
6. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., ITSP-GW.ilync15.local). This FQDN should be updated in the relevant DNS record and then, click **Next**.
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway and click **Next**.

Figure 3-7: Define the IP Address



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

Figure 3-8: Define the Root Trunk



a. In the 'Listening Port for IP/PSTN Gateway' field, type 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 (i.e., 5067).

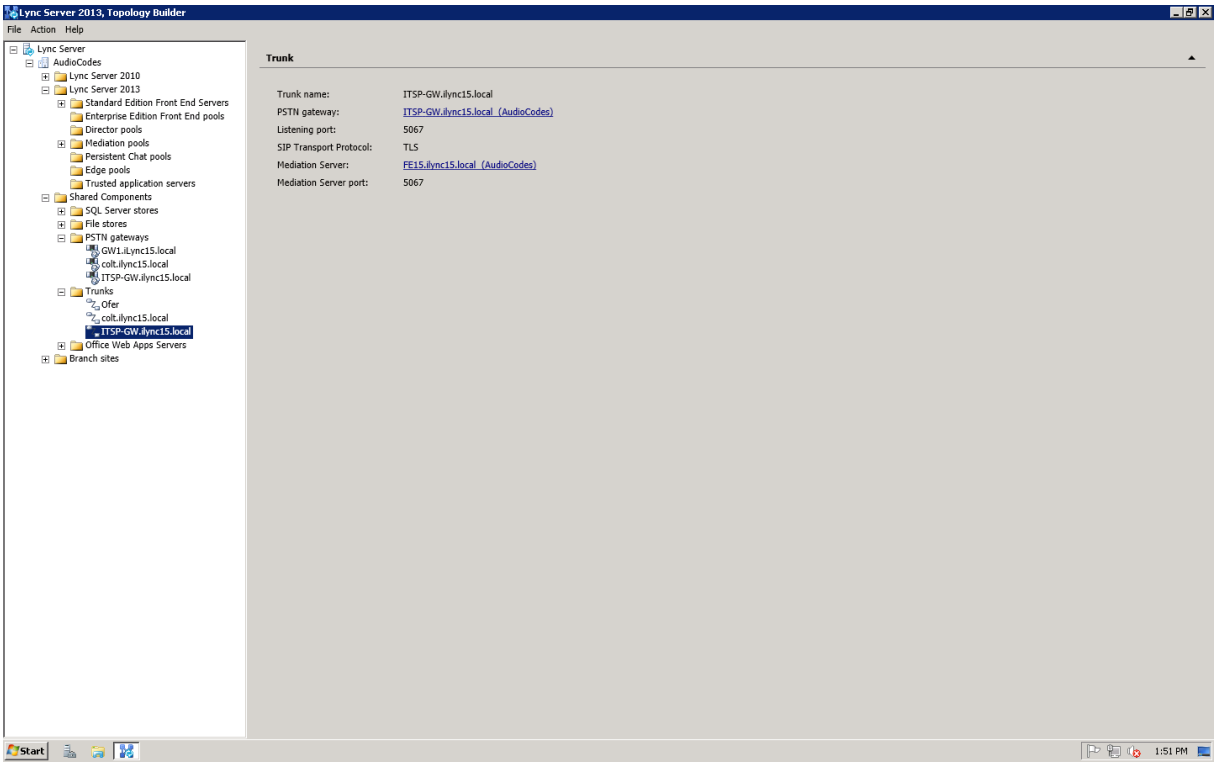
b. In the 'SIP Transport Protocol' field, click the transport type (i.e., TLS) that the trunk uses.

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, type the listening port that the Mediation Server will use for SIP messages from the SBC (i.e., 5067).

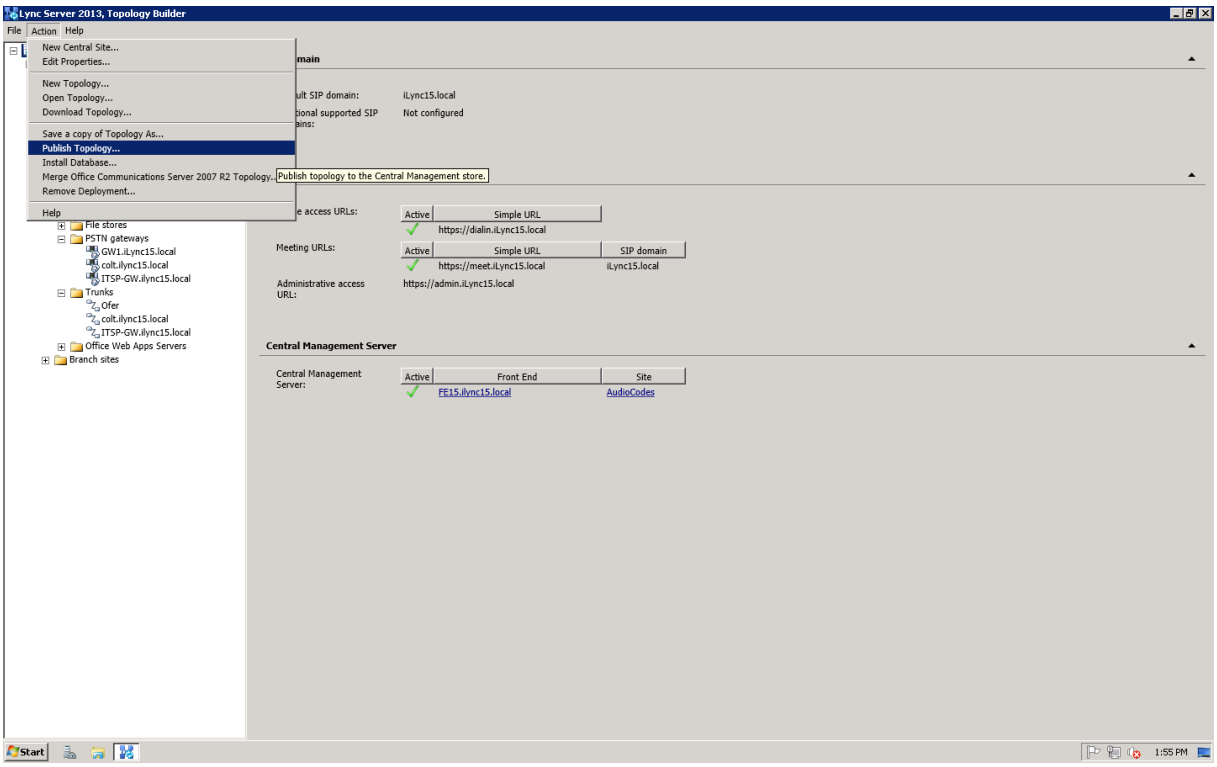
Click **Finish**; the SBC is added as a PSTN Gateway and a trunk is created:

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



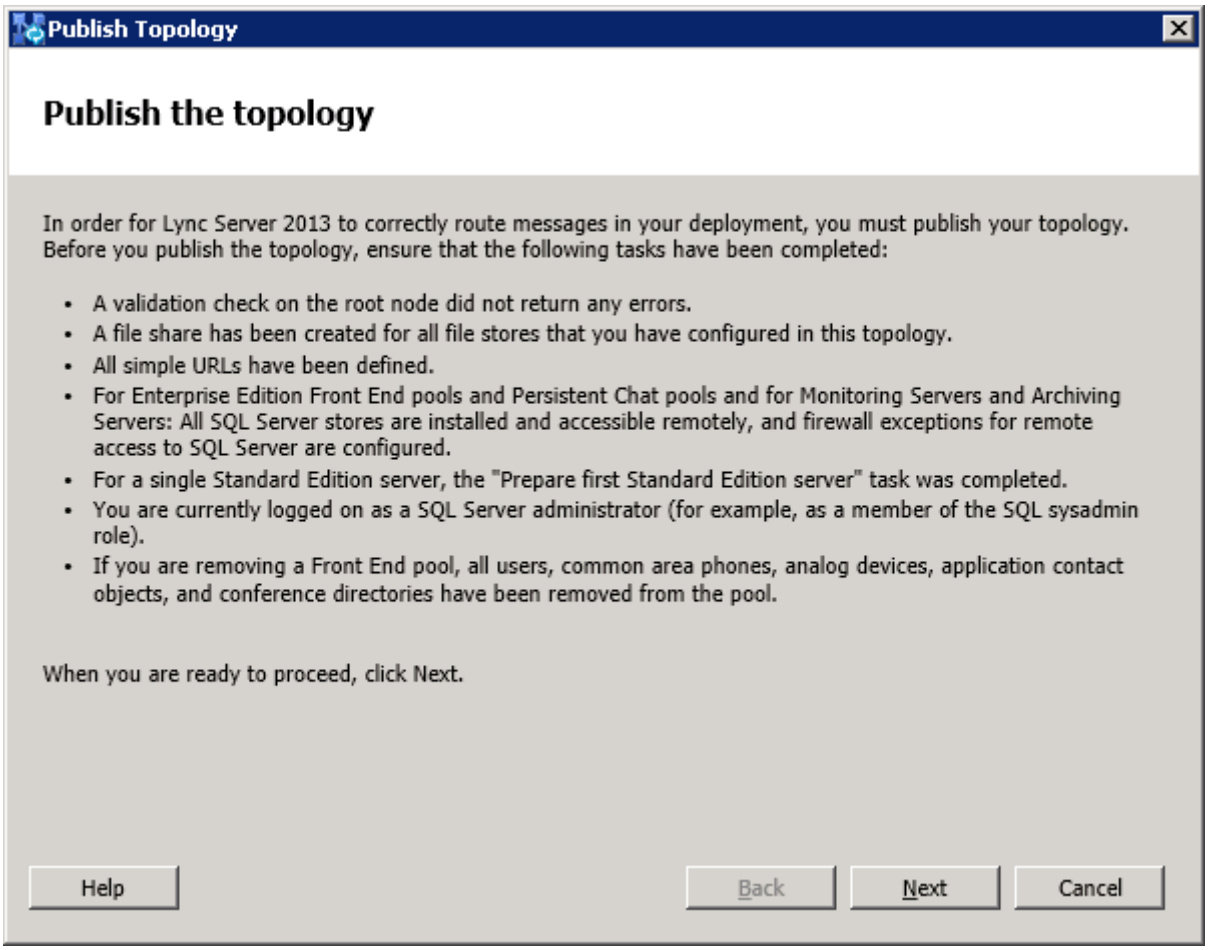
10. Publish the Topology: In the main tree, select the root item **Lync Server** and from the **Action** menu, select **Publish Topology**:

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



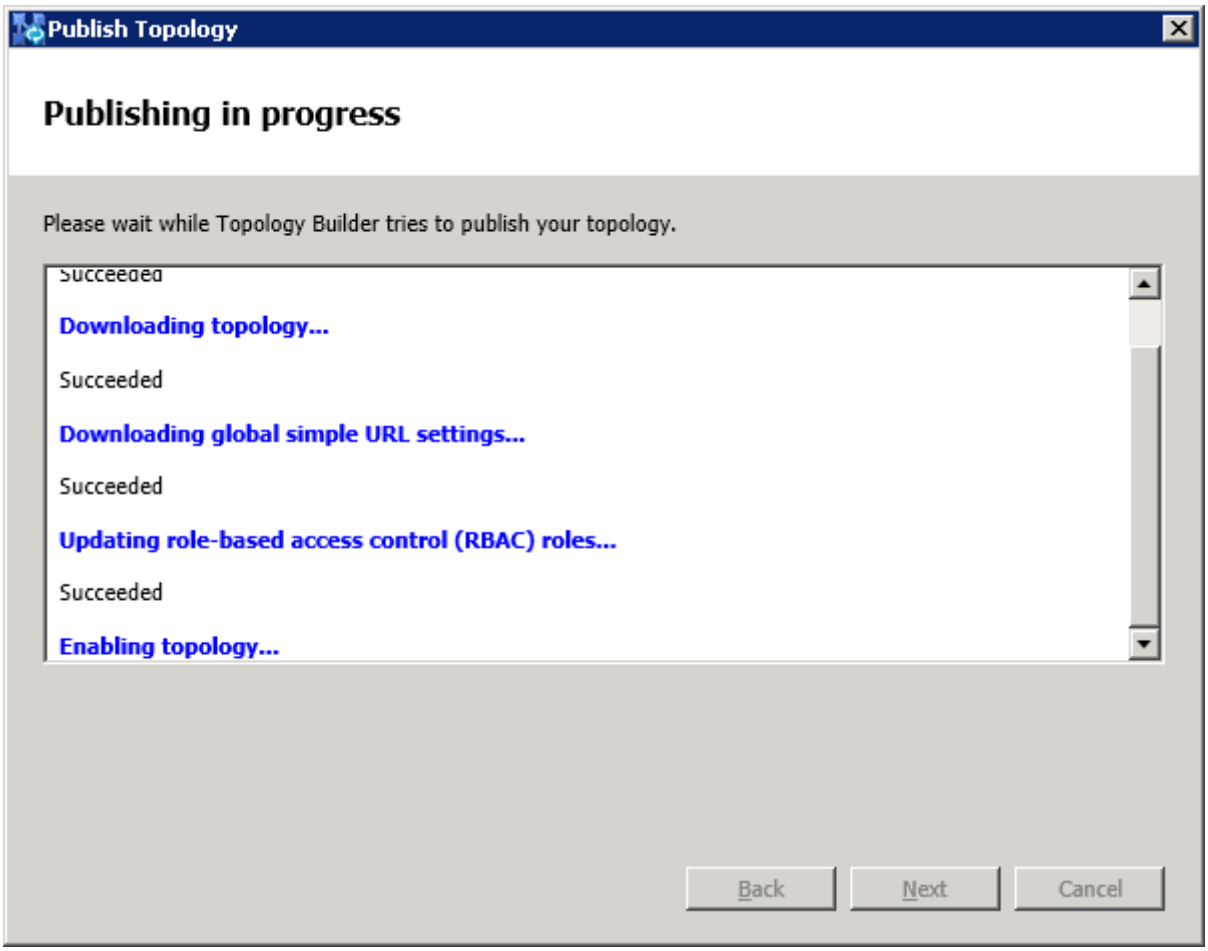
The Publish Topology screen is displayed:

Figure 3-11: Publish Topology



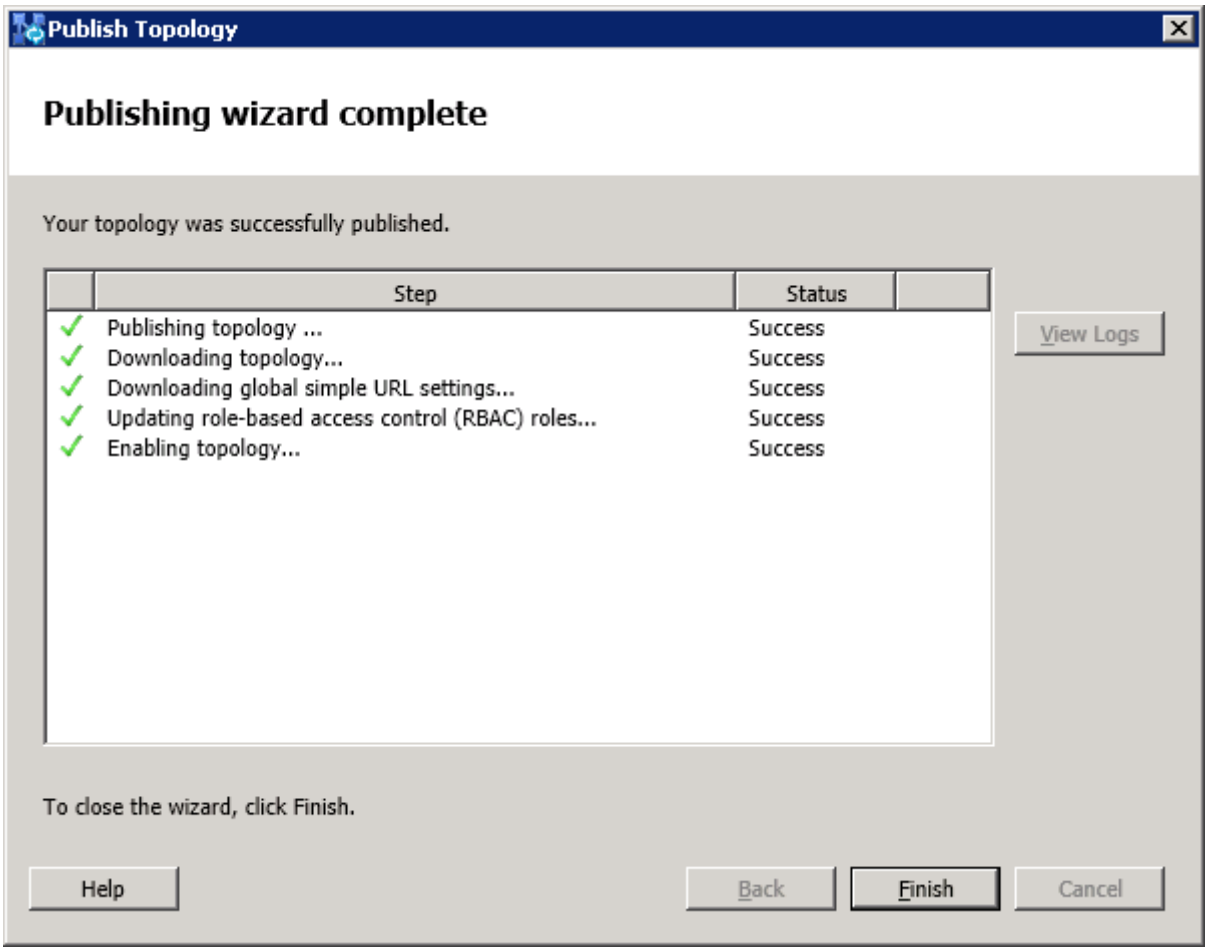
11. Click **Next**; the Topology Builder starts publishing your topology:

Figure 3-12: Publish Topology Progress Screen



12. Wait for the publishing topology process to successfully complete:

Figure 3-13: Publish Topology Successfully Completed



13. Click **Finish**.

3.2 Configuring 'Route' on Lync Server 2013

This section shows how to configure a 'Route' on the Lync Server 2013 and to associate it with the E-SBC PSTN gateway.

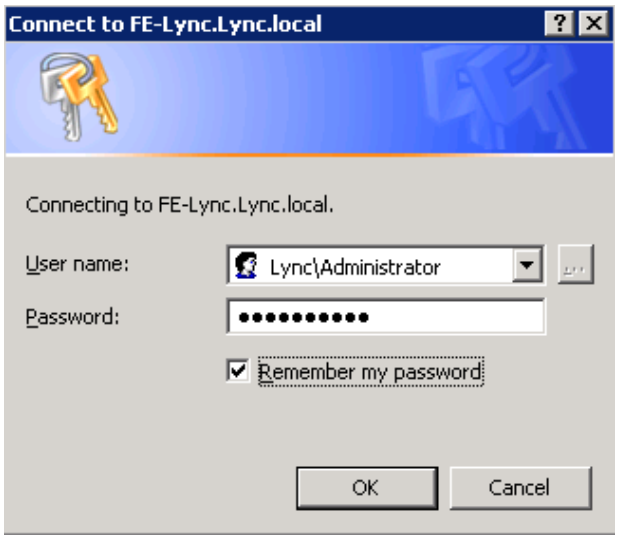
➢ **To configure a 'route' on Lync Server 2013:**

1. Start the Microsoft Lync Server 2013 Control Panel: Click **Start** > **All Programs** > **Microsoft Lync Server 2013** and then click **Lync Server Control Panel**:

Figure 3-14: Opening the Lync Server Control Panel

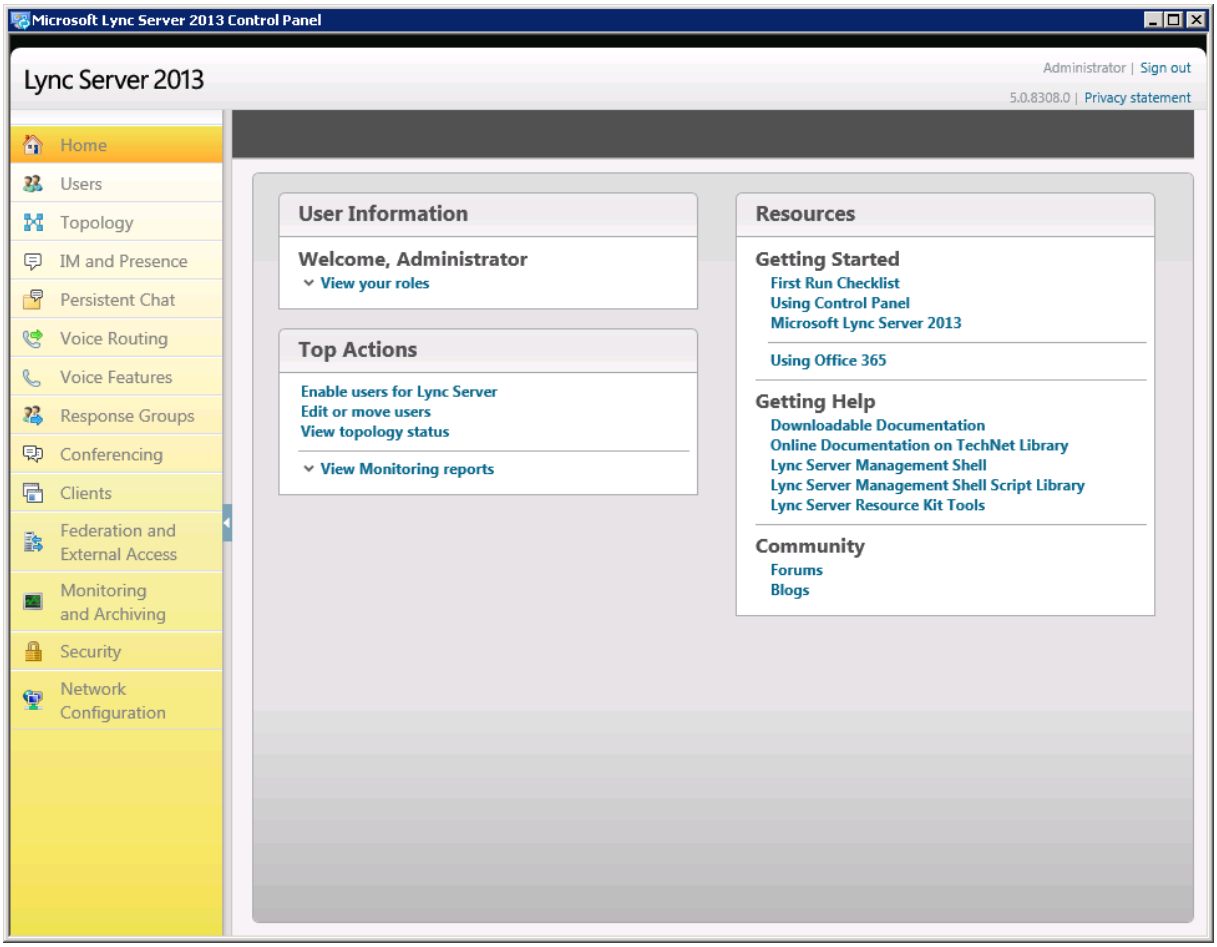
You're prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



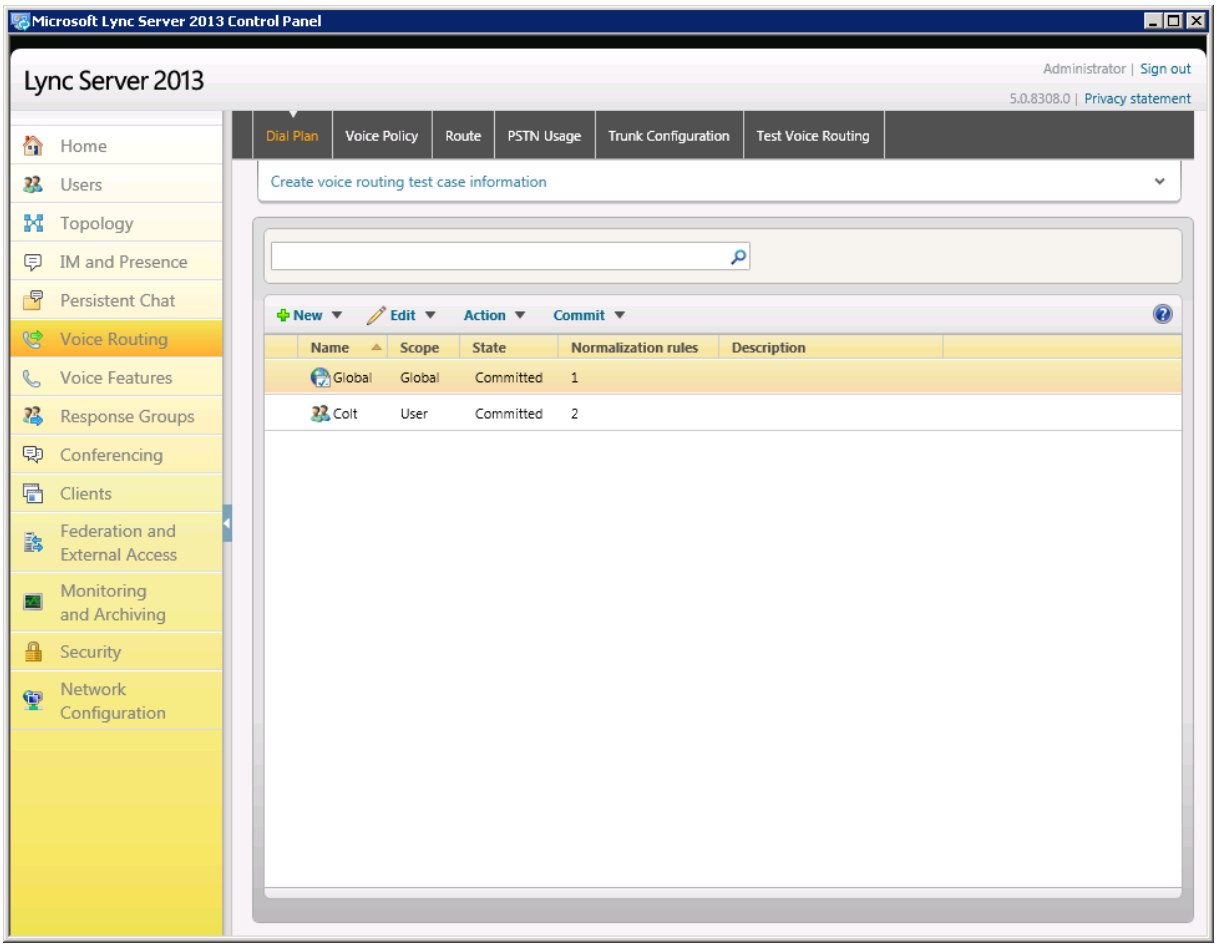
2. Enter your domain 'User name' and 'Password' and click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



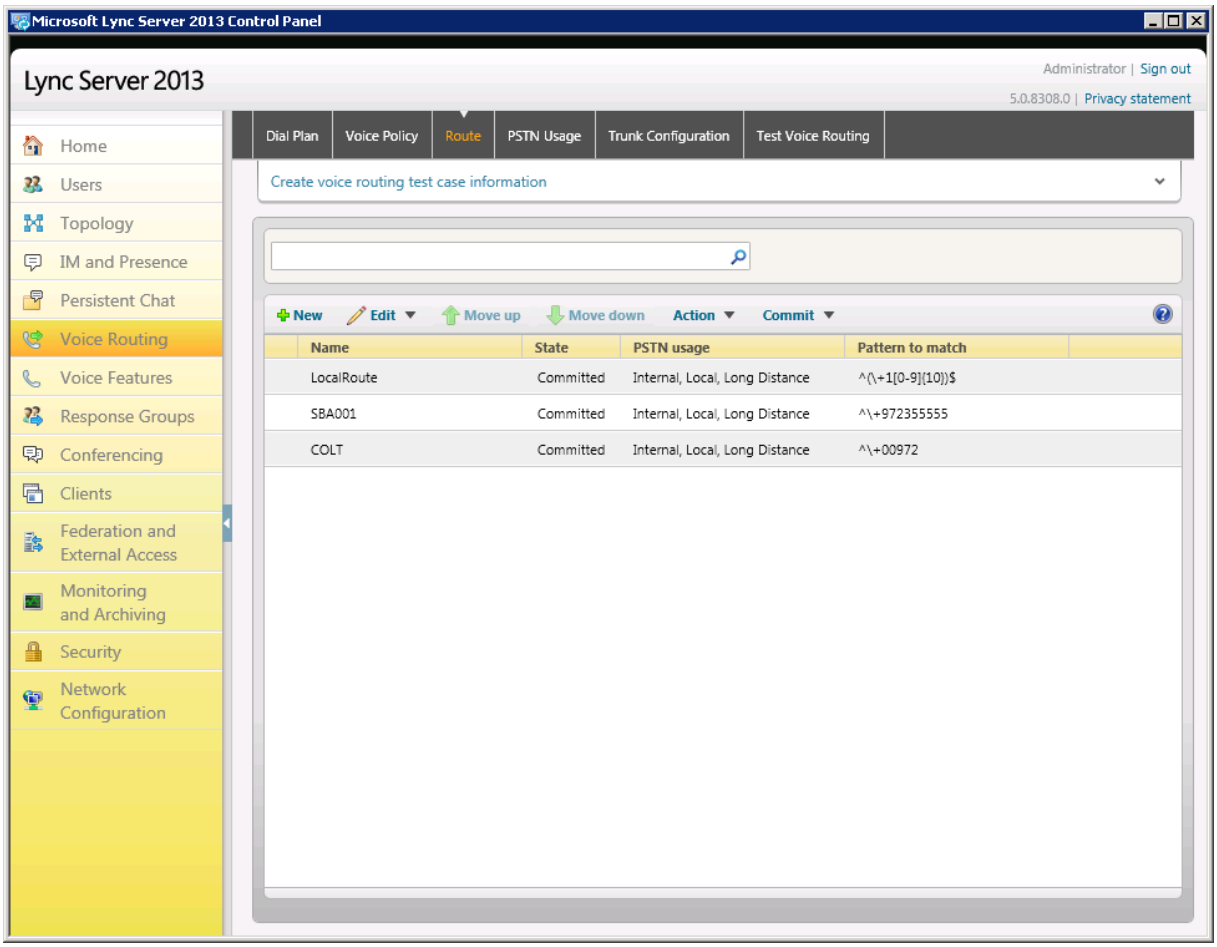
3. In the left navigation pane, select **Voice Routing**:

Figure 3-17: Voice Routing



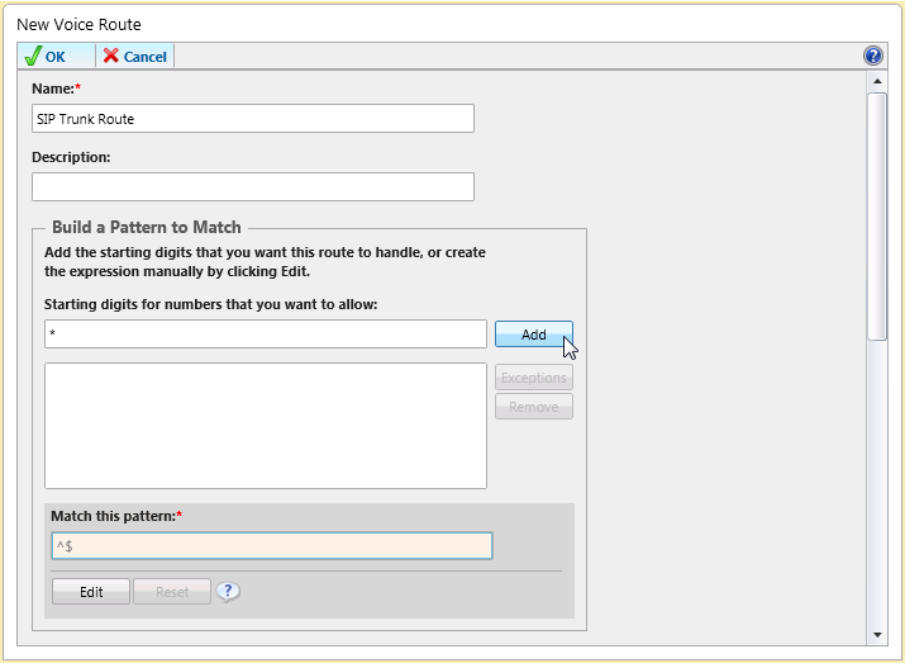
4. In the Voice Routing page, click the **Route** tab:

Figure 3-18: Route Option



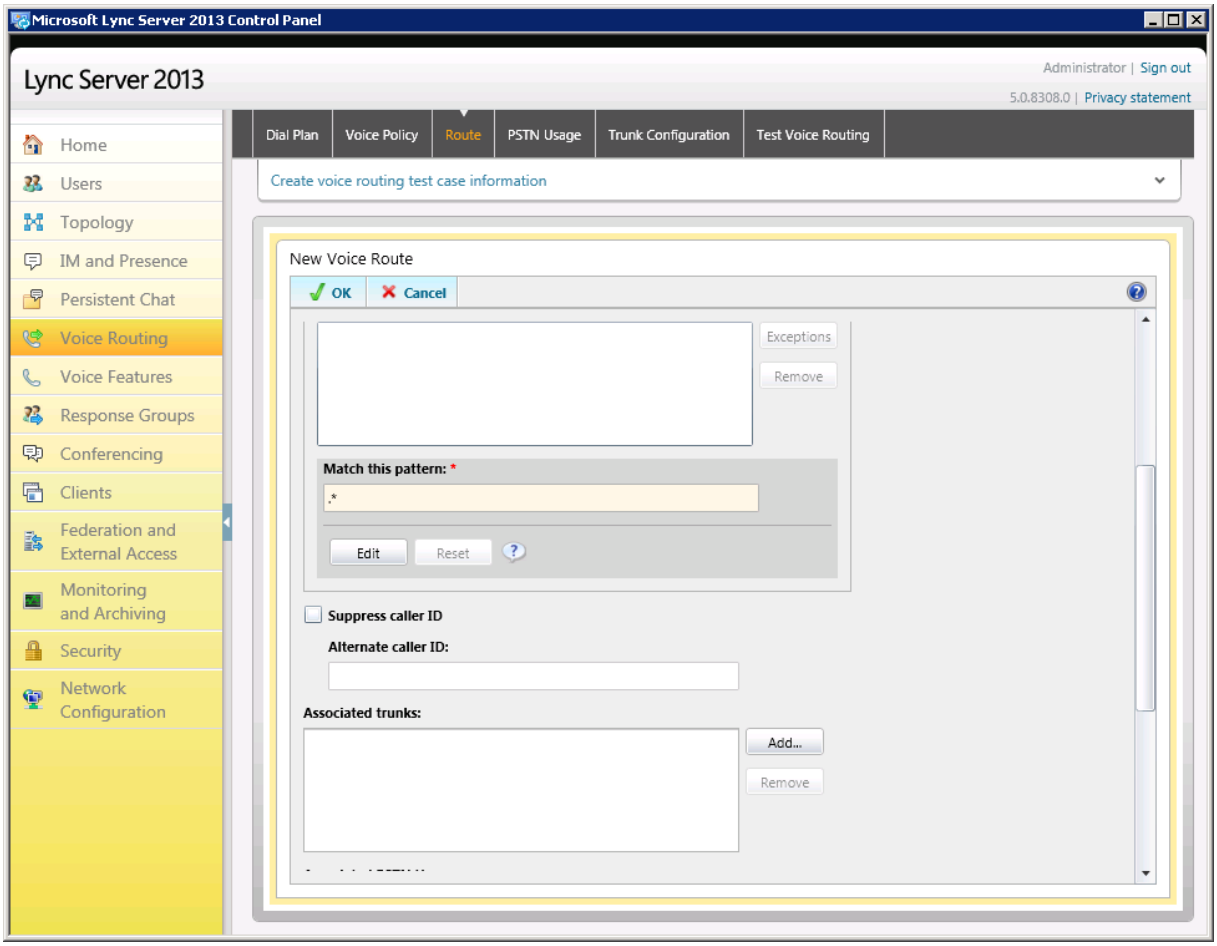
5. Click **New**; the New Voice Route dialog opens:

Figure 3-19: Adding New Voice Route



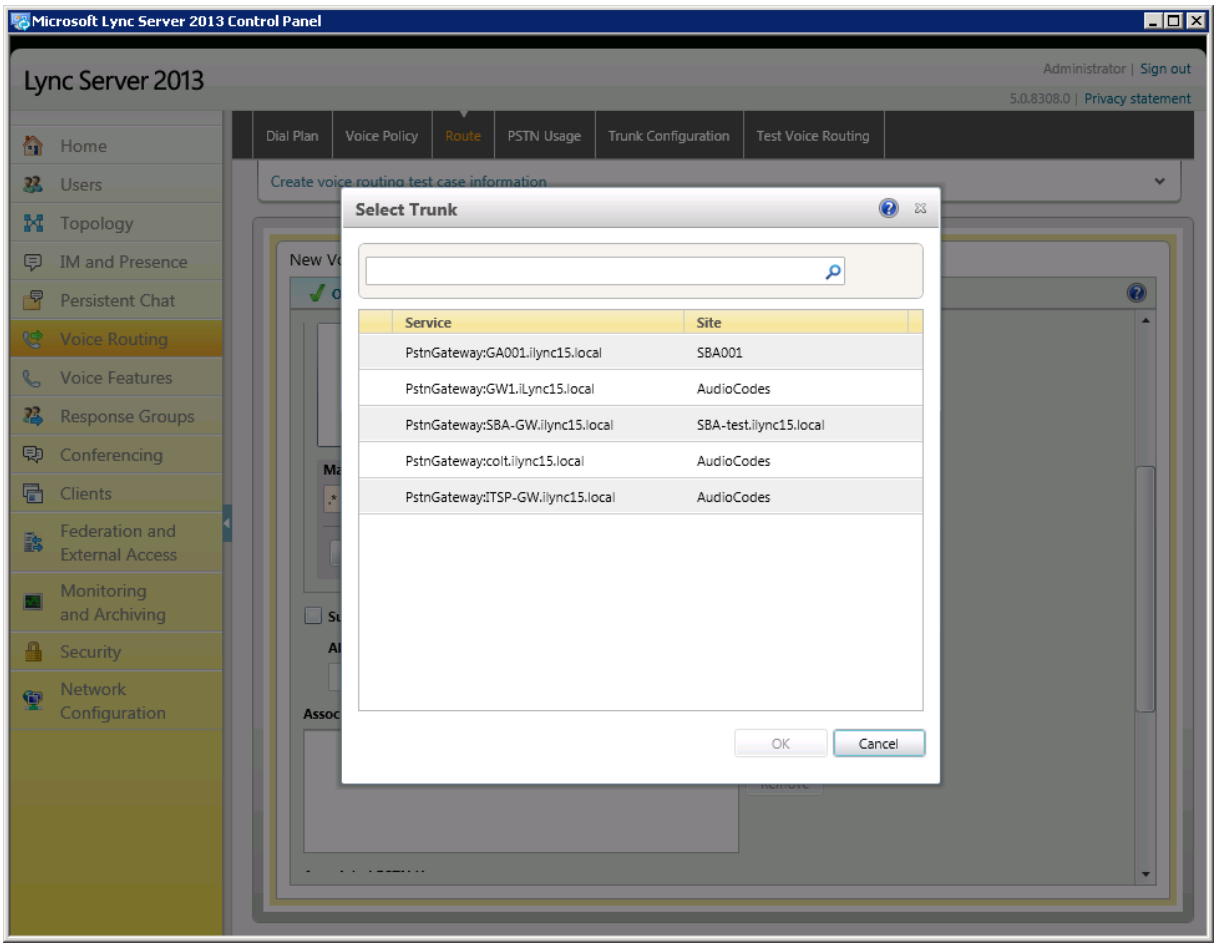
6. In the 'Name' field, enter a name for this route (e.g., SIP Trunk Route).
7. In the 'Build a Pattern to Match' field, enter the starting digits you want this route to handle (e.g., *, i.e., to match all numbers).
8. Click **Add**.

Figure 3-20: Adding New Trunk



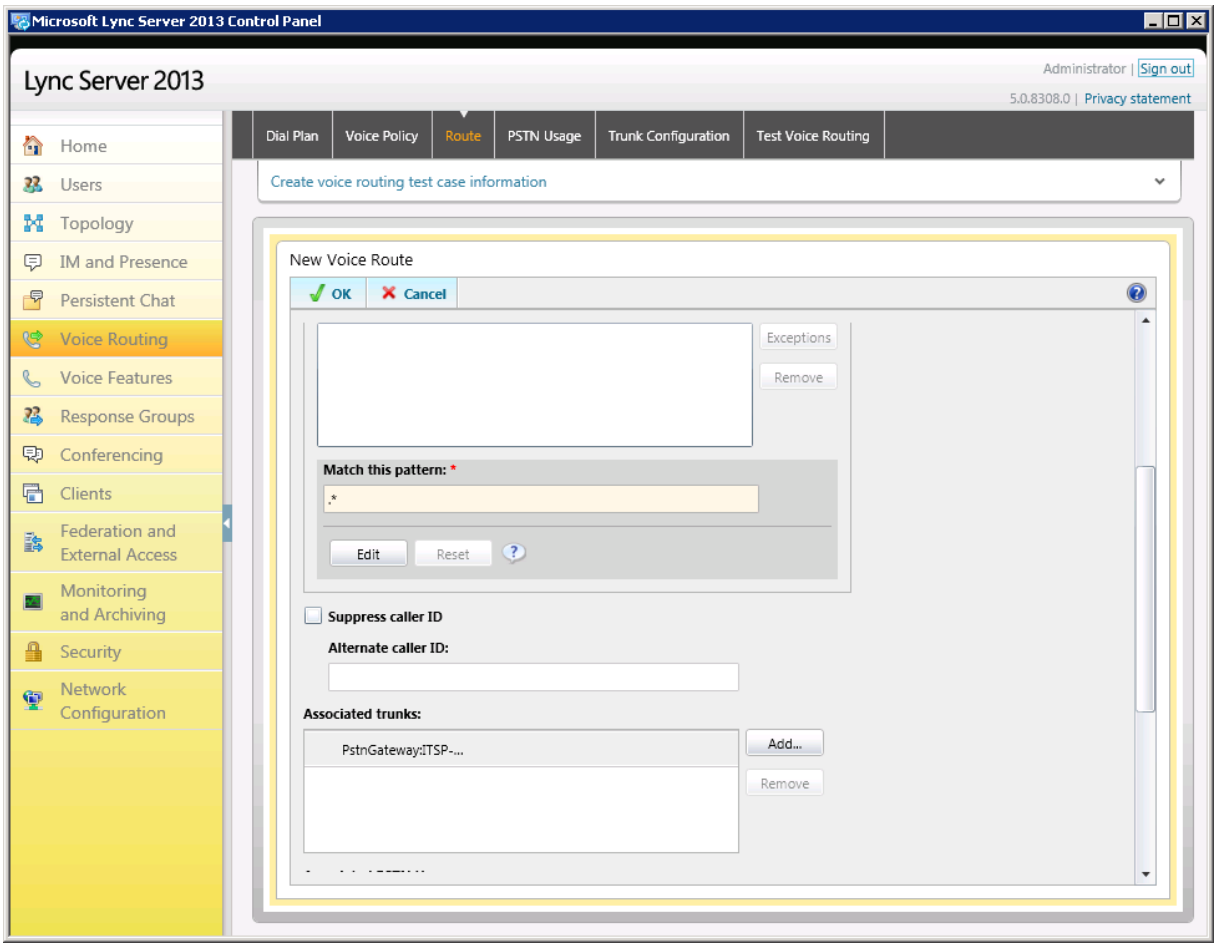
9. Associate the route with the E-SBC Trunk that you created:
   a. In the Associated Trunks pane, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



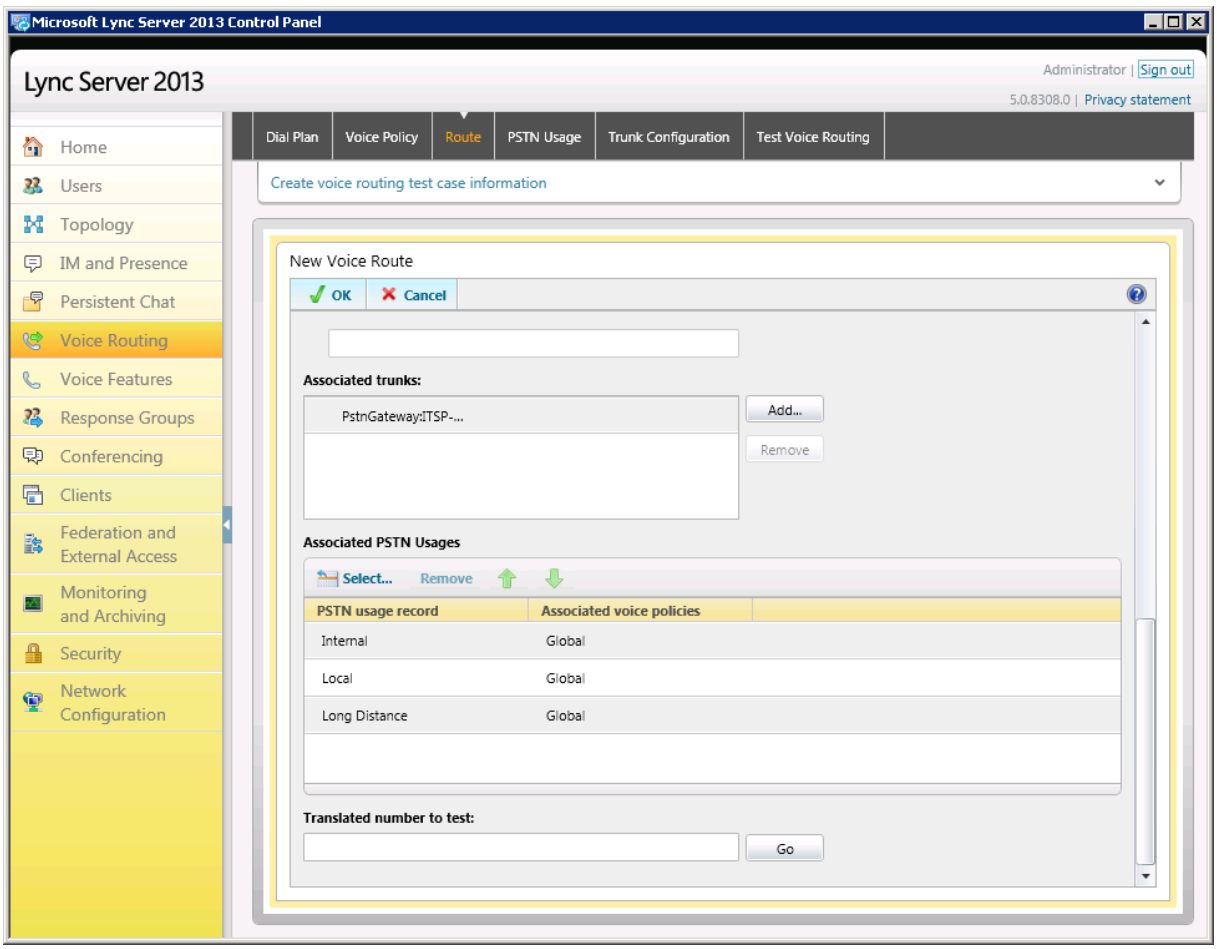
b. Select the E-SBC Trunk you created and click **OK**:

Figure 3-22: Selected E-SBC Trunk



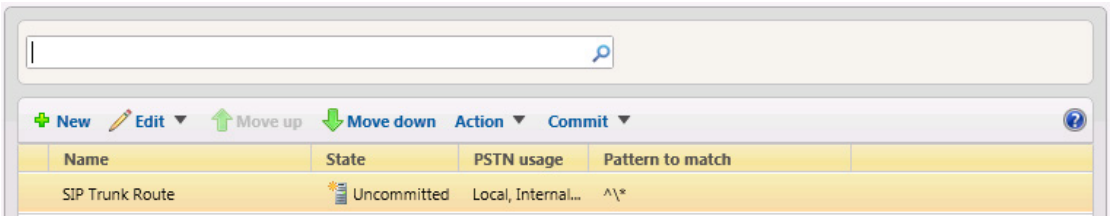
10. Associate a PSTN Usage with this route: In the Associated PSTN Usages group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage with the Route



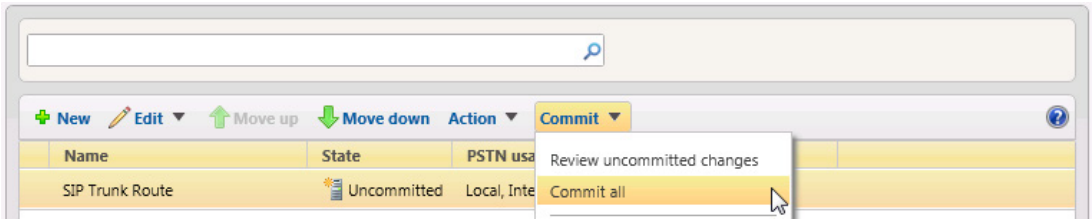
11. Click **OK** (located under the New Voice Route section); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



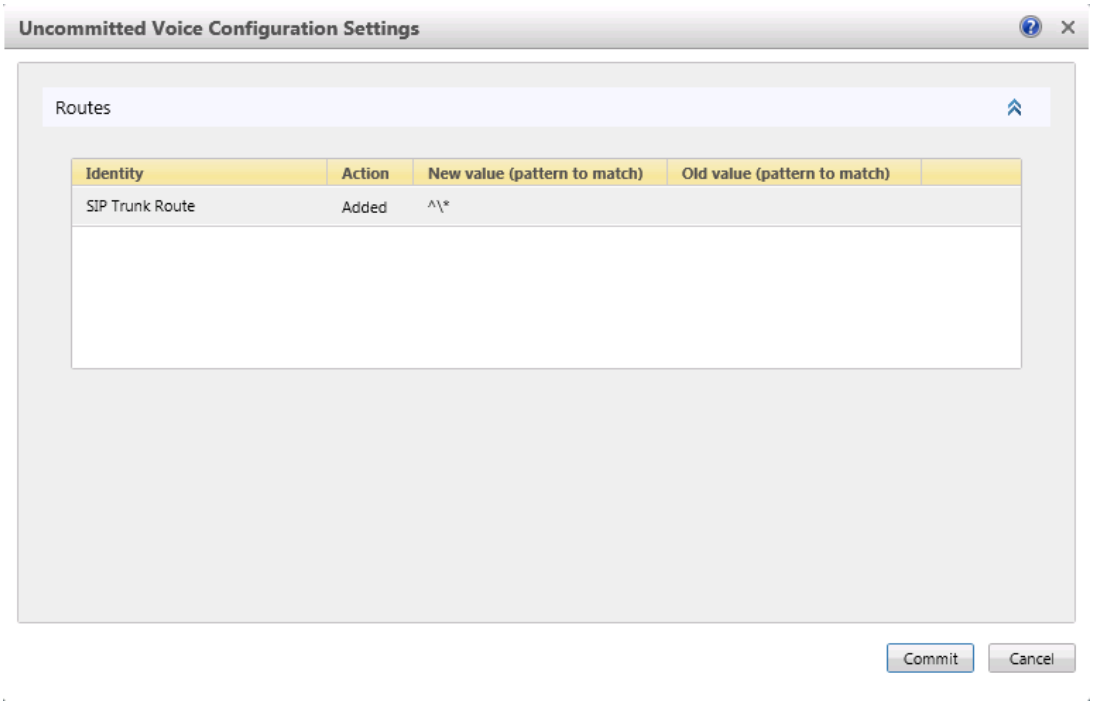
12. From the **Commit** drop-down list, choose **Commit all**:

Figure 3-25: Committing Voice Routes



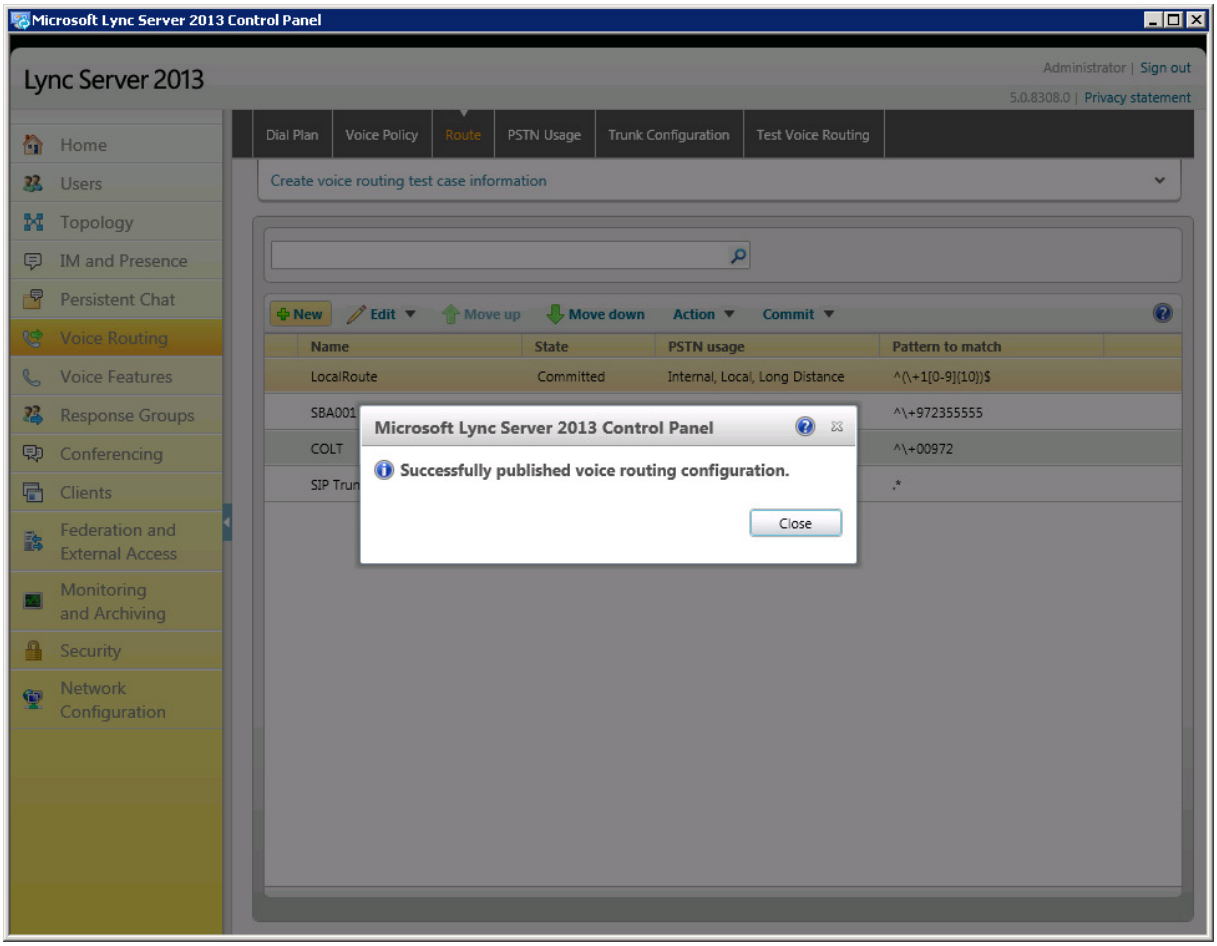
The Uncommitted Voice Configuration Settings dialog opens:

Figure 3-26: Uncommitted Voice Configuration Settings



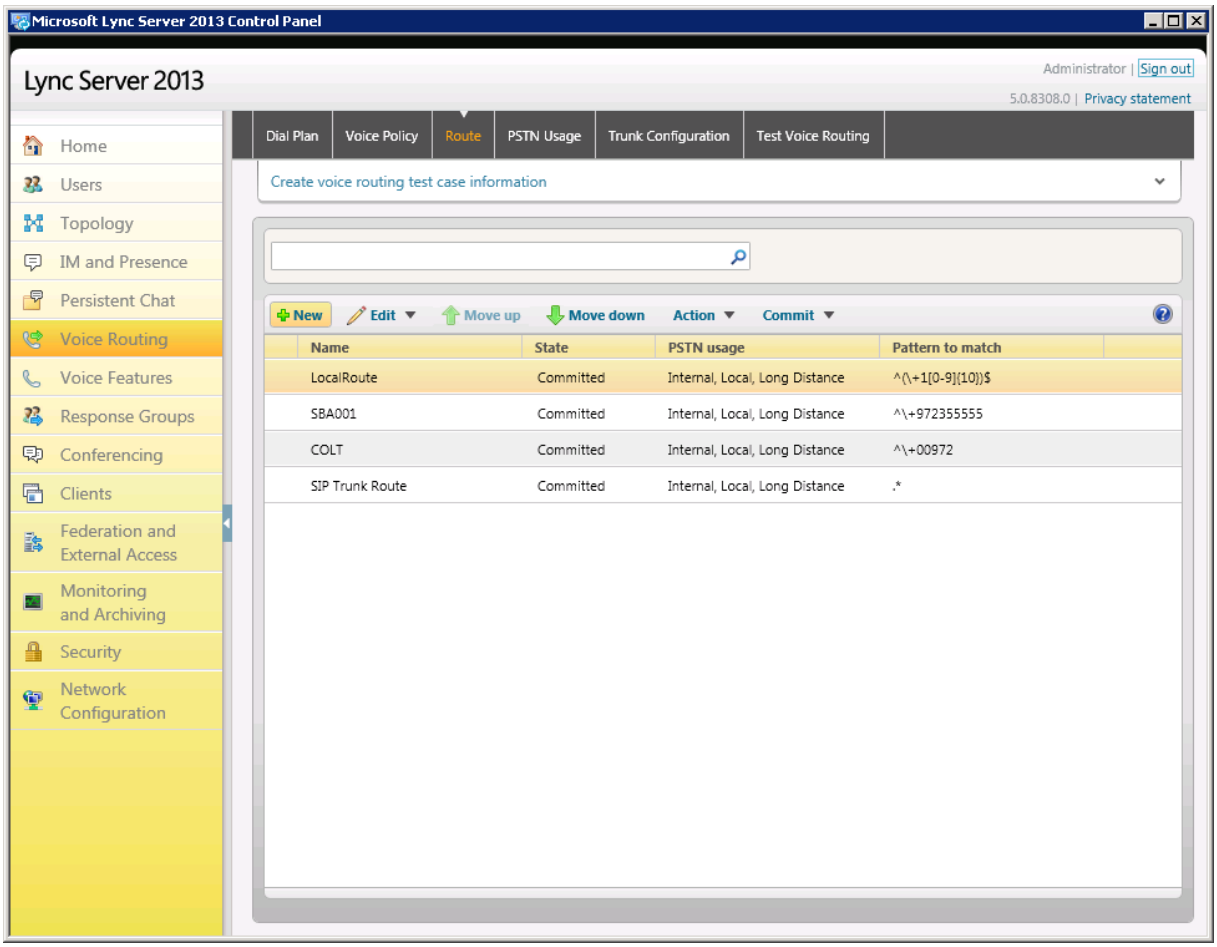
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration:

Figure 3-27: Confirmation of a Successful Voice Routing Configuration



14. Click **Close**; the newly committed Route is displayed in the Voice Routing screen:

Figure 3-28: Voice Routing Screen Displaying Committed Routes



4 Configuring AudioCodes E-SBC

This section shows how to configure AudioCodes' E-SBC for interworking between Microsoft Lync Server 2013 and an ITSP's SIP Trunk:

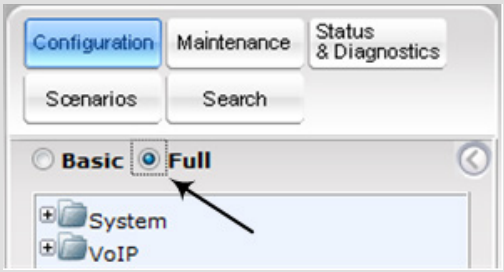
- E-SBC WAN interface: SIP Trunking environment
- E-SBC LAN interface: Lync Server 2013 environment

Configure the E-SBC using the Web-based management interface (embedded Web server).

Notes:

- The E-SBC must be installed with a Software Feature Key that includes the following items:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

  For more information about the Key, contact your AudioCodes representative.
- The scope of this document does *not* cover security aspects of connecting a SIP Trunk to the Microsoft Lync environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, see the *Recommended Security Guidelines Technical Note*.
- The E-SBC must be installed with SIP firmware version 6.6 or later.
- Before beginning to configure the E-SBC, select the **Full** option in the Web interface to display the full Navigation tree:



  When the E-SBC is reset, the Web interface reverts to **Basic** display.
- This document applies to Microsoft Lync 2013 *and* to Microsoft Lync 2010.

4.1 Step 1: Configuring the E-SBC's Network Interfaces

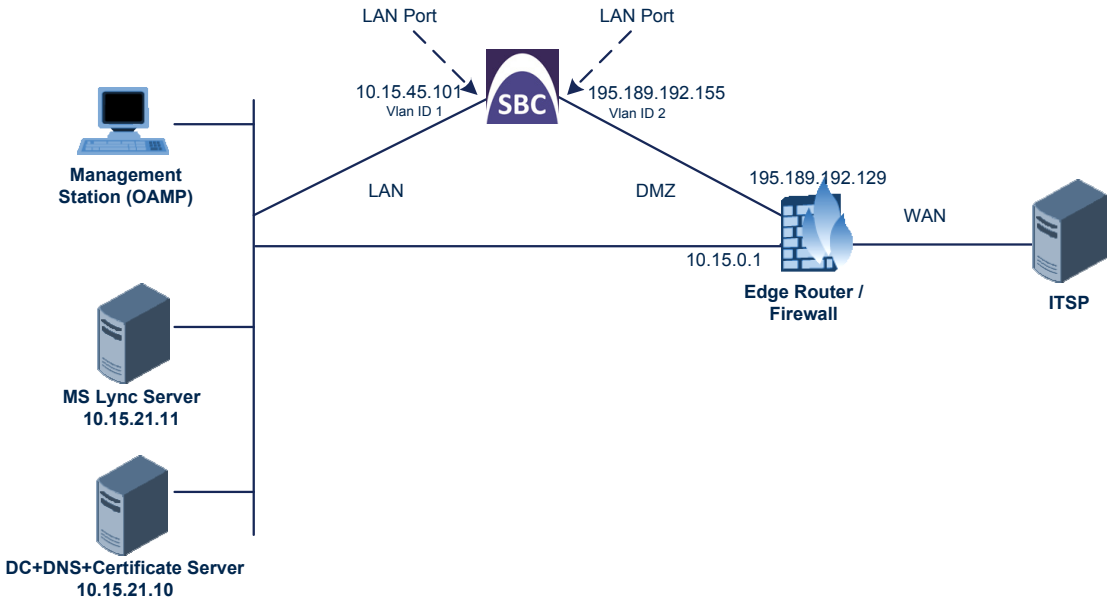
The subsections below show how to configure the E-SBC's network interfaces. Several methods can be used. The scenario exemplified in this document uses this method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the SIP Trunk 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, the 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: Network Interfaces



4.1.1 Configuring IP Network Interfaces for LAN and WAN

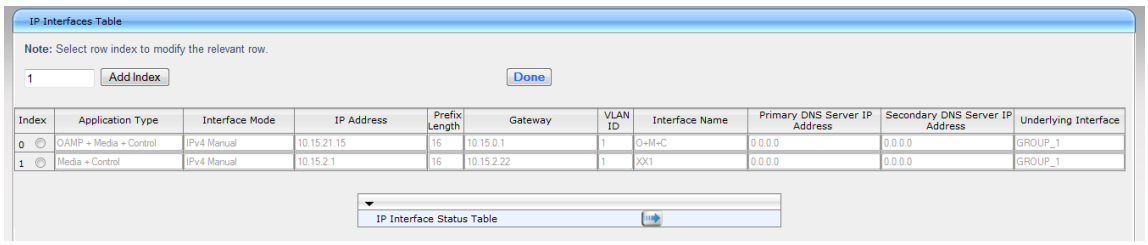
This subsection shows how to configure IP network interfaces for:

- LAN VoIP (Voice)
- WAN VoIP (WANSP)

➢ **To configure the interfaces:**

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** > **Network Settings** > **IP Interfaces Table**).

Figure 4-2: IP Interfaces Table



2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button adjacent to Application Type **OAMP + Media + Control** and click **Edit**.
   b. Configure like this:

Parameter	Example Setting for IPv4	Example Setting for IPv6
Application Type	**OAMP + Media + Control** (application)	**Media + Control**. The OAMP application can be configured only with IPv4.
Interface Mode	See IPv4 in the E-SBC documentation.	See IPv6 in the E-SBC documentation.
IP Address	"10.15.45.101" (E-SBC IP address)	"2001::101" (only a global address can be entered)
Prefix Length	"16" for 255.255.0.0 (Subnet mask, in bits)	"64" (only 64 is supported)
Gateway	Default Gateway "10.15.0.1"	"2001::1"
VLAN ID	VLAN ID. "1".	"1"
Interface Name	Arbitrary descriptive name "Voice"	"IP6Voice"
Primary DNS Server IP Address	DNS IP address "10.15.21.10"	"2001::10"
Underlying Interface	**GROUP_1** (Ethernet port group)	**GROUP_1**

3. Add another network interface for the WAN side:
   a. Enter **1** and click **Add Index**.
   b. Configure like this:

Parameter	Example Setting for IPv4	Example Setting for IPv6
Application Type	**Media + Control** (application)	**Media + Control**
Interface Mode	See IPv4 in the E-SBC documentation.	See IPv6 in the E-SBC documentation.
IP Address	"195.189.192.155" (WAN IP address)	"2002::155"
Prefix Length	"16" for 255.255.0.0	"64" (only 64 is supported)
Gateway	"195.189.192.129" (Default Gateway - router's IP address)	"2002::129"
VLAN ID	"2" (WAN VLAN ID)	"2"
Interface Name	"WANSP" (arbitrary descriptive name of WAN interface)	"IP6WANSP"
Primary DNS Server IP Address	"80.179.52.100" (DNS IP address)	2001:4860:4860::8888
Secondary DNS Server IP Address	"80.179.55.100" (DNS IP address)	2001:4860:4860::8844
Underlying Interface	**GROUP_2** (Ethernet port group)	**GROUP_2**

4. Click **Apply** and **Done**.

4.1.2 Configuring the Native VLAN ID

This subsection shows how to configure the Native VLAN ID for the two network interfaces (LAN and WAN).

➢ **To configure the Native VLAN ID for the LAN and WAN interfaces:**

1. Open the Physical Ports Settings page (**Configuration** tab> **VoIP** > **Network** > **Physical Ports Table**).
2. In the **GROUP_1** member ports, set the 'Native Vlan' field to 1; this VLAN is assigned to network interface Voice.
3. In the **GROUP_2** member ports, set the 'Native Vlan' field to 2; this VLAN is assigned to network interface WANSP.

Figure 4-3: Ports Native VLAN

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

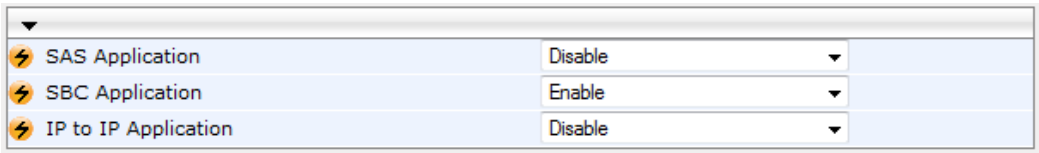
4.2 Step 2: Enabling the SBC Application

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: Applications Enabling



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 73).

4.3 Step 3: Configuring SRDs

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

4.3.1 Configuring 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.

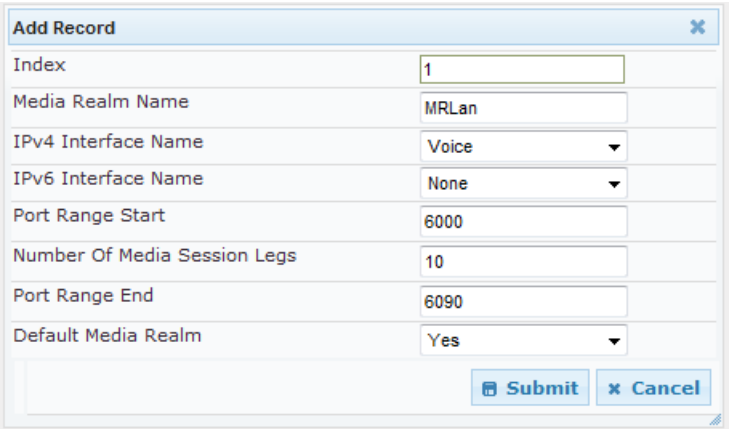
Simplest is to configure one Media Realm for internal (LAN) traffic and another for external (WAN) traffic as shown below, applied to the example scenario.

➢ **To configure Media Realms:**

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

Parameter	Example Setting
Index	"1"
Media Realm Name	"MRLan" (an arbitrary name)
IPv4 Interface Name	**Voice** (the interface name)
IPv6 Interface Name	**IP6Voice** (the interface name). Note: Only applicable if using IPv6.
Port Range Start	"6000" (a number representing the lowest UDP port number to be used for media on the LAN)
Number of Media Session Legs	"10" (the number of media sessions assigned with the port range)

Figure 4-5: Configuring a LAN Media Realm

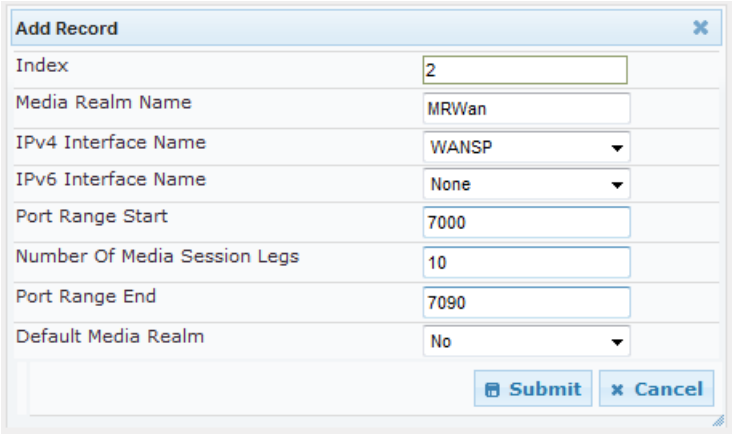


   c. Click **Submit**.

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

Parameter	Example Setting
Index	"2"
Media Realm Name	"MRWan" (an arbitrary name)
IPv4 Interface Name	**WANSP** (the interface name)
IPv6 Interface Name	**IP6WANSP** (the interface name) Note: Only applicable if using IPv6.
Port Range Start	"7000" (a number representing the lowest UDP port number to be used for media on the WAN)
Number of Media Session Legs	"10" (the number of media sessions assigned with the port range)

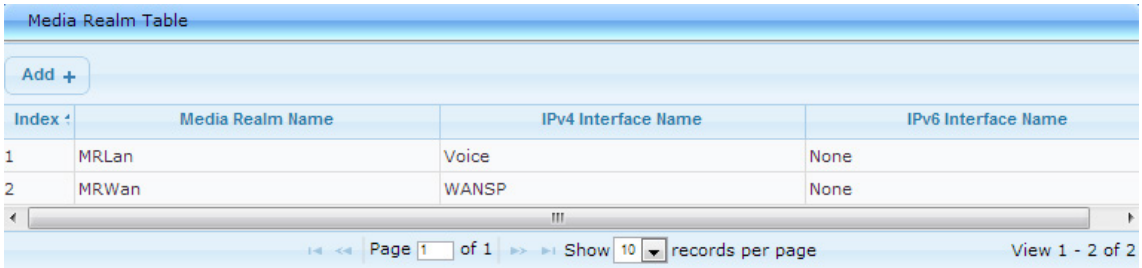
Figure 4-6: Configuring a WAN Media Realm



   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-7: Required Media Realm Table



4.3.2 Configuring SRDs

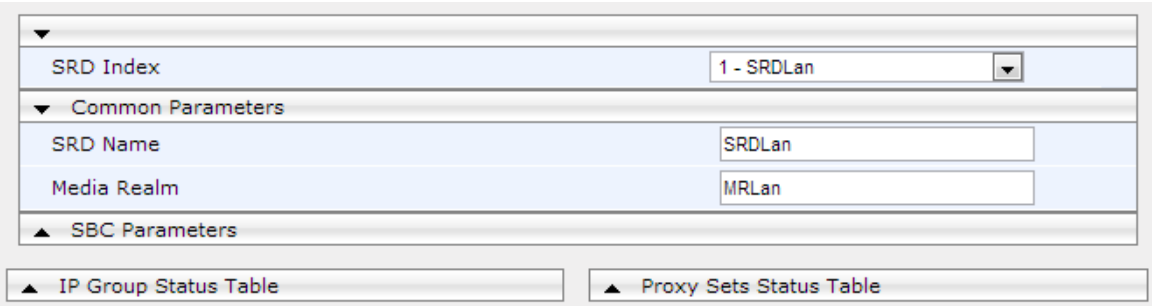
This subsection shows how to configure the SRDs.

➢ **To configure the 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 these parameters:

Parameter	Example Setting
SRD Index	**1**
SRD Name	"SRDLan" (descriptive name for the SRD)
Media Realm	"MRLan" (associates the SRD with a Media Realm)

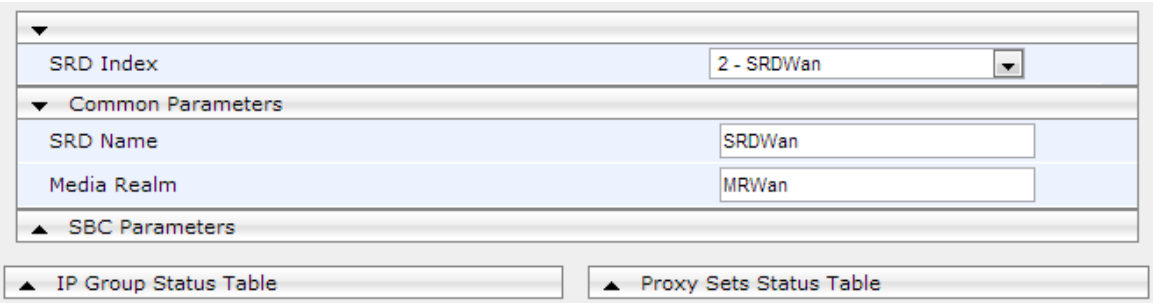
Figure 4-8: Configuring the LAN SRD



   b. Click **Submit**.
3. Add an SRD for the E-SBC's external interface (toward the SIP Trunk):
   a. Configure these parameters:

Parameter	Example Setting
SRD Index	**2**
SRD Name	"SRDWan" (descriptive name for the SRD)
Media Realm	"MRWan" (associates the SRD with a Media Realm)

Figure 4-9: Configuring the WAN SRD



   b. Click **Submit**.

4.3.3 Configuring 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 the example scenario, an internal and external SIP interface must be added 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 these parameters:

Parameter	Example Setting
Index	"1"
Network Interface	"Voice" (for IPv4) / "IP6Voice" (for IPv6)
Application Type	**SBC**
TLS Port	"5067"
TCP and UDP	"0"
SRD	"1"

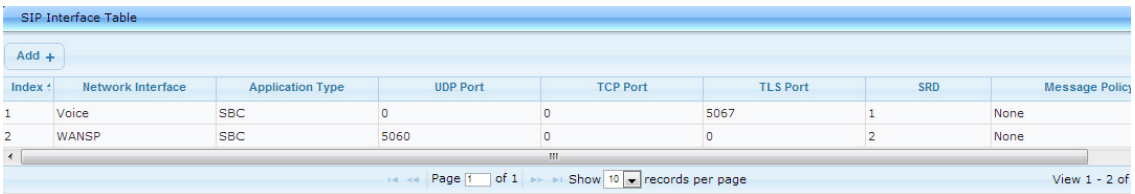
   c. Click **Submit**.
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure these parameters:

Parameter	Example Setting
Index	"2"
Network Interface	"WANSP" (for IPv4) / "IP6WANSP" (for IPv6)
Application Type	**SBC**
UDP Port	"5060"
TCP and TLS	"0"
SRD	"2"

   c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-10: Required SIP Interface Table



4.4 Step 4: Configuring 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, two Proxy Sets must be configured for:

- Microsoft Lync Server 2013
- SIP Trunk

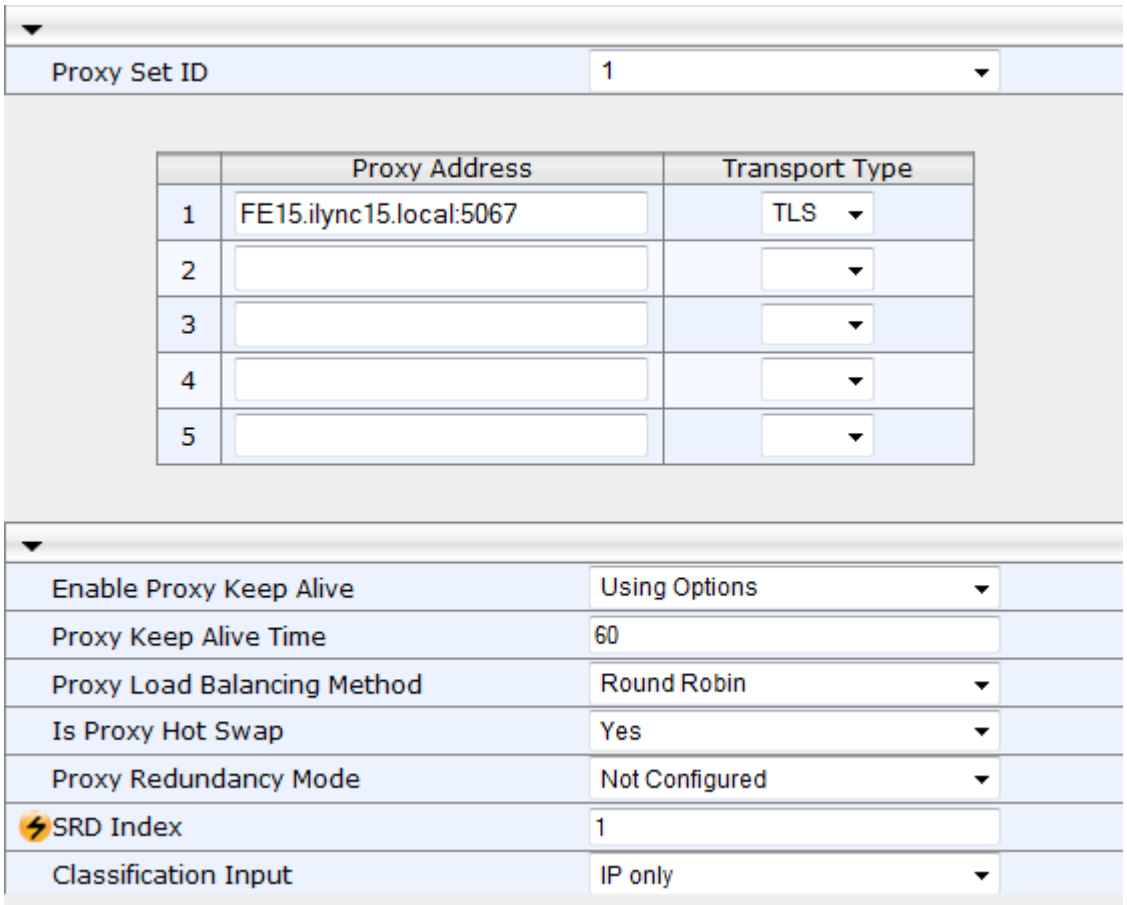
These Proxy Sets will later be associated with IP Groups.

➢ **To add Proxy Sets:**

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

Parameter	Example Setting
Proxy Set ID	**1**
Proxy Address	"FE15.ilync15.local:5067" (the Lync Server 2013 SIP Trunking IP address or FQDN and destination port)
Transport Type	**TLS**
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
SRD Index	"1"

Figure 4-11: Proxy Set for Microsoft Lync Server 2013



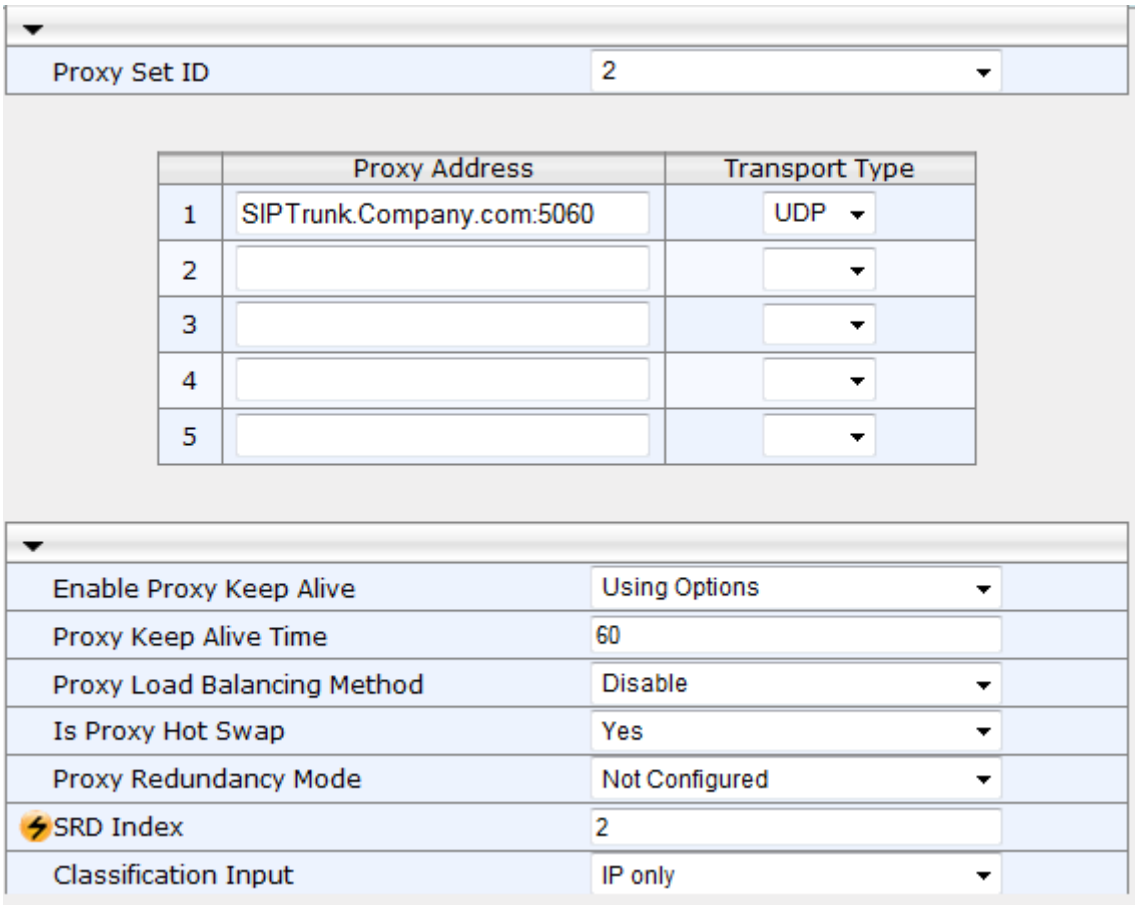
b. Click **Submit**.

3. Add a Proxy Set for the SIP Trunk:

a. Configure these parameters:

Parameter	Example Setting
Proxy Set ID	**2**
Proxy Address	"SIPTrunk.Company.com:5060" (SIP Trunk IP address or FQDN and destination port)
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	"2" (enables classification by Proxy Set for this SRD in the IP Group belonging to the SIP Trunk)

Figure 4-12: Configuring a Proxy Set for the SIP Trunk



b. Click **Submit**.

4.5 Step 5: Configuring 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 the example scenario, IP Groups are created for:

- Lync Server 2013 (Mediation Server) on the LAN
- SIP Trunk on the WAN

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** > **Control Network** > **IP Group Table**).
2. Add an IP Group for the Lync Server 2013 Mediation Server:
   a. Click **Add**.
   b. Configure the parameters like this:

Parameter	Example Setting
Index	"1"
Type	**Server**
Description	"Lync Server" (a descriptive name)
Proxy Set ID	"1"
SRD	"1"
Media Realm Name	"MRLan"
IP Profile ID	"1"

   c. Click **Submit**.
3. Add an IP Group for the SIP Trunk:
   a. Click **Add**.
   b. Configure the parameters like this:

Parameter	Example Setting
Index	"2"
Type	**Server**
Description	"SIP Trunk" (a descriptive name)
Proxy Set ID	"2"
SRD	"2"
Media Realm Name	"MRWan"
IP Profile ID	"2"

   c. Click **Submit**.

The figure below shows the configured IP Group table:

Figure 4-13: Configured IP Group Table

IP Group Table

Add +

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	Local Host Name	SRD	Media Realm Name	IP Profile ID
1	Server	Lync	1				1	LanMR	1
2	Server	SIP Trunk	2				2	WanMR	2

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

4.6 Step 6: Configuring IP Profiles

This step shows how to configure IP Profiles. In the 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 SIP Trunk.

Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 47).

In the example, an IP Profile is added for each entity:

- Microsoft Lync Server 2013 - to operate in secure mode using SRTP and TLS
- SIP trunk - to operate in non-secure mode using RTP and UDP

➢ **To add 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 like this:

Parameter	Example Setting
Profile ID	**1**
Media IP Version Preference	**Only IPv4 / Only IPv6**
Reset SRTP State Upon Re-key	**Enable**
Extension Coders Group ID	**Coders Group 1**
Media Security Behavior	**SRTP**
SBC Remote Early Media RTP	**Delayed** (mandatory because the Lync Server 2013 does not immediately send RTP to the remote side if it sends a SIP 18x response)
RFC 2833 Behavior	**Extend** (in case the SIP Trunk does not send RFC 2833 in SDP)
SBC Remote Update Support	**Supported Only After Connect**
SBC Remote Re-Invite Support	**Supported Only With SDP**
SBC Remote Refer Behavior	**Handle Locally** (mandatory because Lync Server 2013 does not support receive Refer)
SBC Remote 3xx Behavior	**Handle Locally** (mandatory because Lync Server 2013 does not support receive 3xx)
SBC Remote Hold Format	**Inactive**

Figure 4-14: Configured IP Profile for Lync Server 2013

Profile ID	1
Profile Name	Lync
Media IP Version Preference	Only IPv4
Reset SRTP State Upon Re-key	Enable
SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 1
Allowed Coders Group ID	None
Allowed Coders Mode	Restriction
SBC Preferences Mode	Doesn't Include Extensions
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	SRTP
RFC 2833 Behavior	Extend
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Delayed
SBC Remote Can Play Ringback	Yes
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	supported
SBC Early Media Response Type	Transparent
SBC Remote Update Support	Supported Only After Connect
SBC Remote Re-Invite Support	Supported only with SDP
SBC Remote Refer Behavior	Handle Locally
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Handle Locally
SBC Remote Delayed Offer Support	Not Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce
SBC User Registration Time	-1
SBC Remote Hold Format	inactive

b. Click **Submit**.

3. Add an IP Profile for the SIP Trunk:
   a. Configure the parameters like this:

Parameter	Example Setting
Profile ID	**2**
Media IP Version Preference	**Only IPv4 / Only IPv6**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Preference** (enables the received SDP offer to list Allowed coders first and then the original coders received in the SDP).
Media Security Behavior	**RTP**
SBC Remote Refer Behavior	**Handle Locally** (the E-SBC handles the incoming REFER request itself, without forwarding the REFER towards the SIP Trunk)

Note: The SIP Trunk's IP Profile depends on the SIP Trunk behavior. Refer to the explanations of the IP Profile parameters in the *E-SBC User's Manual* in order to configure the profile according to SIP Trunk behavior.

Figure 4-15: Configured IP Profile for SIP Trunk

Profile ID	2
Profile Name	SIP Trunk
Media IP Version Preference	Only IPv4
SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Preference
SBC Preferences Mode	Include Extensions
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Immediate
SBC Remote Can Play Ringback	Yes
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	supported
SBC Early Media Response Type	Transparent
SBC Remote Update Support	Supported
SBC Remote Re-Invite Support	Supported
SBC Remote Refer Behavior	Handle Locally
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Transparent
SBC Remote Delayed Offer Support	Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce

b. Click **Submit**.

4.7 Step 7: Configuring Coders

This step shows how to configure coders (termed *Coder Groups*). You can configure up to four different Coder Groups. As Lync Server 2013 supports the G.711 coder while the network connection to SIP Trunk may restrict you to operate with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.711 coders for Lync Server 2013, and Coder Group with the G.729 coder for the SIP Trunk.

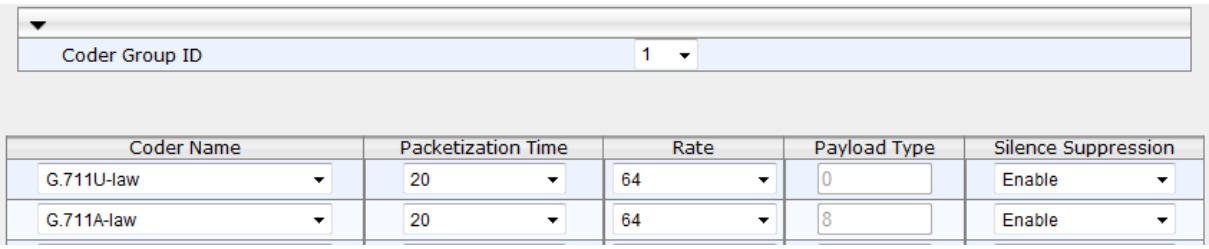
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 49).

➢ **To configure coders:**

1. Add a Coder Group for Lync Server 2013.
   a. Configure the parameters like this:

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

Figure 4-16: Configured Coder Group for Lync Server 2013

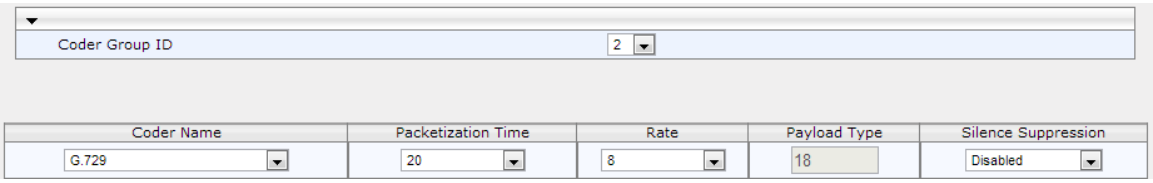


   b. Click **Submit**.

2. Add a Coder Group for SIP Trunk:
   a. Configure the parameters like this:

Parameter	Example Setting
Coder Group ID	**2**
Coder Name	**G.729**

Figure 4-17: Configured Coder Group for the SIP Trunk



   b. Click **Submit**.

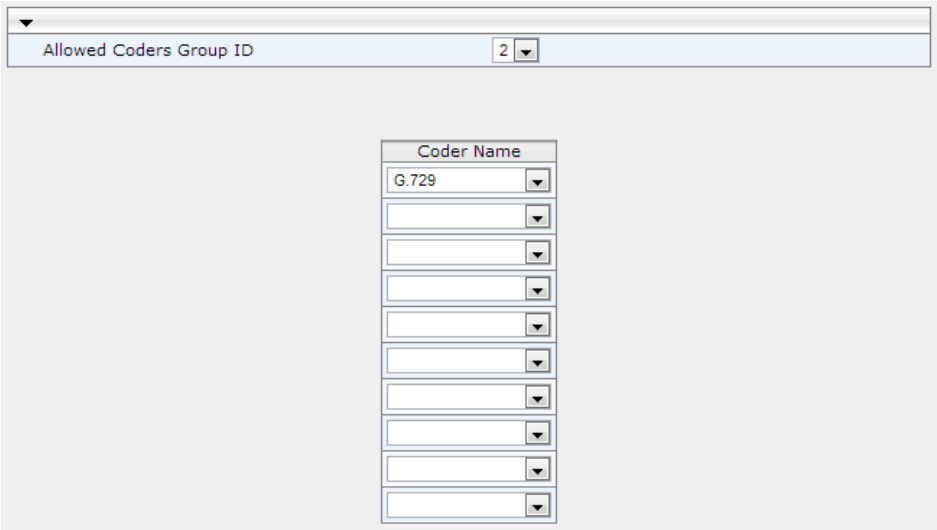
The step below adds an Allowed Coders Group to ensure that voice sent to the SIP Trunk uses the G.729 coder whenever possible.

Note that this Allowed Coders Group ID (and its preference) was assigned to the IP Profile belonging to the SIP Trunk in the previous step (see Section 4.6 on page 49).

➢ To set a preferred coder for the SIP Trunk:

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** > **SBC** > **Allowed Coders Group**).
2. From the 'Allowed Coders Group ID' drop-down list, select **2**.
3. From the 'Coder Name' drop-down list, select **G.729**.

Figure 4-18: Allowed Coders Group for SIP Trunk



4. Click **Submit**.

4.8 Step 8: Configuring a SIP TLS Connection

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

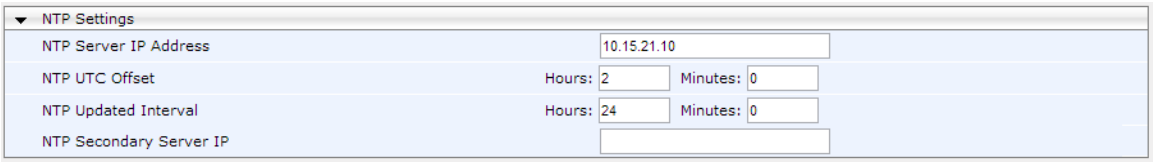
4.8.1 Configuring the NTP Server Address

This step shows how to configure the NTP server's IP address. It's 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**).
2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., 10.15.21.10).

Figure 4-19: Configuring the NTP Server IP Address



3. Click **Submit**.

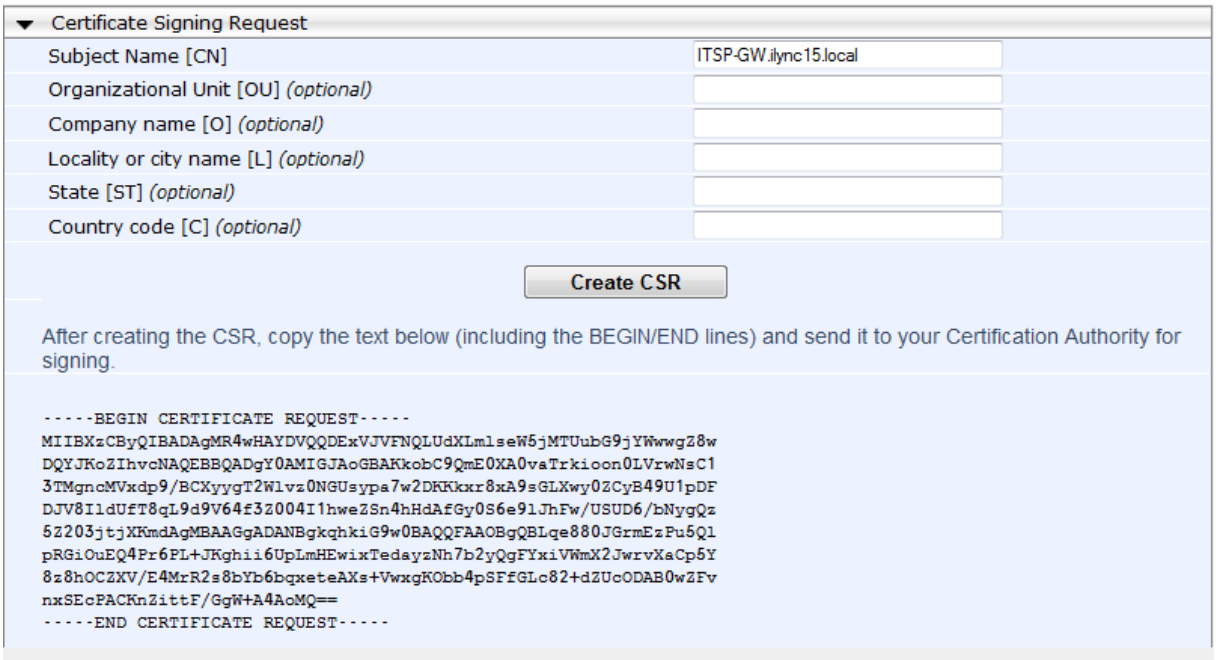
4.8.2 Configuring a Certificate

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 the management station (i.e., the computer used to manage the E-SBC through its embedded Web server).

➢ **To configure a certificate:**

1. Open the Certificates page (**Configuration** tab > **System** > **Certificates**).

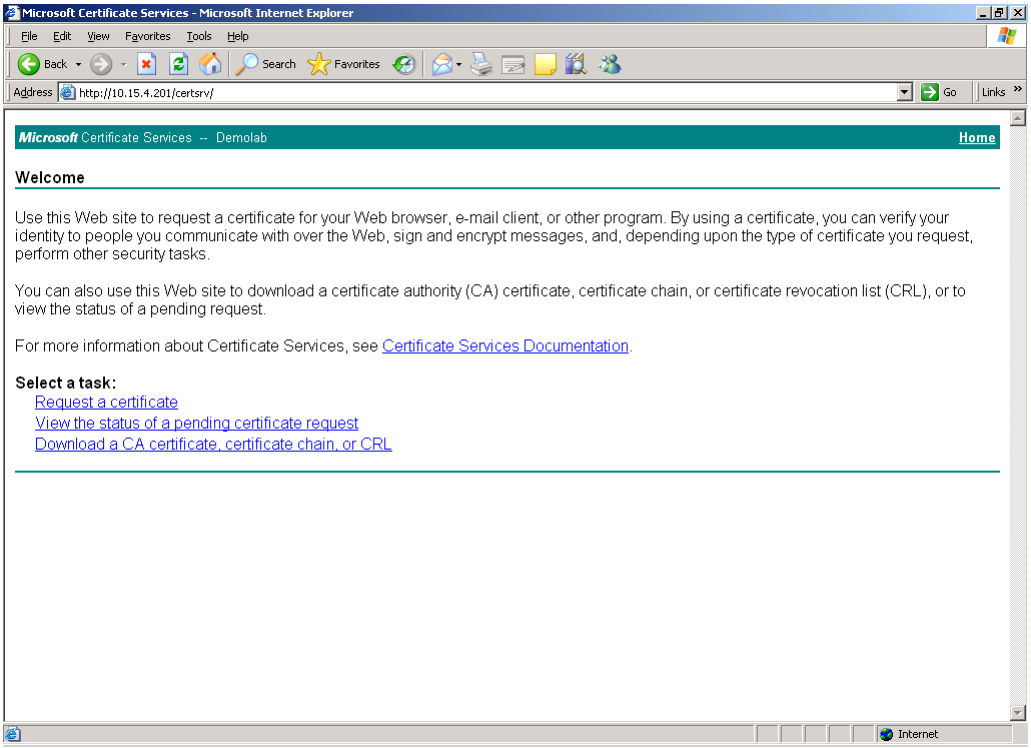
Figure 4-20: Certificates Page - Creating CSR



2. In the 'Subject Name' field, enter the media gateway name (e.g., ITSP-GW.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 15).
3. Click **Create CSR**; a certificate request is generated.
4. Copy the CSR (from the line ----BEGIN CERTIFICATE to the line END CERTIFICATE REQUEST----) to a text file (such as Notepad) and save it to a folder on your computer with the file name *certreq.txt*.

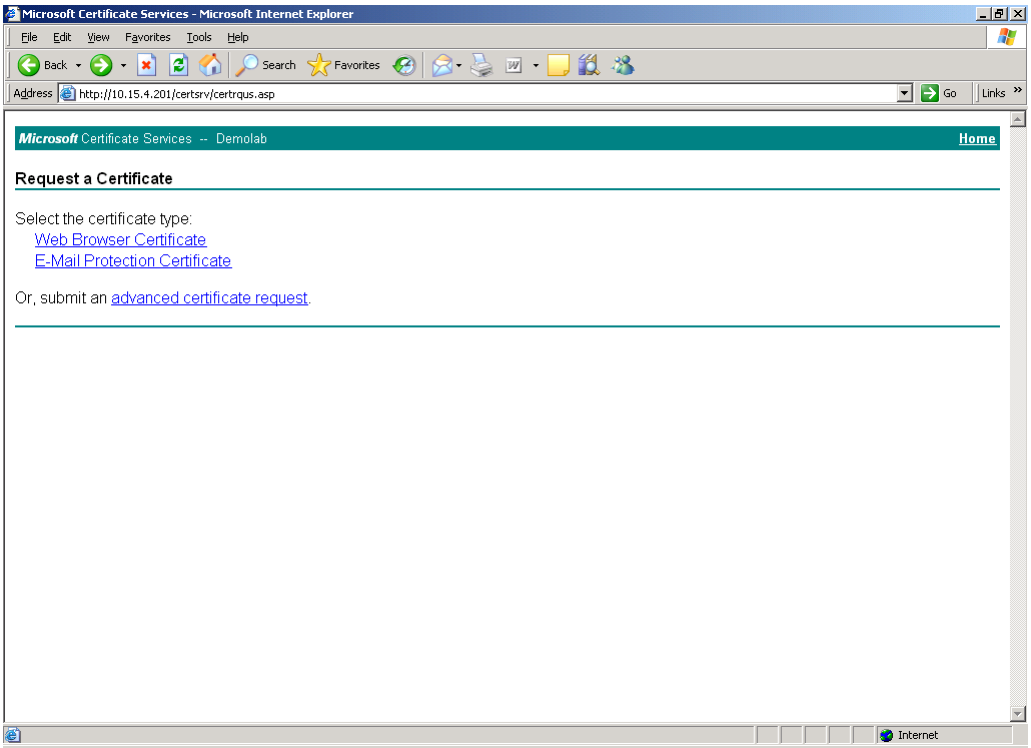
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-21: Microsoft Certificate Services Web Page



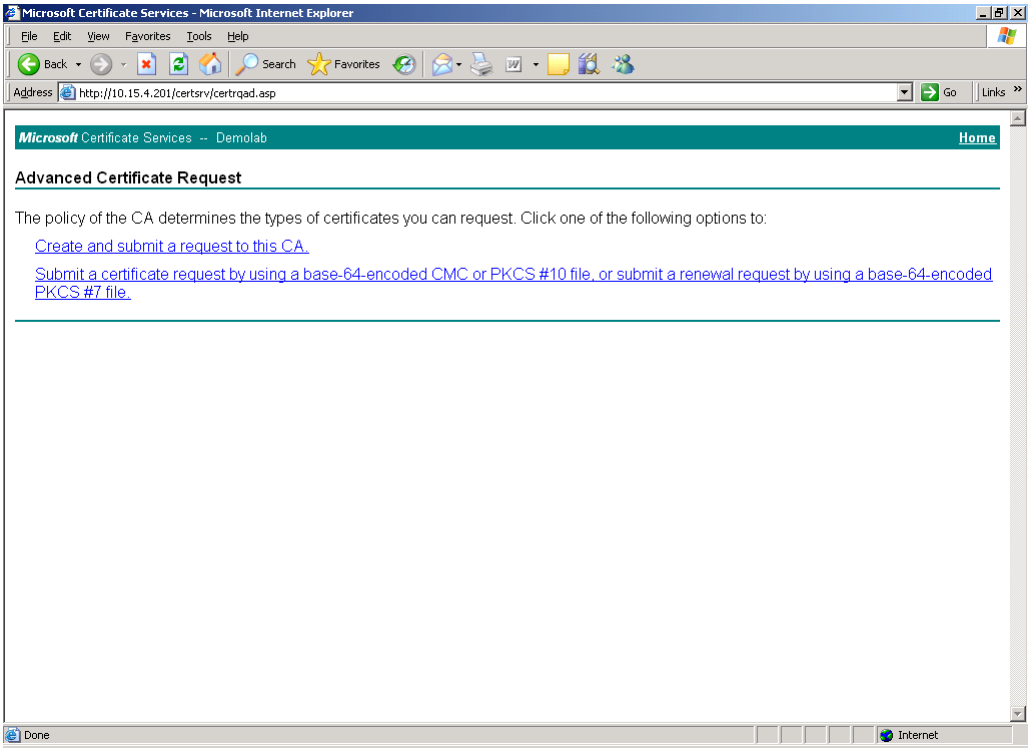
6. Click **Request a certificate**.

Figure 4-22: Request a Certificate Page



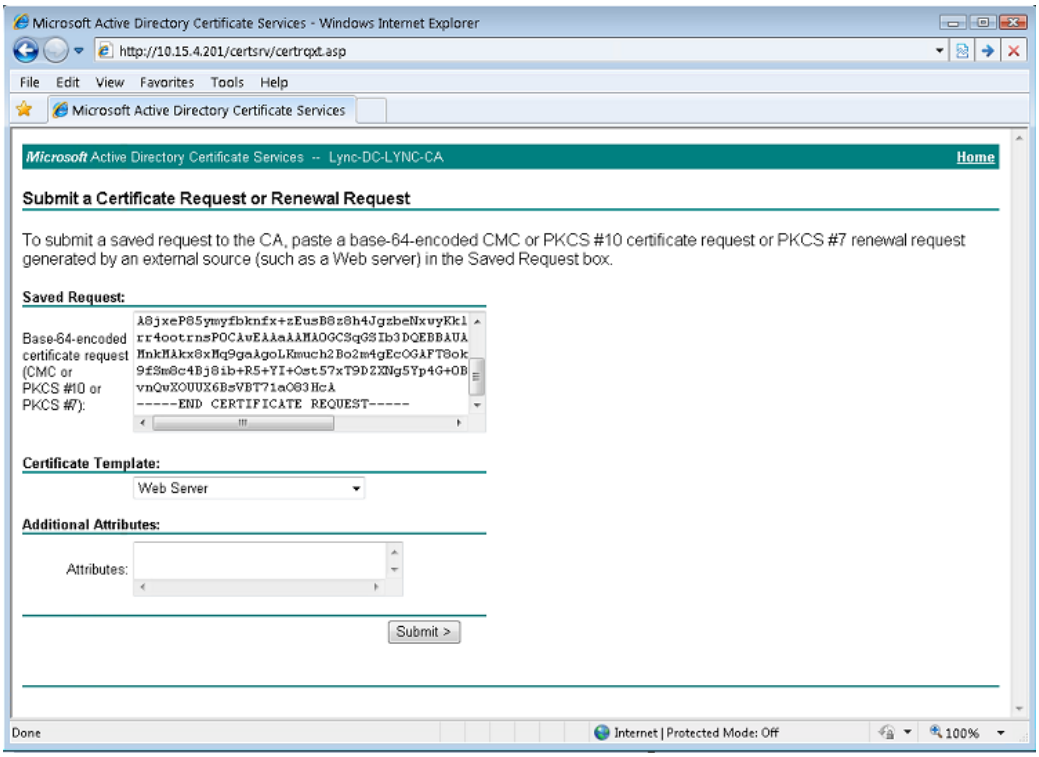
7. Click **advanced certificate request** and click **Next**.

Figure 4-23: Advanced Certificate Request Page



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

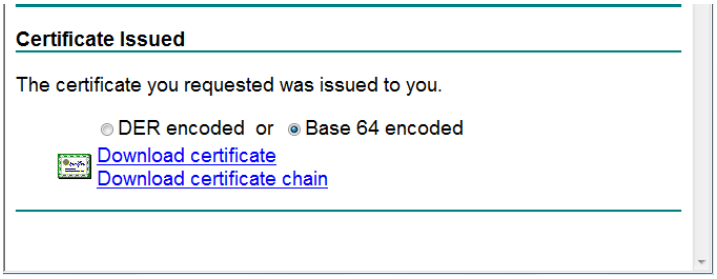
Figure 4-24: Submit a Certificate Request or Renewal Request Page



9. Open the *certreq.txt* file that you created and saved in Step 4 and copy its contents to the 'Base-64-Encoded Certificate Request' field.
10. From the 'Certificate Template' drop-down list, select **Web Server**.

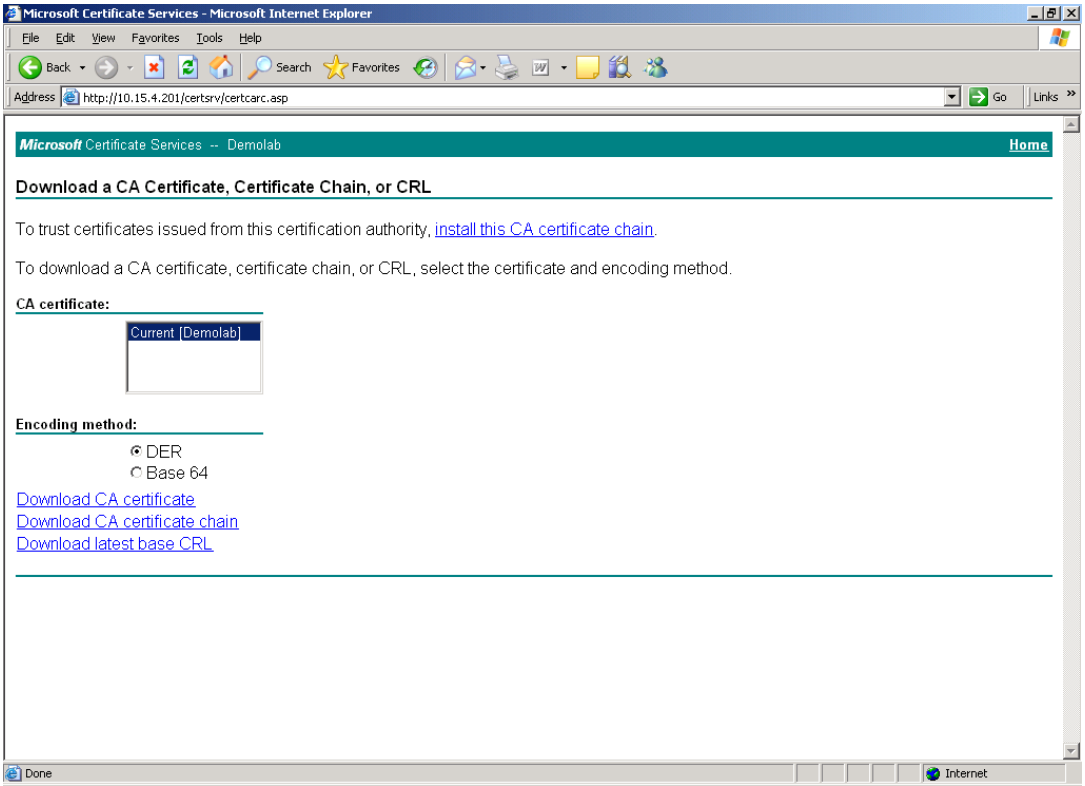
11. Click **Submit**.

Figure 4-25: Certificate Issued Page



12. Select the **Base 64 encoded** option for encoding and click **Download 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**:

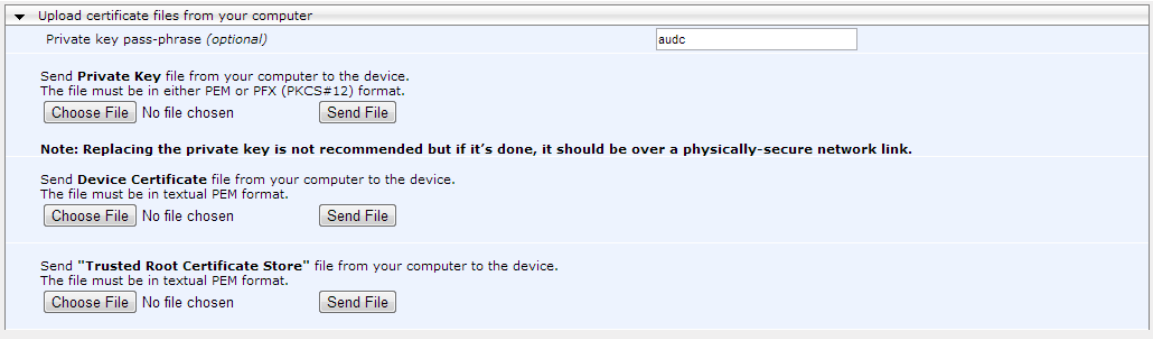
Figure 4-26: Download a CA Certificate, Certificate Chain, or CRL



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 this:
    a. In the 'Device Certificate' field, click **Choose File** and select the *gateway.cer* certificate file that you saved on your computer in Step 13; then click **Send File** to upload the certificate to the E-SBC.
    b. In the 'Trusted Root Certificate Store' field, click **Choose File** and select the *certroot.cer* certificate file that you saved on your computer in Step 18; then click **Send File** to upload the certificate to the E-SBC.

Figure 4-27: Certificates Page (Uploading Certificate)



20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 73).

4.9 Step 9: Configuring SRTP

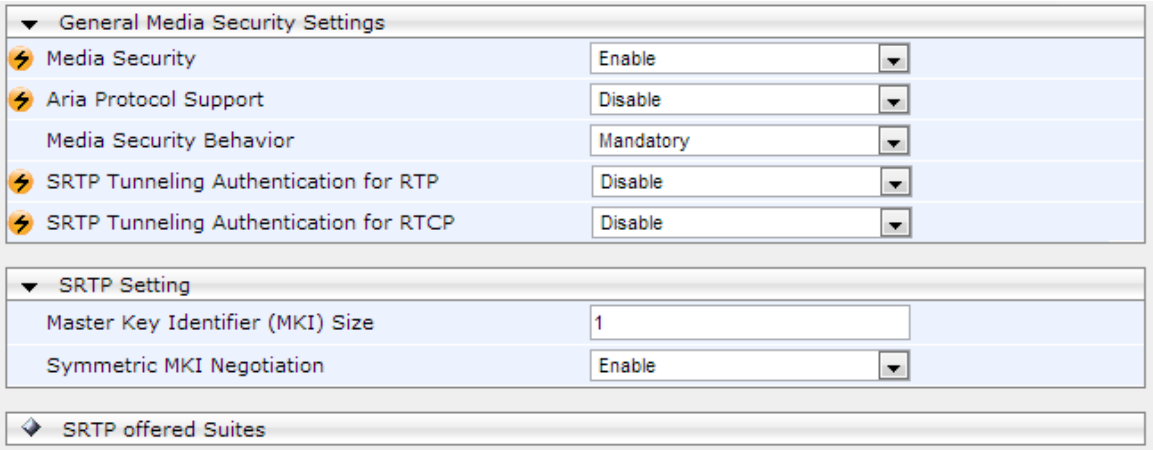
This step shows how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), configure the E-SBC to do so as well.

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 49).

➢ **To configure media security:**

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

Figure 4-28: Media Security Page



2. Configure the parameters like this:

Parameter	Example Setting
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 on page 73).

4.10 Step 10: Configuring IP Media

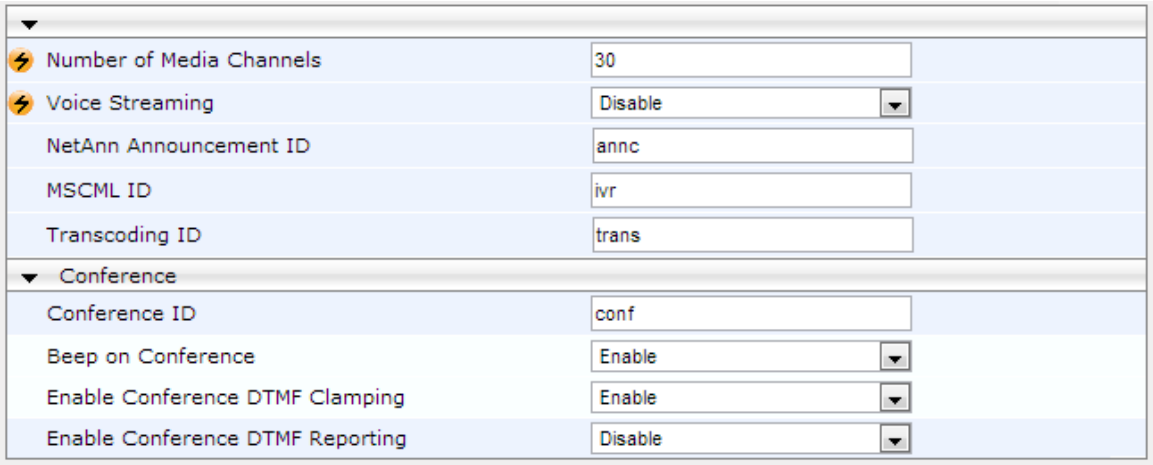
This step shows how to configure the number of media channels for IP-based media. To perform coder transcoding, define digital signaling processors (DSP) channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to sessions.

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

➢ **To configure IP media:**

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

Figure 4-29: IP Media Settings



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environment's transcoding calls (e.g., 30).
3. Click **Submit**.

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

This step shows how to configure IP-to-IP call routing rules (configured 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, the following IP-to-IP routing rules must be added in order to route calls between Lync Server 2013 (LAN) and SIP Trunk (WAN):

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

The routing rules use IP Groups to denote the source and destination of the call.

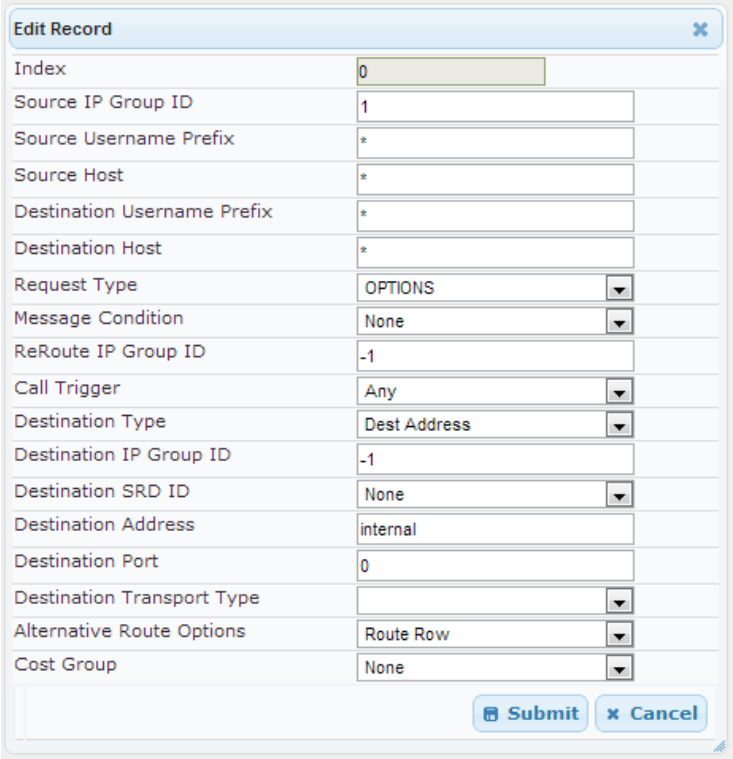
As configured in Step 5 (see Section 4.5 on page 47), IP Group ID 1 was assigned to Lync Server 2013, and IP Group ID 2 to SIP Trunk.

➢ **To add IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Configuration tab > VoIP** > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to terminate SIP OPTIONS messages received from the LAN:
   a. Click **Add**.
   b. Configure the parameters like this:

Parameter	Example Setting
Index	"0"
Source IP Group ID	"1"
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	"internal"

Figure 4-30: Configured IP-to-IP Routing Rule to Terminate SIP OPTIONS Messages Received from the LAN



c. Click **Submit**.

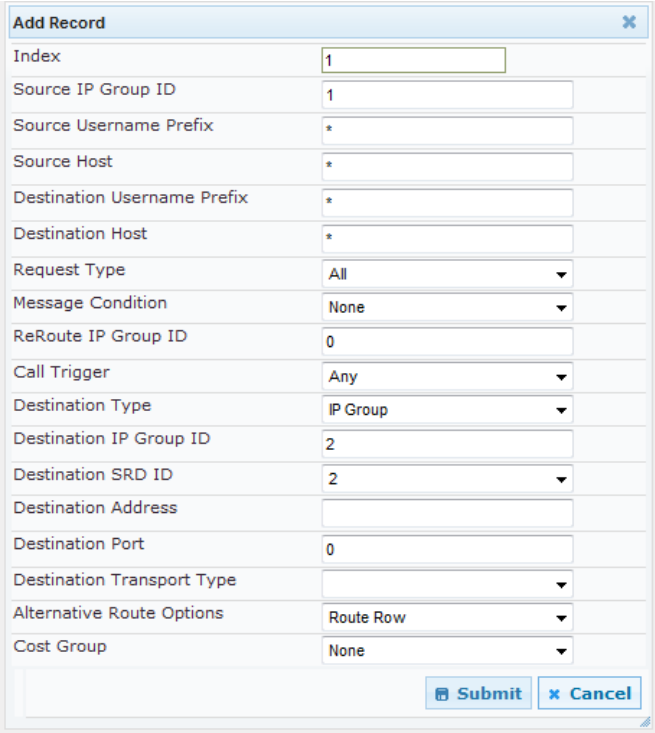
3. Add a rule to route calls from LAN to WAN:

a. Click **Add**.

b. Configure the parameters like this:

Parameter	Example Setting
Index	"1"
Source IP Group ID	"1"
Destination Type	**IP Group**
Destination IP Group ID	"2"
Destination SRD ID	"2"

Figure 4-31: IP-to-IP Routing Rule for LAN to WAN



c. Click **Submit**.

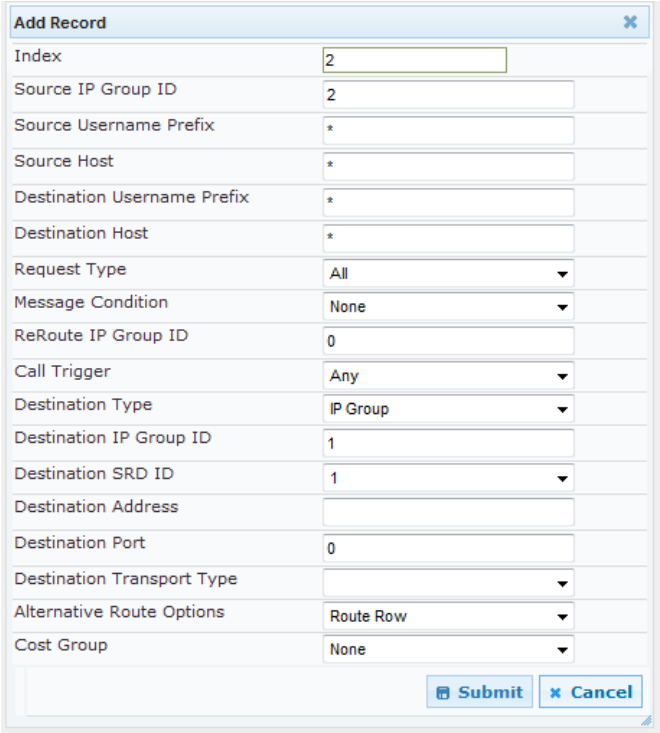
4. Add a rule to route calls from WAN to LAN:

a. Click **Add**.

b. Configure the parameters like this:

Parameter	Example Setting
Index	"2"
Source IP Group ID	"2"
Destination Type	**IP Group**
Destination IP Group ID	"1"
Destination SRD ID	"1"

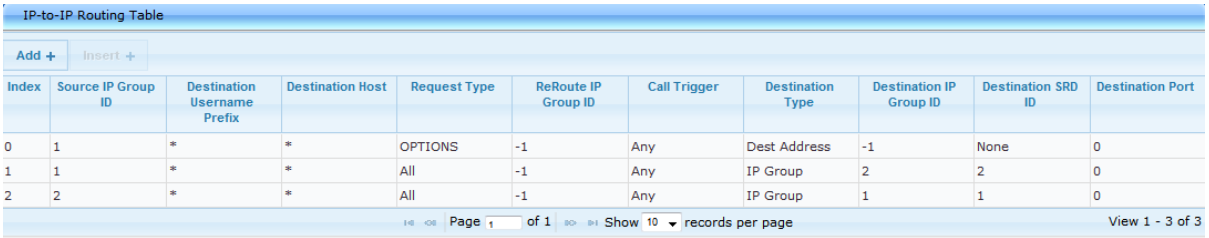
Figure 4-32: Configured IP-to-IP Routing Rule to Route Calls from WAN to LAN



c. Click **Submit**.

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

Figure 4-33: IP-to-IP Routing Table



IP-to-IP Routing Table

Add + Insert +

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	1	*	*	OPTIONS	-1	Any	Dest Address	-1	None	0
1	1	*	*	All	-1	Any	IP Group	2	2	0
2	2	*	*	All	-1	Any	IP Group	1	1	0

Page 1 of 1 Show 10 records per page View 1 - 3 of 3

Note: The routing configuration may change according to the local deployment topology.

4.12 Step 12: Configuring IP-to-IP Outbound Manipulation

This step shows how to configure IP-to-IP manipulation rules. They concern number manipulation of the source and / or destination number. They use IP Groups to denote the source and destination of the call. As configured in Step 5 (see Section 4.5 on page 47), IP Group ID 1 was assigned to Lync Server 2013 and IP Group ID 2 to the SIP Trunk.

Note: Adapt the manipulation table according to you environment dial plan.

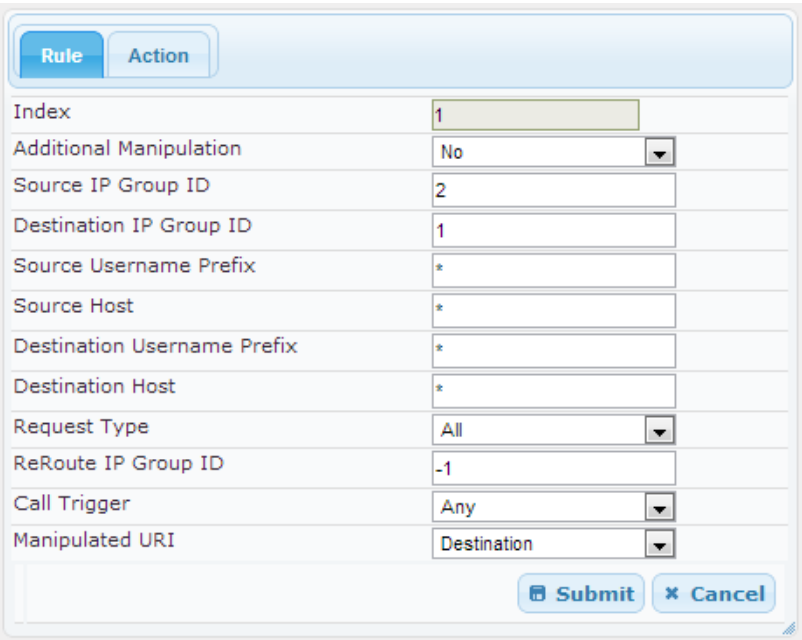
The step below exemplifies configuring a manipulation rule which adds a plus sign + to the destination number for calls from IP Group 2 (SIP Trunk) destined to IP Group 1 (i.e., Lync Server 2013), when the destination number prefix is any number (*).

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

1. Open the IP to IP Outbound Manipulation page (**Configuration** tab > **VoIP** > **SBC** > **Manipulations SBC** > **IP-to-IP Outbound**).
2. Click **Add**.
3. Click the **Rule** tab and configure the parameters like this:

Parameter	Example Setting
Index	"1"
Source IP Group	"2"
Destination IP Group	"1"
Destination Username Prefix	"*"
Manipulated URI	**Destination**

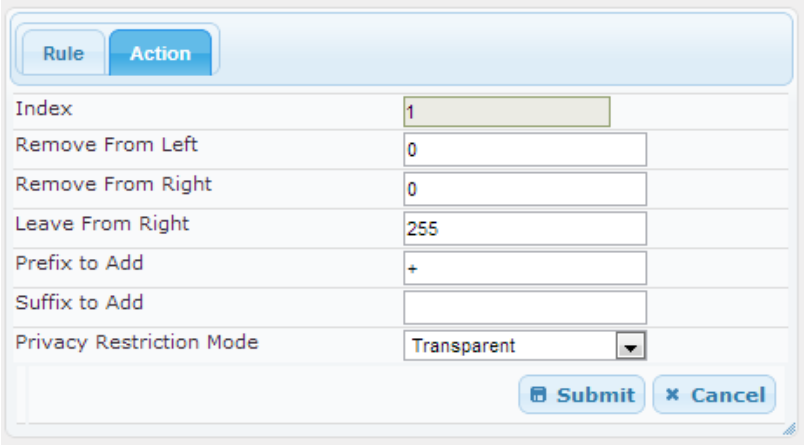
Figure 4-34: IP-to-IP Outbound Manipulation Rule – Rule Tab



4. Click the **Action** tab and configure the parameters like this:

Parameter	Example Setting
Prefix to Add	"+"

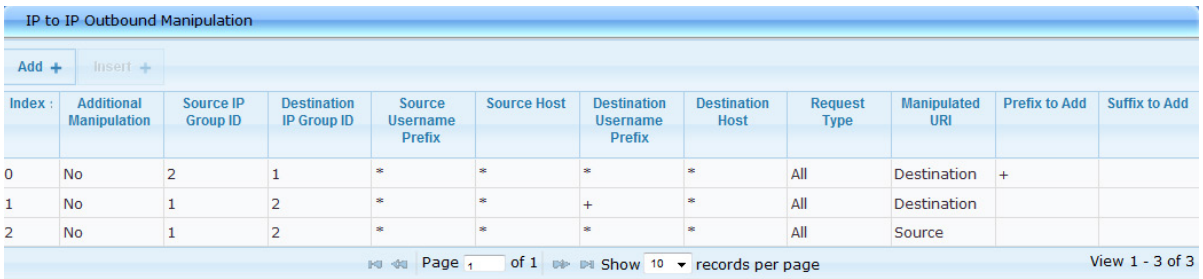
Figure 4-35: Configured IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

The IP-to-IP Outbound Manipulation table displayed below includes four manipulation rules for calls between IP Group 1 (i.e., Lync Server 2013) and IP Group 2 (i.e., SIP Trunk):

Figure 4-36: IP-to-IP Outbound Manipulation



Index :	Additional Manipulation	Source IP Group ID	Destination IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulated URI	Prefix to Add	Suffix to Add
0	No	2	1	*	*	*	*	All	Destination	+	
1	No	1	2	*	*	+	*	All	Destination		
2	No	1	2	*	*	*	*	All	Source		

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

4.13 Step 13: Configuring SIP Message Manipulation Rules

This step shows how to configure SIP message manipulation rules (configured 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, assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

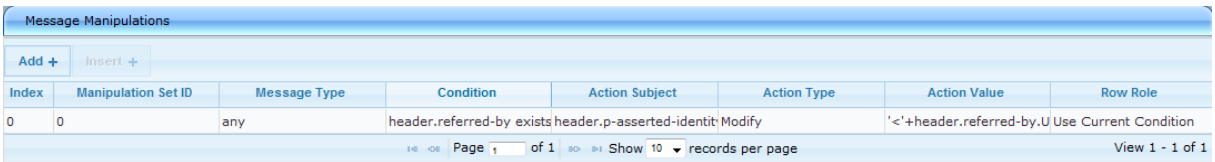
See an example below of a message manipulation rule configuration; use the *E-SBC User's Manual* for detailed instructions on how to configure message manipulation rules according to your requirements.

In the example scenario, the configured manipulation rule manipulates the P-Asserted-Identity user part of the header, and replaces it with the user part that appears on the Referred-By header.

➢ **To configure SIP message manipulation rules:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).

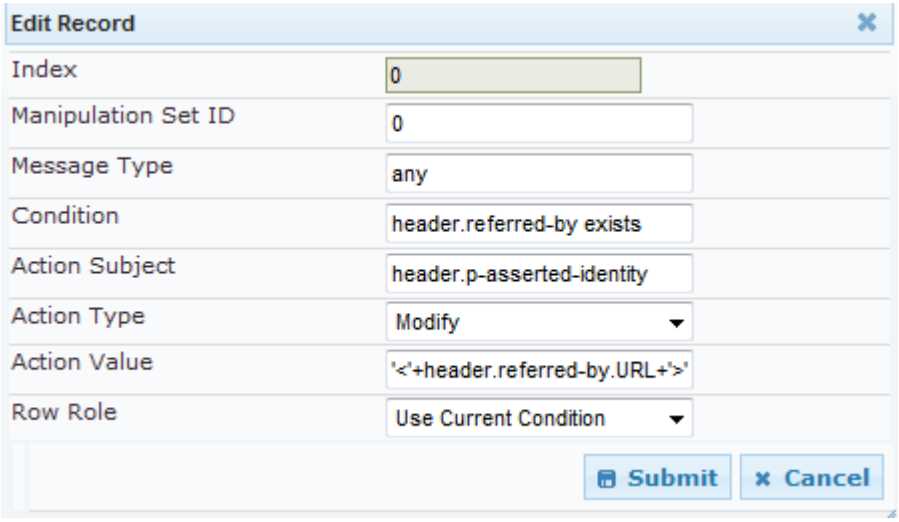
Figure 4-37: Message Manipulations Page



2. Add the following manipulation rules for Manipulation Set ID 0:

Parameter	Example Setting
Index	"0"
Manipulation Set ID	"0"
Message Type	any **Note:** Enter the value as is.
Condition	header.referred-by exists **Note:** Enter the value as is.
Action Subject	header.p-asserted-identity **Note:** Enter the value as is.
Action Type	**Modify**
Action Value	'<'+header.referred-by.URL+'>' Note: Enter the value as is.

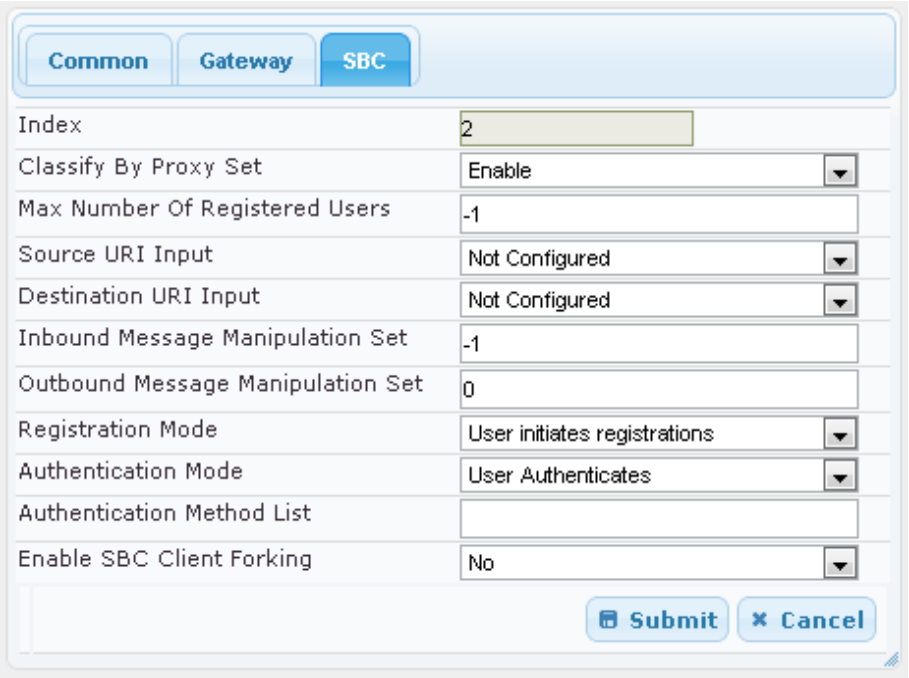
Figure 4-38: Configured SIP Message Manipulation Rule



- Click **Submit**.

3. Assign the Manipulation Set ID 0 to IP Group 2:
   a. Open the IP Group Table page (**Configuration** tab > **VoIP** > **Control Network** > **IP Group Table**).
   b. Select the row of IP Group 2 and click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Outbound Message Manipulation Set' field to 0.

Figure 4-39: Assigning a Manipulation Rule to IP Group 2



   e. Click **Submit**.

4.14 Step 14: Configuring a Registration Account

This step shows how to configure SIP registration accounts (in the Account Table page) so that the E-SBC can register with the SIP Trunk on behalf of Lync Server 2013.

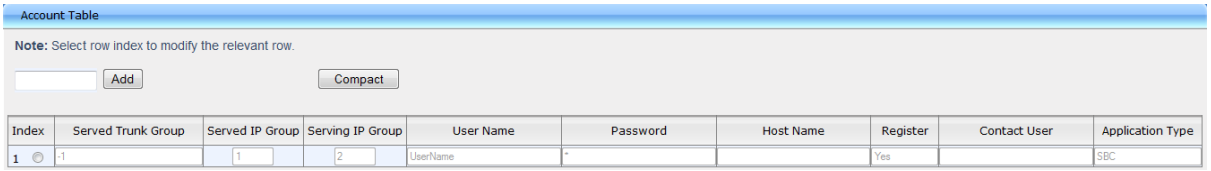
Note: Not *all* SIP Trunks require registration (and authentication) to provide service. If your SIP Trunk doesn't require registration, skip this step.

In this example, the Served IP Group is Lync Server 2013 (IP Group 1) and the Serving IP Group is SIP Trunk (IP Group 2).

➢ **To configure a registration account:**

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

Figure 4-40: Configuring a SIP Registration Account



2. Enter an index number (1) and click **Add**.
3. Configure the account according to the information provided by the SIP Trunk provider, for example:

Parameter	Example Setting
Served IP Group	"1" (i.e., Lync Server 2013)
Serving IP Group	"2" (i.e., SIP Trunk)
Username	(Provided by the SIP Trunk provider)
Password	(Provided by the SIP Trunk provider)
Register	**Yes**
Application Type	**SBC**

4. Click **Apply**.

4.15 Step 15: Configuring Miscellaneous E-SBC Functionalities

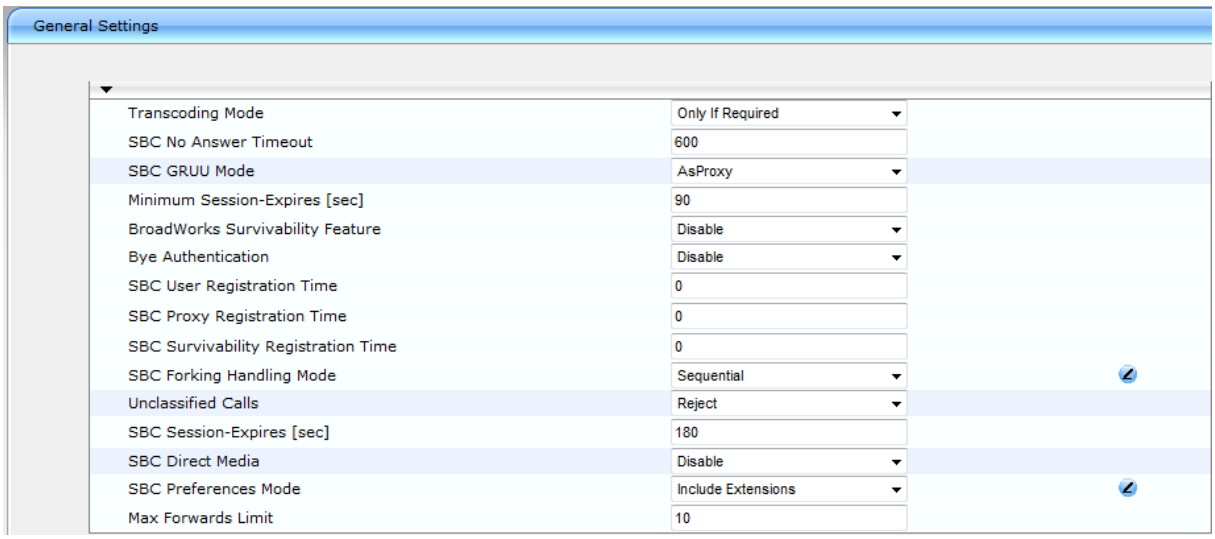
This step shows how to configure the E-SBC's handling of SIP 18x responses received due to call forking of an INVITE.

In the example scenario, if an 18x 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 a 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 4-41: Configuring Forking Mode



3. From the 'SBC Preferences Mode' drop-down list, select **Include Extensions** to ensure that Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Coders Group table.
4. Click **Submit**.

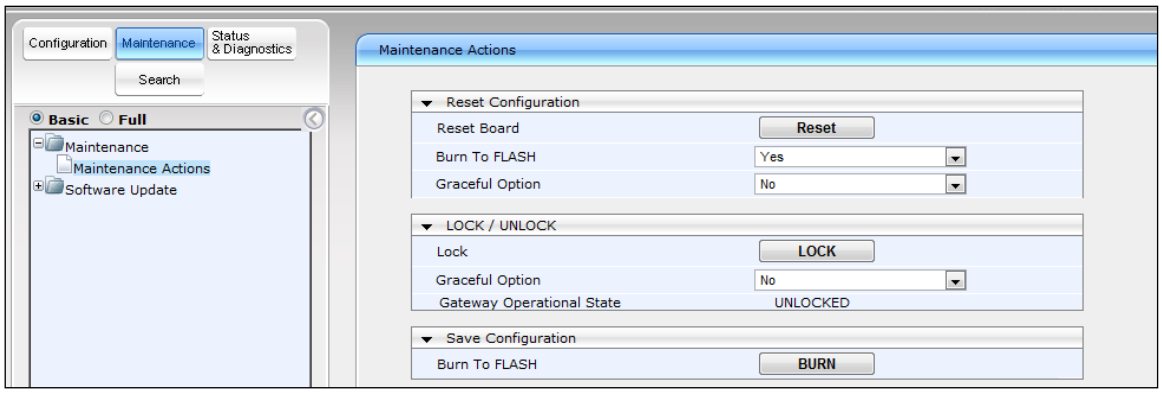
4.16 Step 16: Resetting the E-SBC

After completing the configuration of the E-SBC as described in the preceding steps, save (burn) the configuration to the E-SBC's flash memory with a reset; the settings will now take effect.

➢ **To save the configuration to flash memory with a reset:**

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

Figure 4-42: Resetting the E-SBC



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

Reader's Notes

A Configuring E-SBC to Send 414 Request-URI Too Long Response

This step shows how to configure the E-SBC to send a 414 Request-URI Too Long response when it encounters a Request URI it cannot handle due to excessive length.

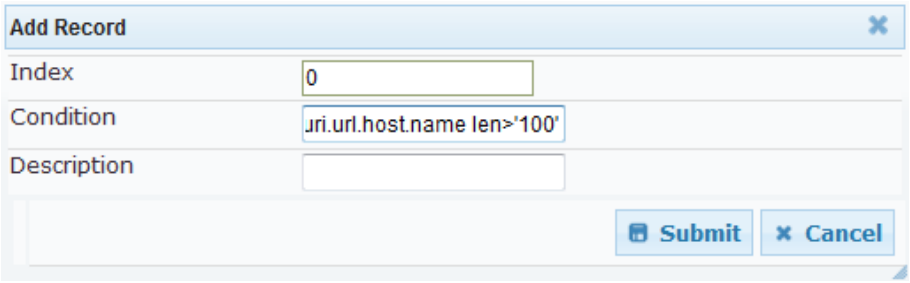
When the E-SBC receives an INVITE with a long Request URI (a condition rule), it will route it to an unknown destination IP address (i.e., 1.1.1.1) and it will set a variable for this call to **1**. After a timeout, the E-SBC will generate an internal 408 Request Timeout response. Using message manipulation, the E-SBC will convert this response to a 414 Request-URI Too Long response (only if the variable value is **1**).

➢ **To configure a condition for this route:**

1. Open the Condition Table page (**Configuration tab > VoIP** > **SBC** > **Routing SBC** > **Condition Table**).
2. Click the **Add** tab and configure the parameters like this:

Parameter	Example Setting
Index	"0"
Condition	header.request-uri.url.host.name len>'100' Note: You can choose the length of the Request-URI to process.

Figure A-1: Configuring a Condition for the Route



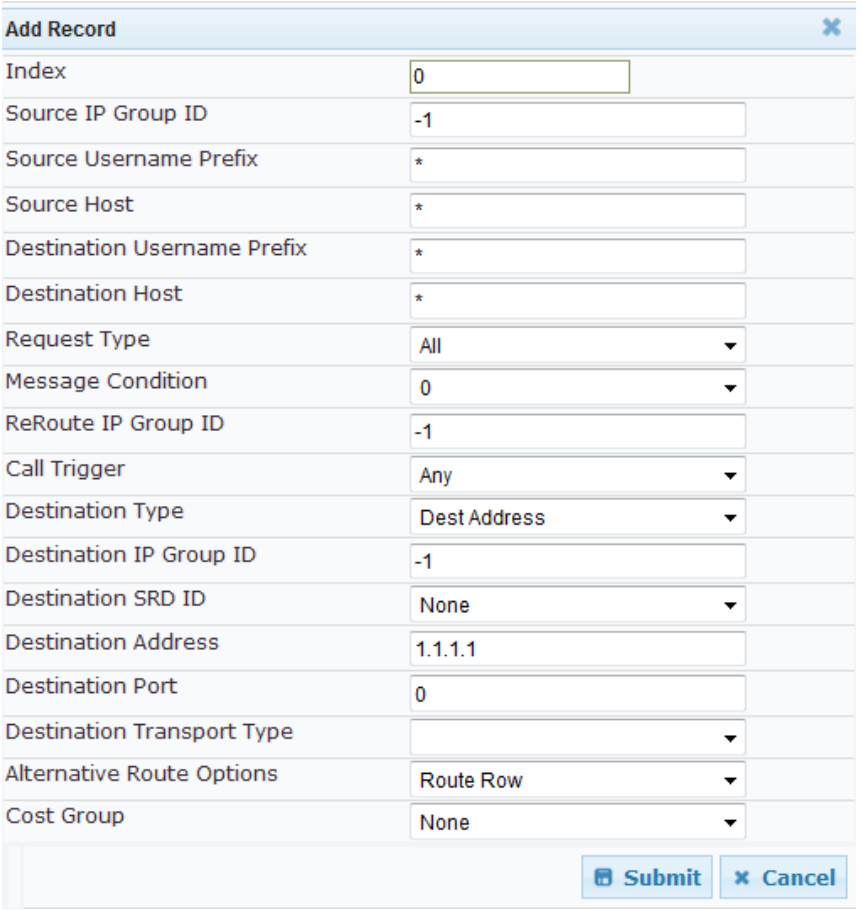
3. Click **Submit**.

➢ **To configure the route:**

1. Open the IP-to-IP Routing Table page (**Configuration tab > VoIP** > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route long-URI calls to unknown IP address:
   a. Click **Add**.
   b. Configure the parameters like this:

Parameter	Example Setting
Index	"0" (this rule should be the first rule in the table)
Message Condition	"0" (this number is the index of the condition configured above)
Destination Type	**Dest address**
Destination Address	"1.1.1.1" (unreachable IP address)

Figure A-2: IP-to-IP Routing Rule for Long-URI Calls

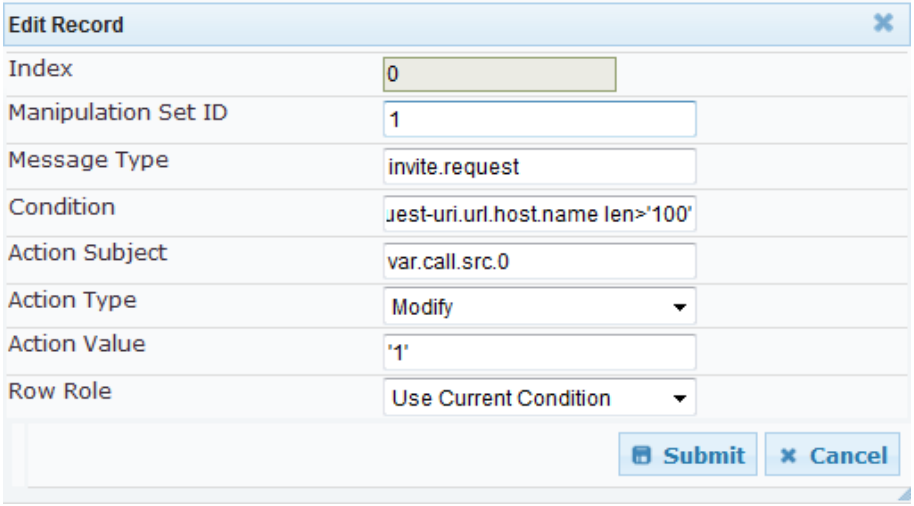


➢ **To configure a message manipulation rule:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add a rule to set a variable to **1** in the case of a long-URI call:
   a. Click **Add**.
   b. Configure the parameters like this:

Parameter	Example Setting
Index	"0"
Manipulation Set ID	"1"
Message Type	invite.request
Condition	header.request-uri.url.host.name len>'100'
Action Subject	var.call.src.0
Action Type	**Modify**
Action Value	'1'

Figure A-3: Manipulation Rule to Set a Variable to '1' in Case of Long-URI Call



c. Click **Submit**.

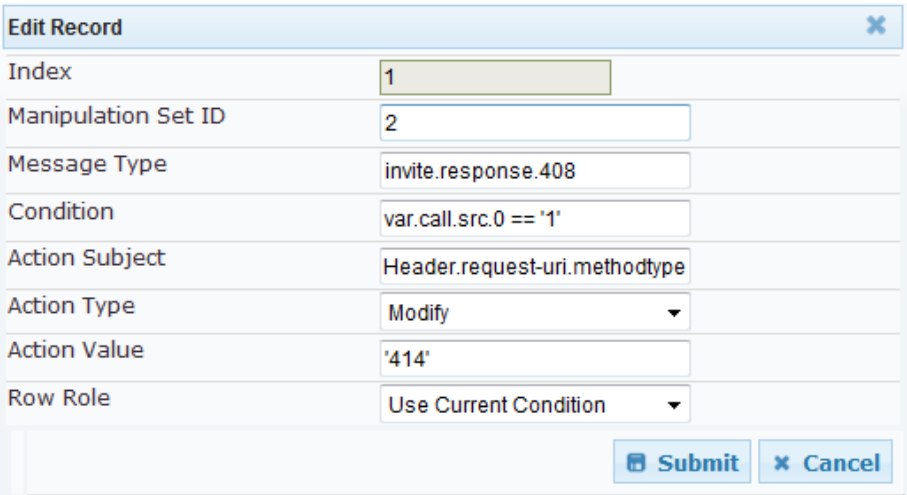
3. Add a rule to convert 408 to '414':

a. Click **Add**.

b. Configure the parameters like this:

Parameter	Example Setting
Index	"1"
Manipulation Set ID	"2"
Message Type	invite.response.408
Condition	var.call.src.0 == '1'
Action Subject	header.request-uri.methodtype
Action Type	**Modify**
Action Value	'414'

Figure A-4: Manipulation Rule to Convert 408 to '414'



c. Click **Submit**.

Figure A-5: Message Manipulations Page

Message Manipulations

Add + Insert +

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	1	invite.request	header.request-ur	var.call.src.0	Modify	'1'	Use Current Cond
1	2	invite.response.40	var.call.src.0 == '1	Header.request-ur	Modify	'414'	Use Current Cond

4. Assign the Manipulation Set to IP Group 1 :
   a. Open the IP Group Table page (**Configuration** tab > **VoIP** > **Control Network** > **IP Group Table**).
   b. Select the row of IP Group 1 and click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Inbound Message Manipulation Set' field to 1.
   e. Set the 'Outbound Message Manipulation Set' field to 2.

Figure A-6: Assigning Manipulation Rule to IP Group 1

Common | Gateway | SBC

Index	1
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	1
Outbound Message Manipulation Set	2
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
Enable SBC Client Forking	No

Submit Cancel

   f. Click **Submit**.

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com