Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2013 and G12 Communications' SIP Trunk using Mediant E-SBC

Microsoft Partner
Gold Communications

Lync

G12 COMMUNICATIONS

AudioCodes

April 2014

Document #: LTRT- 39360

Table of Contents

Reader's Notes

Notice

This document describes how to connect the Microsoft Lync Server 2013 and G12 Communications' SIP Trunk using the 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: May-07-2014

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

Reader's Notes

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between G12 Communications' SIP Trunk and Microsoft's Lync Server 2013 environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and G12 Partners who are responsible for installing and configuring G12 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 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 SBC
Software Version	SIP_6.60A.250.009
Protocol	▪ SIP/UDP (to the G12 SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 G12 SIP Trunking Version

Table 2-2: G12 Version

Vendor/Service Provider	G12 Communications
SSW Model/Service	NetSapiens
Software Version	
Protocol	SIP
Additional Notes	None

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

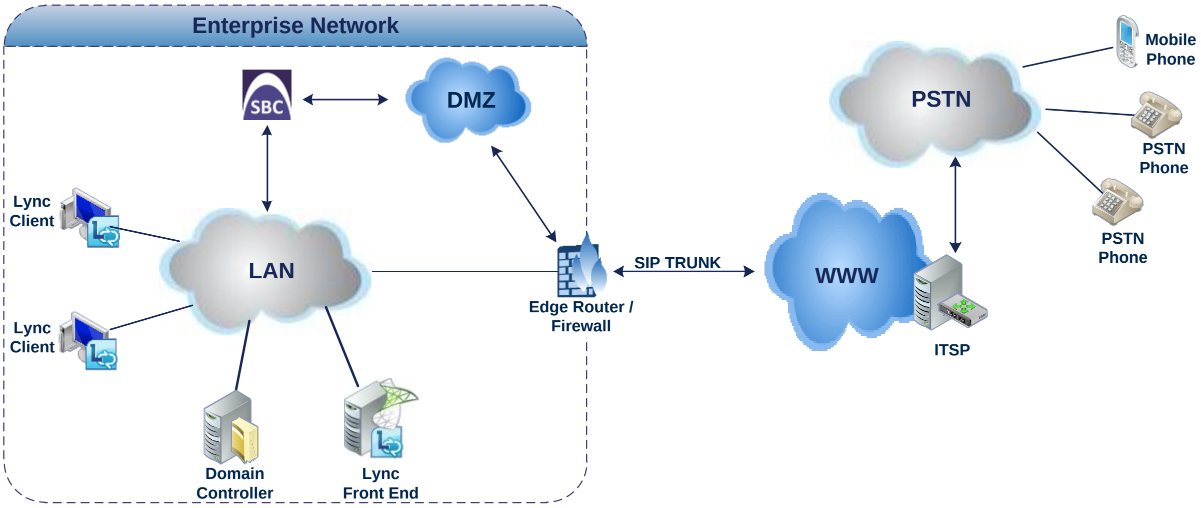
2.4 Interoperability Test Topology

Interoperability testing between AudioCodes' E-SBC and G12's SIP Trunk with Lync 2013 was performed using the following topology:

- The enterprise deployed Microsoft Lync Server 2013 in its private network for enhanced communications within the enterprise.
- The enterprise wanted to offer its employees enterprise-voice capabilities and to connect the enterprise to the PSTN network using G12's SIP Trunking service.
- AudioCodes' E-SBC was implemented to interconnect between the enterprise LAN and the SIP Trunk.
    - **Session:** Real-time voice session using IP-based SIP (Session Initiation Protocol).
    - **Border:** IP-to-IP network border between Lync Server 2013 network in the enterprise LAN and G12's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology



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 ▪ G12 SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ G12 SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ G12 SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ G12 SIP Trunk operates with RTP media type

2.4.2 Known Limitations

The following limitation was observed in the Interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and G12's SIP Trunk:

1. If any of following Error Responses are sent from the Lync server:
   - Lync Client response with “503 Service Unavailable”
   - Lync Client response with “480 Busy Here”

   G12 SIP Trunk still sends re-INVITEs and not disconnects the call. In order to deal with this and disconnect the call, message manipulation rule used to replace above Error Responses by “488 Not Acceptable Here” (see Section 4.13 on page 61).
2. In all outgoing calls (Lync to PSTN), G12 SIP Trunk wait RTP packets in order to ring ‘Ring Back Tone’. Lync not send these packets because it not recognizes comfort noise as RTP stream. In order to deal with this issue, force transcoding enabled in the E-SBC G12 IP Profile (see Section 4.6 on page 43).

Reader's Notes

3 Configuring 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.

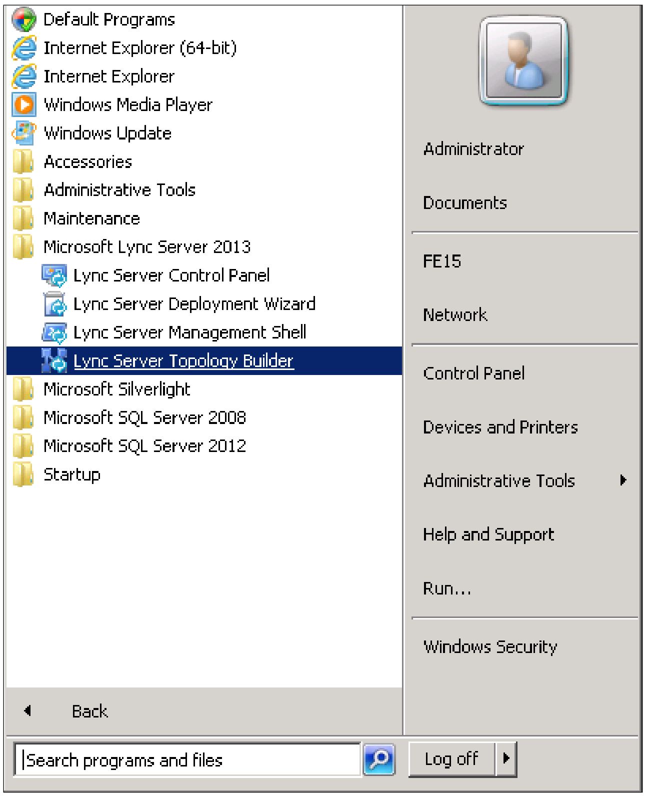
3.1 Configuring the E-SBC as an IP / PSTN Gateway

The procedure below describes 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:**

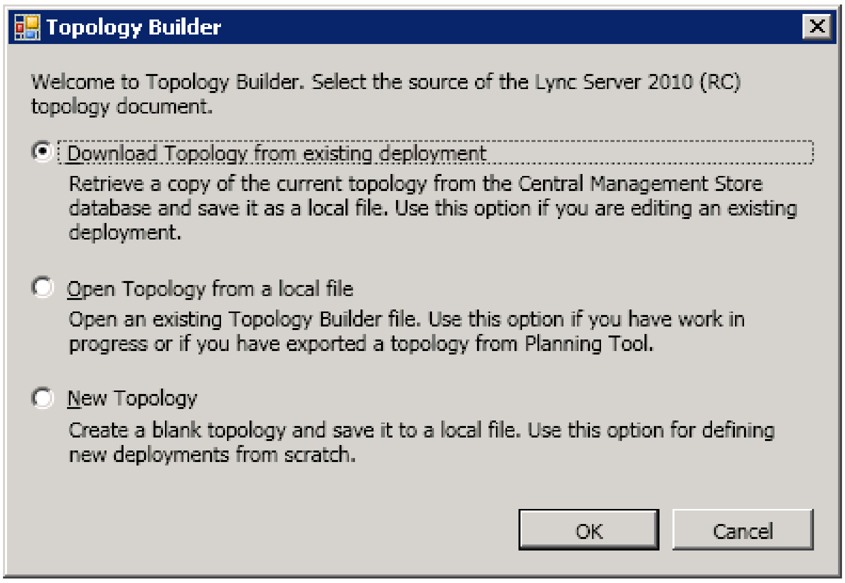
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**):

Figure 3-1: Starting the Lync Server Topology Builder



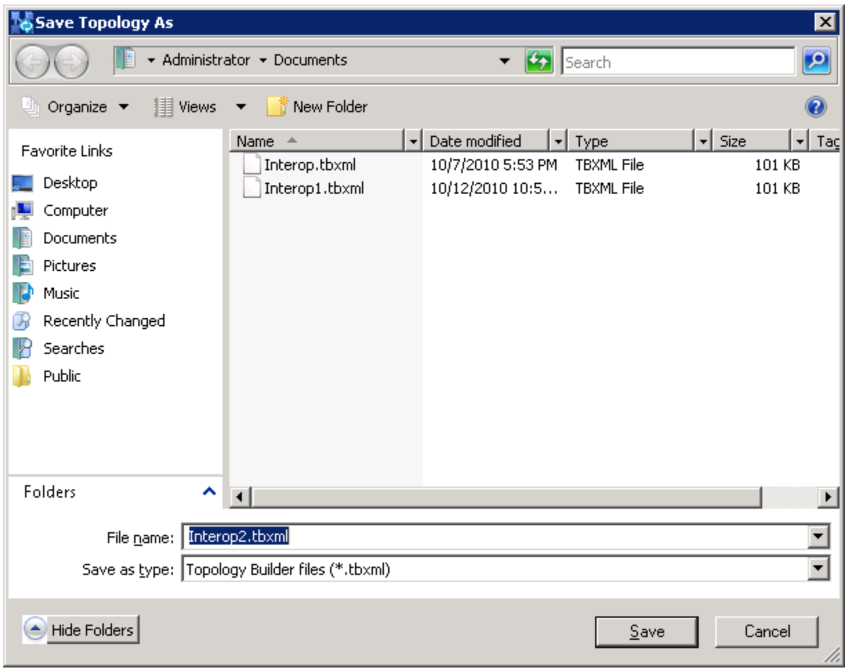
The following is displayed:

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:

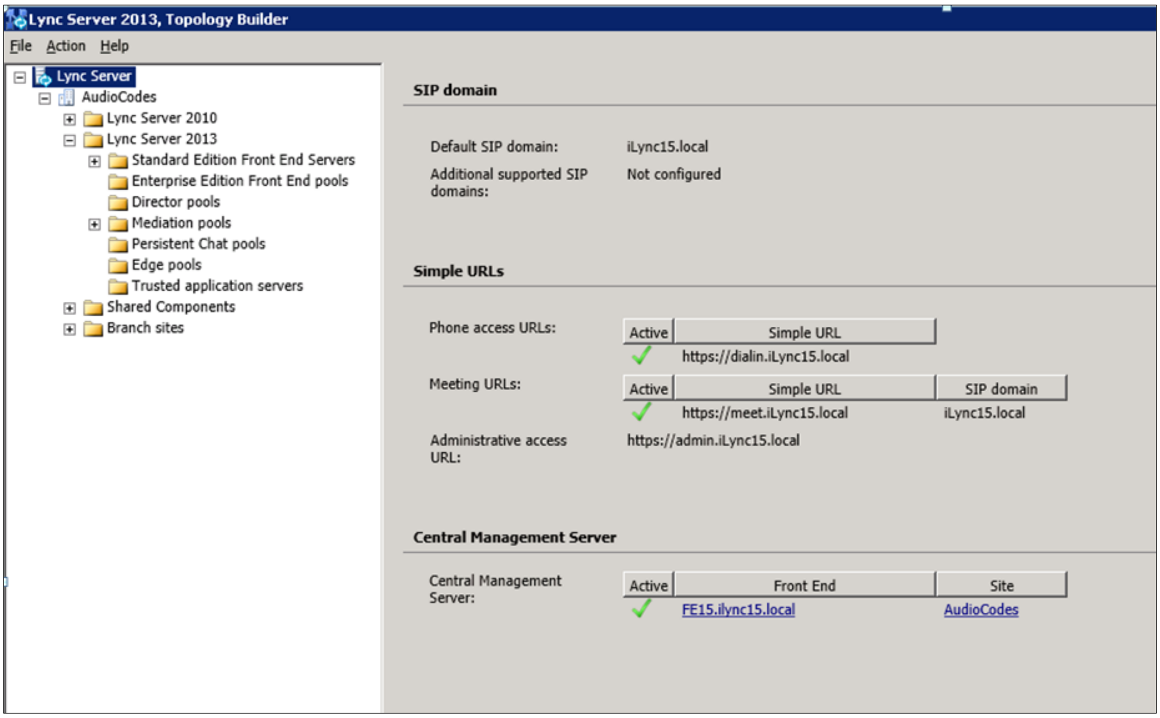
Figure 3-3: Save Topology Dialog Box



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.

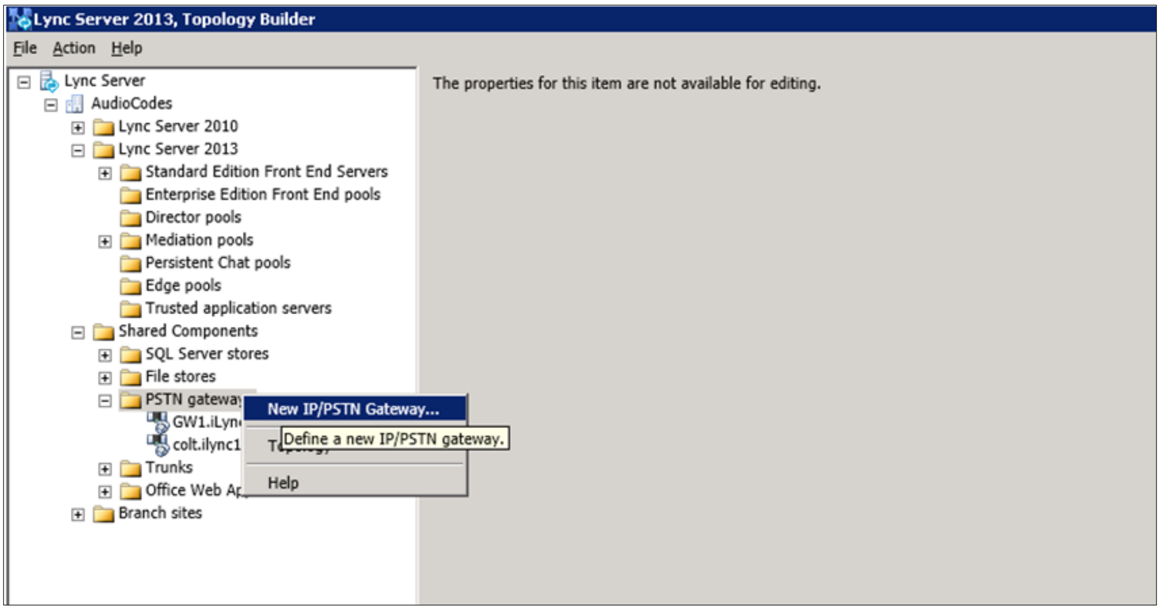
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



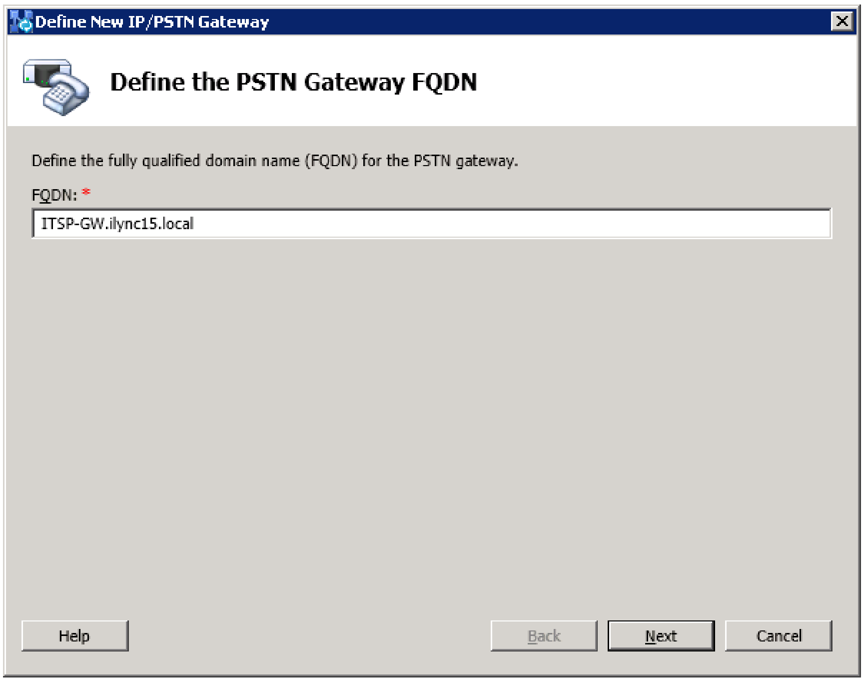
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



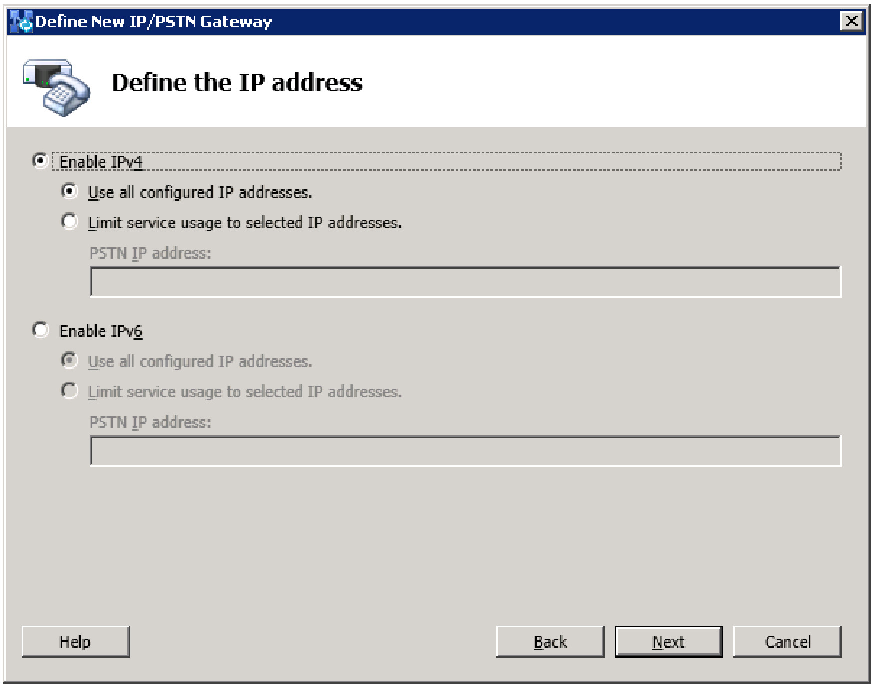
The following is displayed:

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



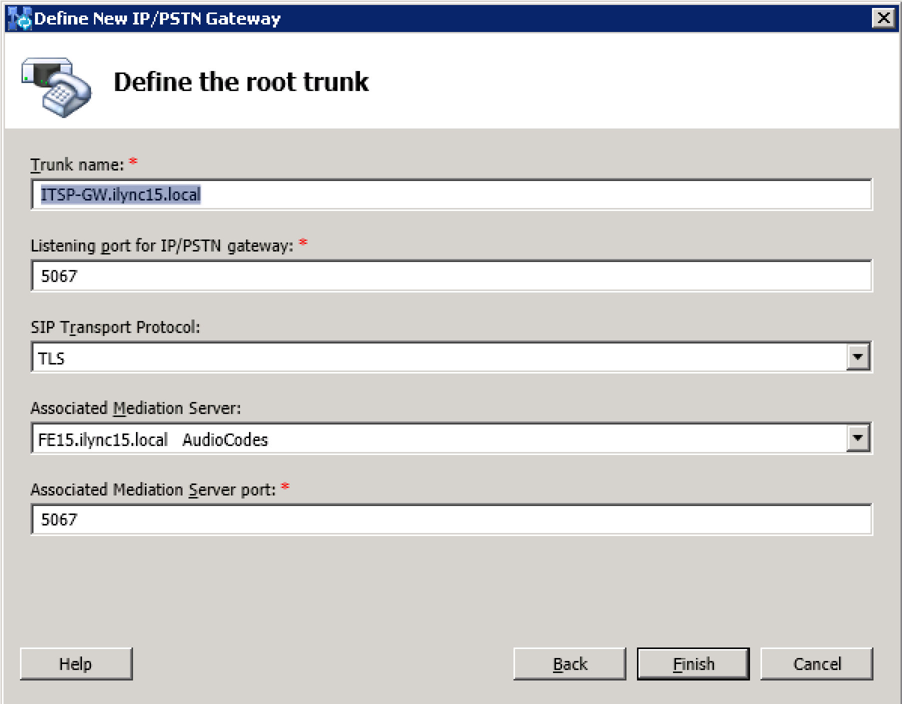
6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

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.

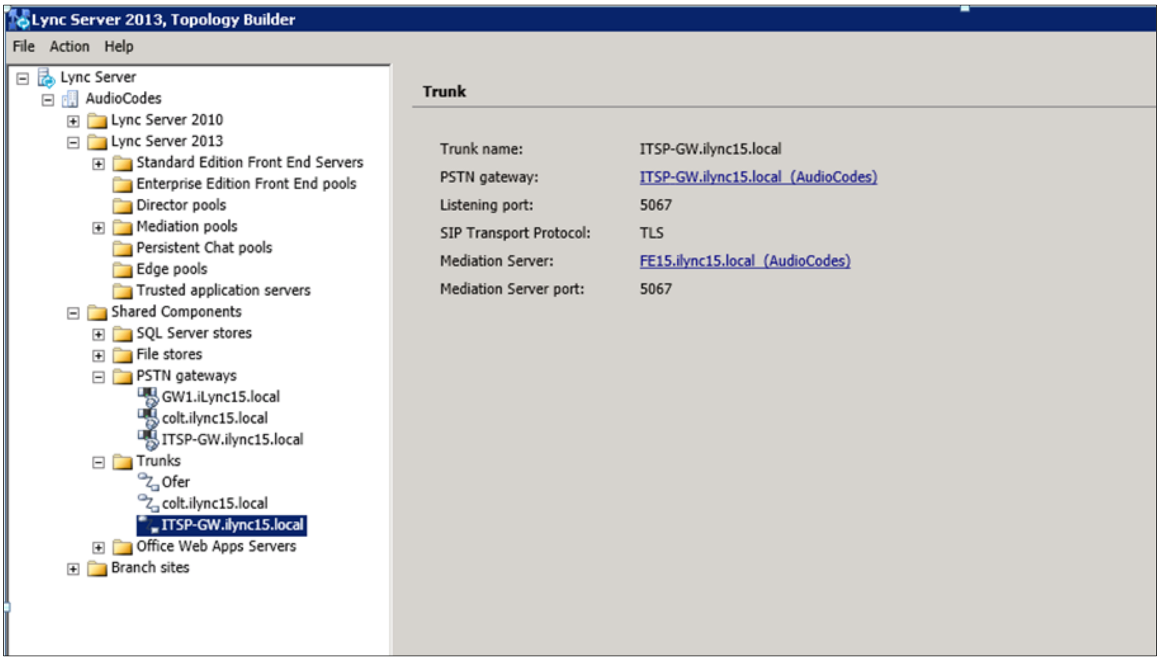
Figure 3-8: Define the Root Trunk



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**.

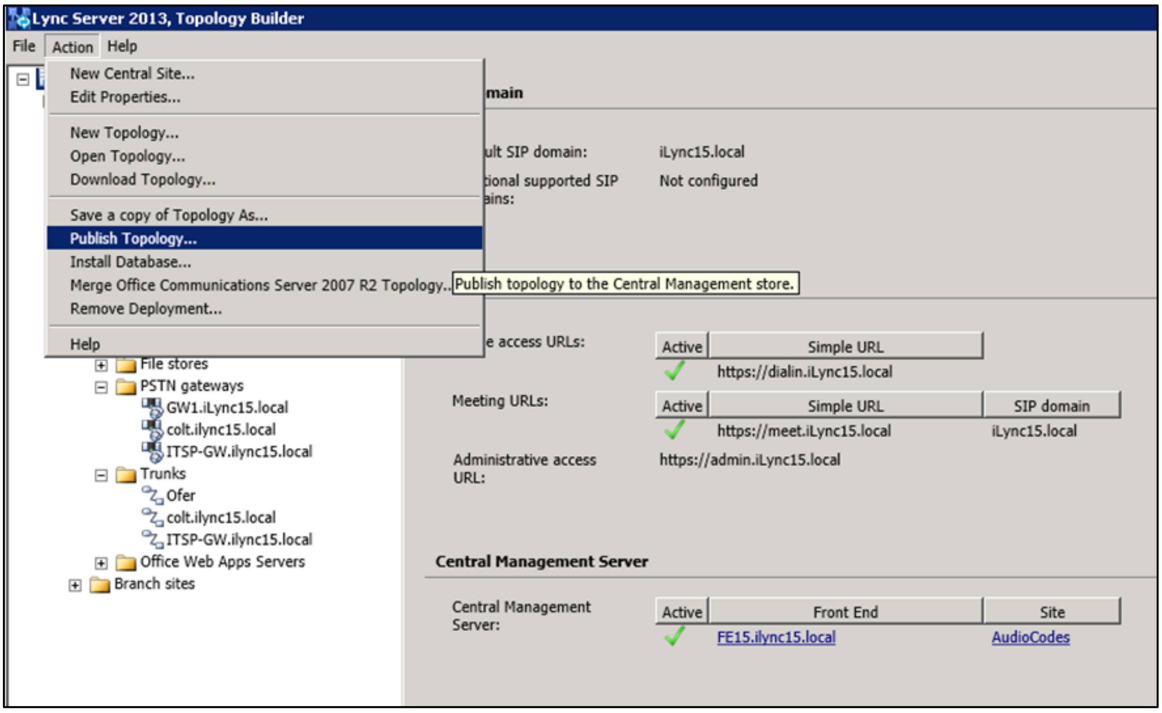
The E-SBC is added as a PSTN gateway and a trunk is created, as shown below:

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



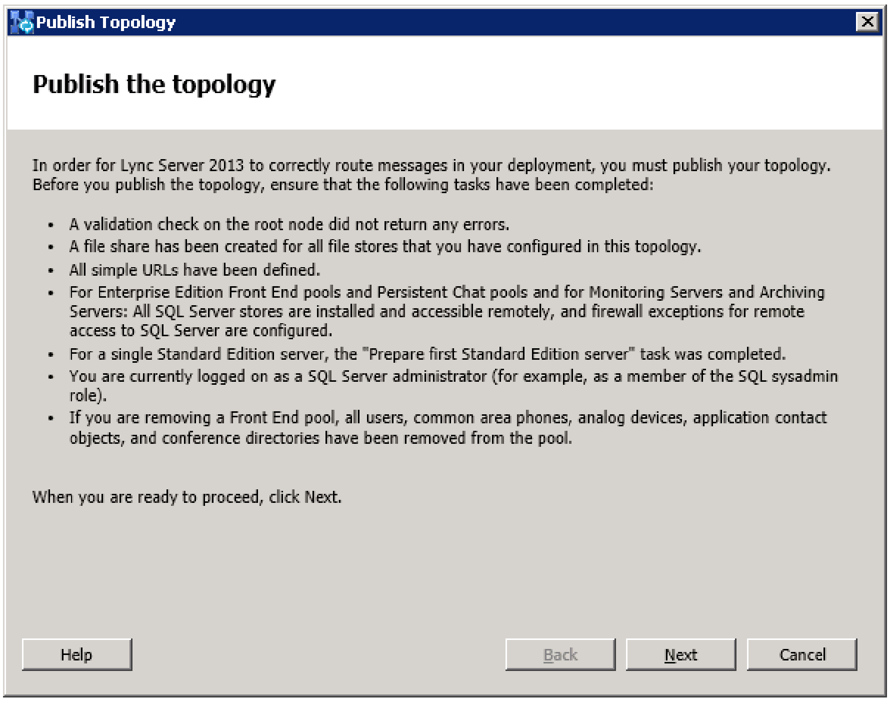
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



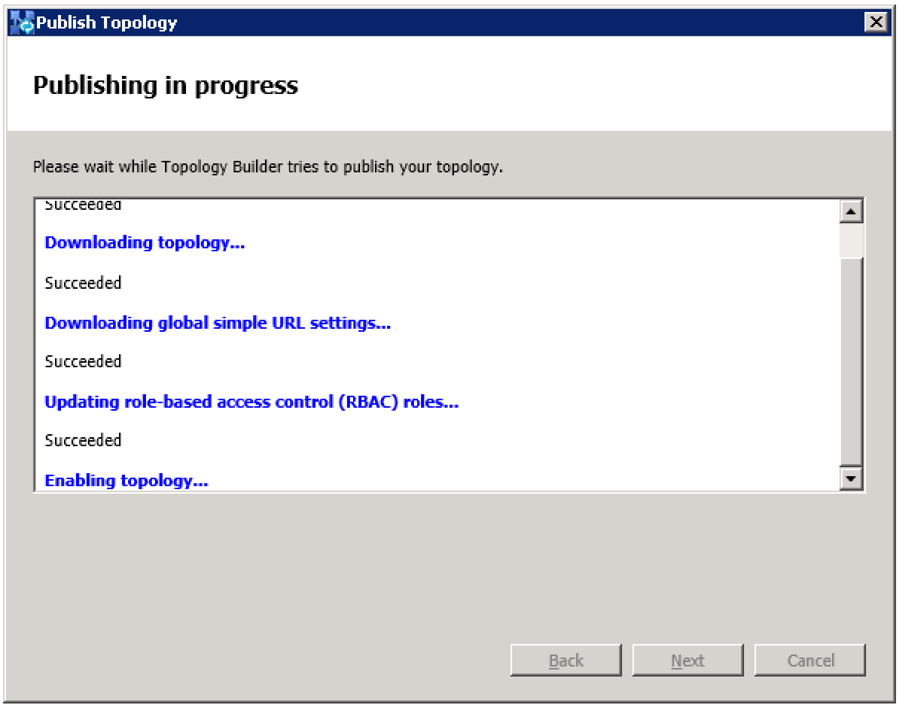
The following is displayed:

Figure 3-11: Publish the Topology



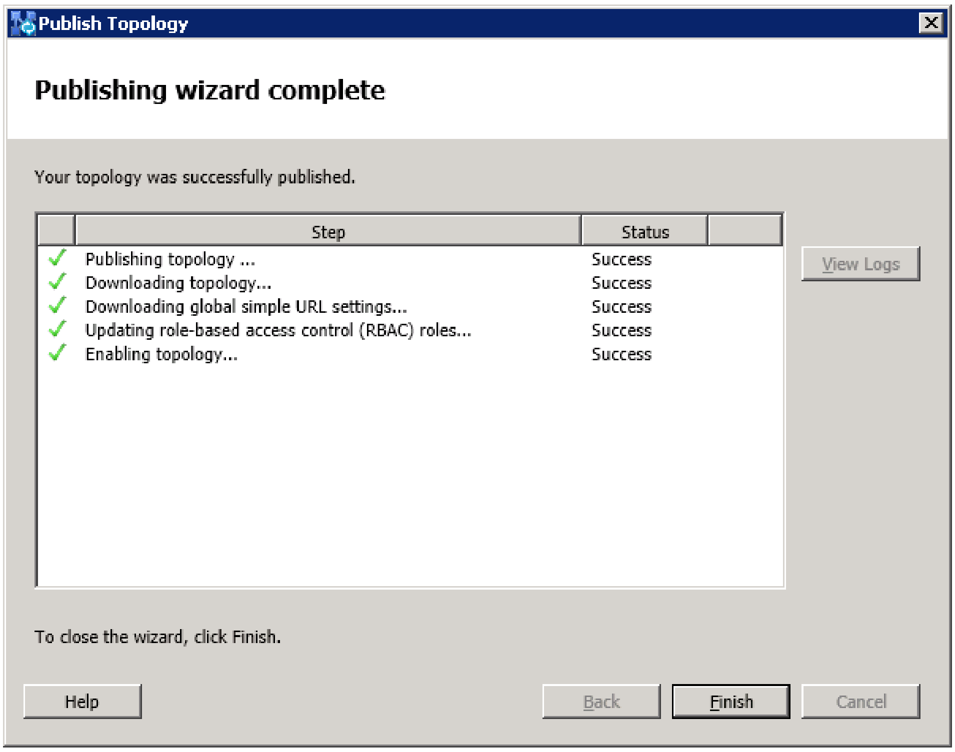
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

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.

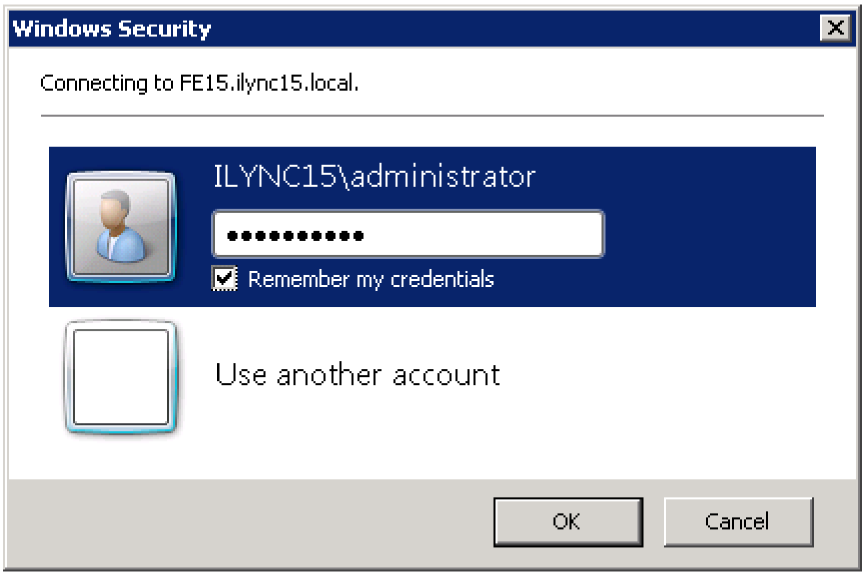
➢ **To configure the "route" on Lync Server 2013:**

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

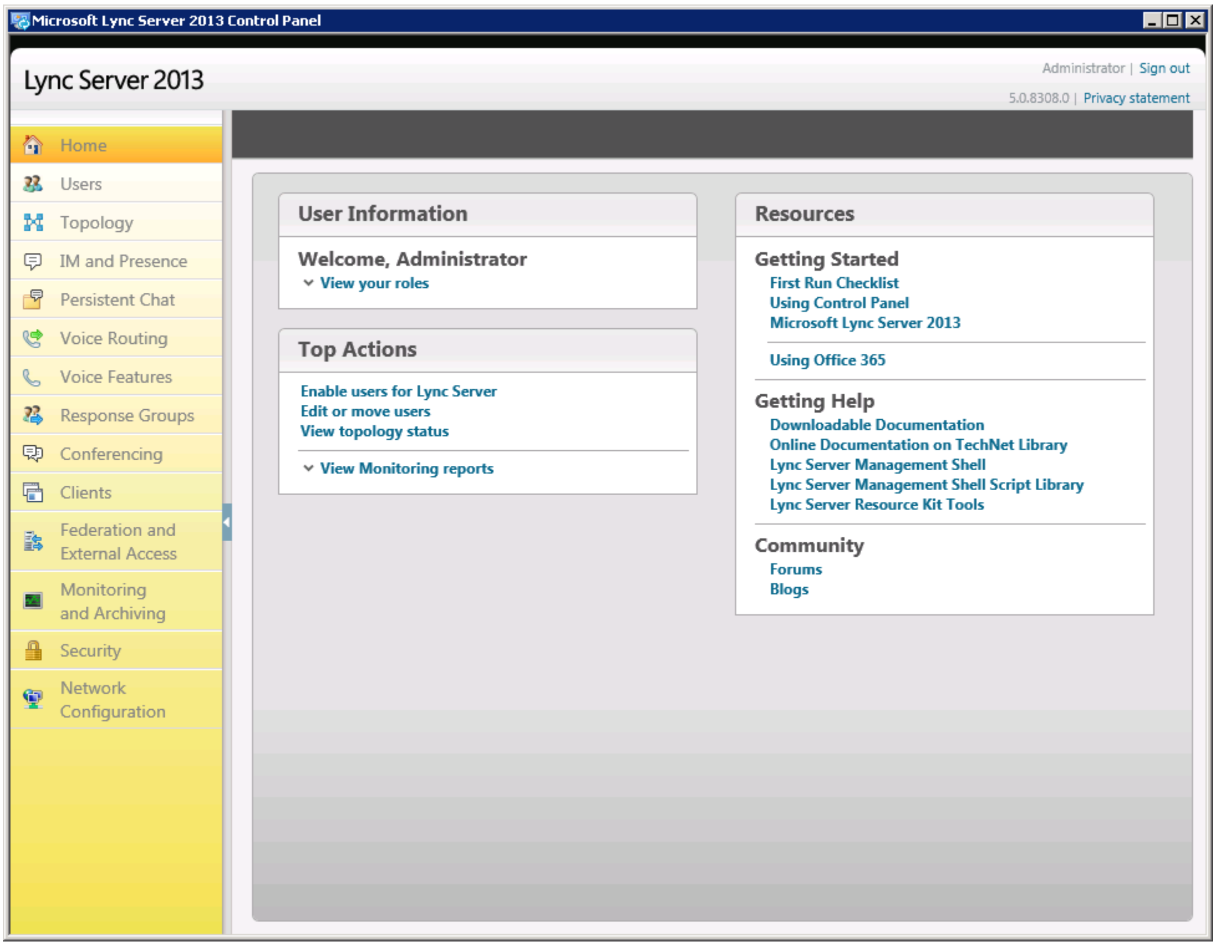
You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



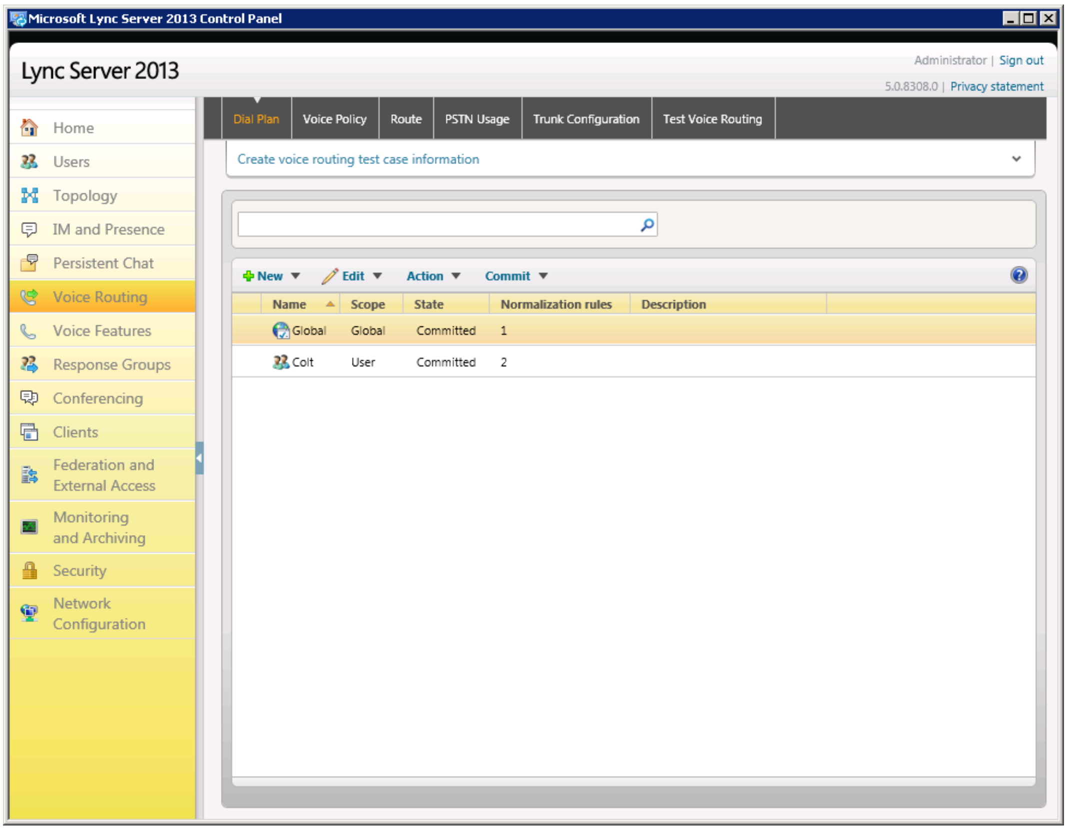
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



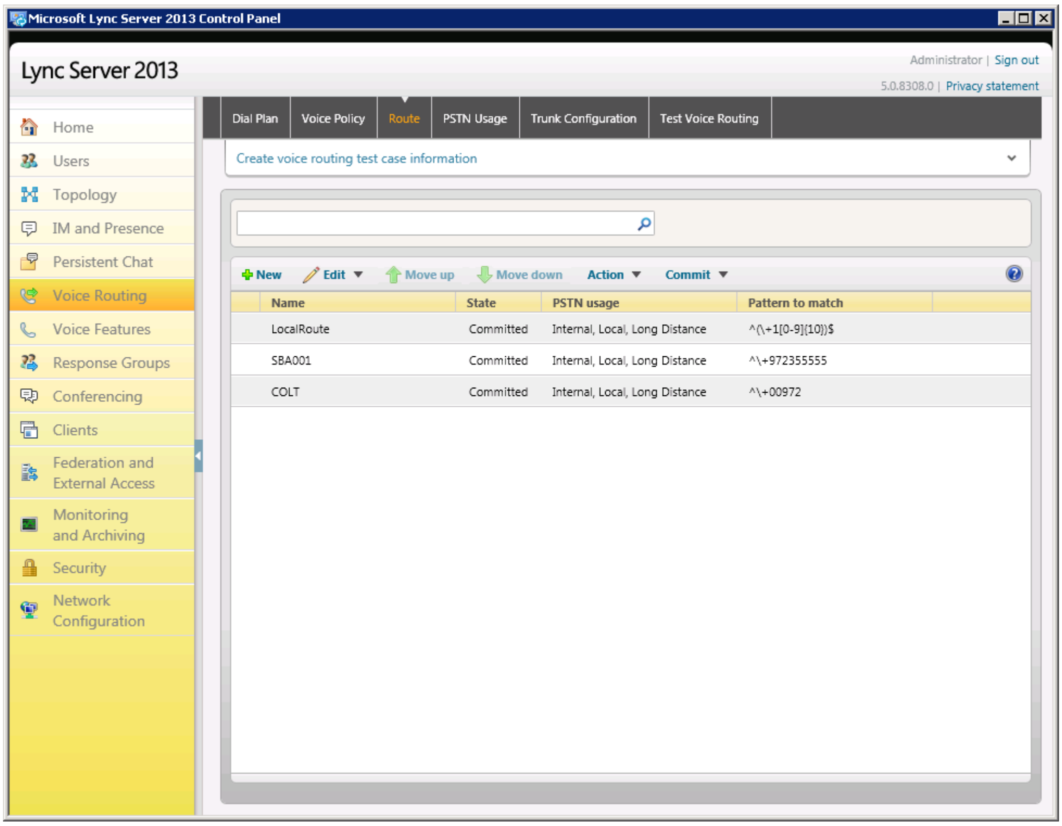
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



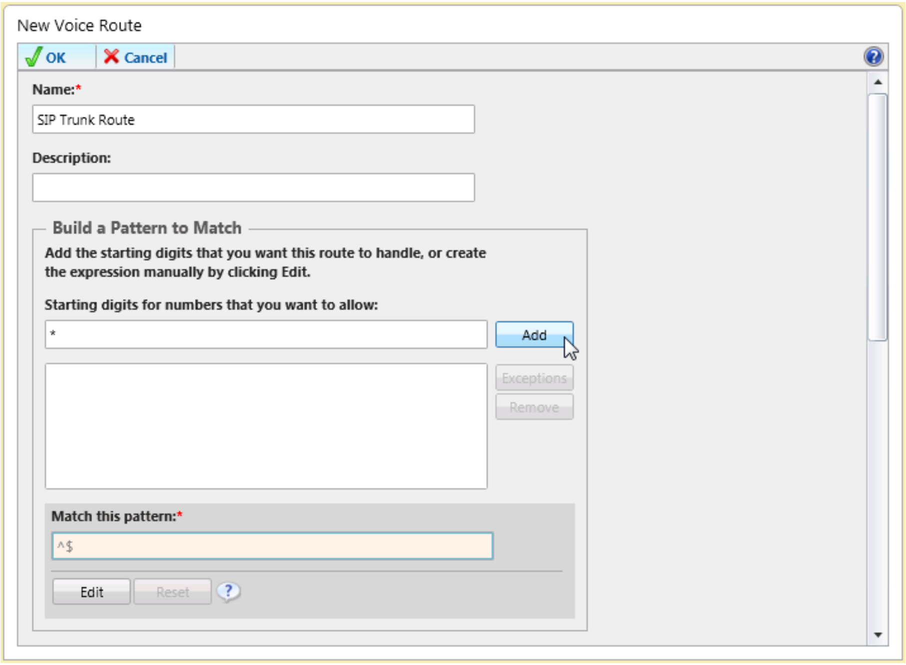
4. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



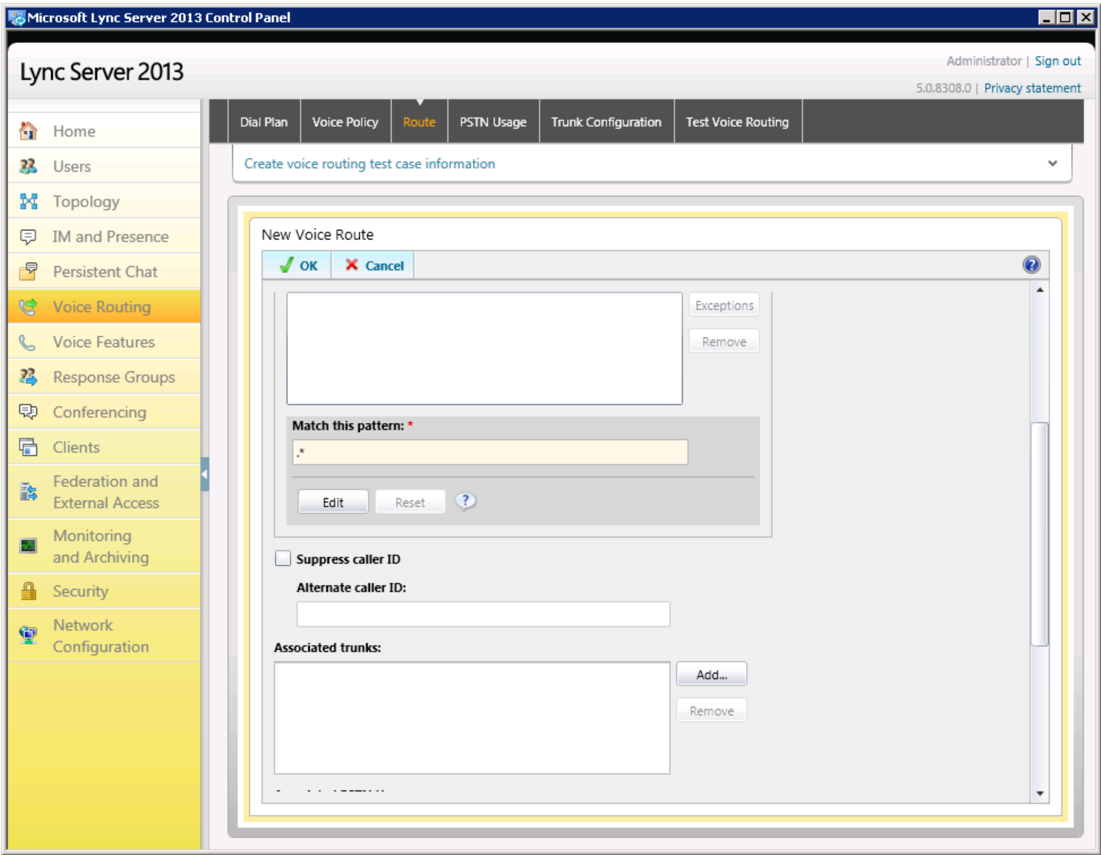
5. Click **New**; the New Voice Route page appears:

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**.

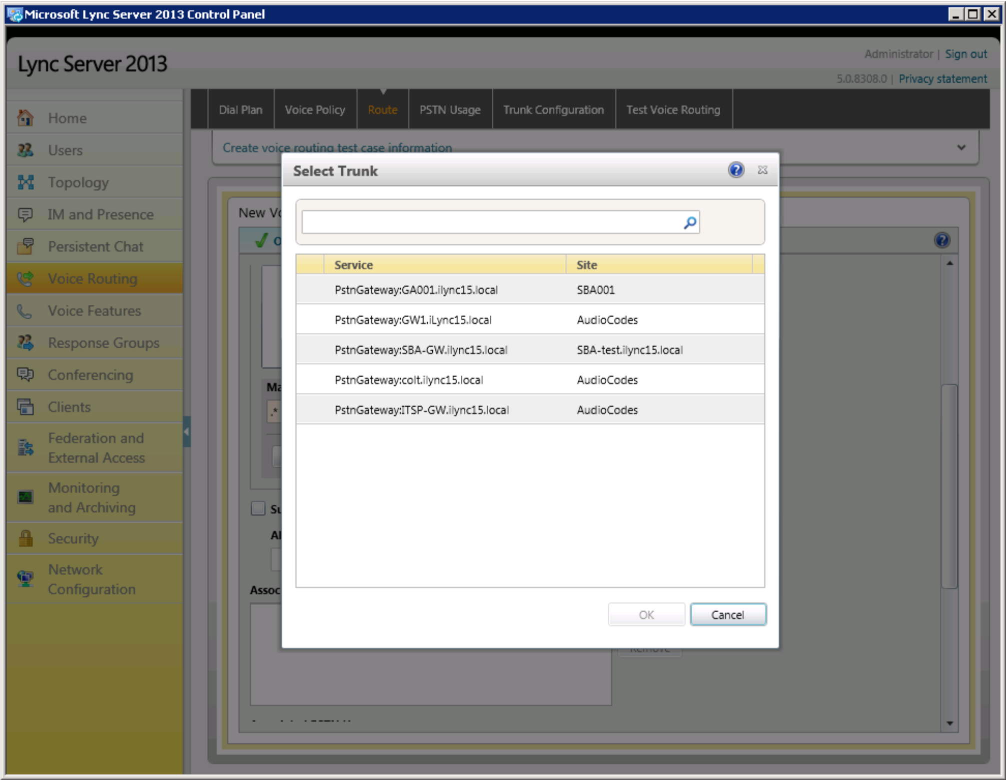
Figure 3-20: Adding New Trunk



8. Associate the route with the E-SBC Trunk that you created:

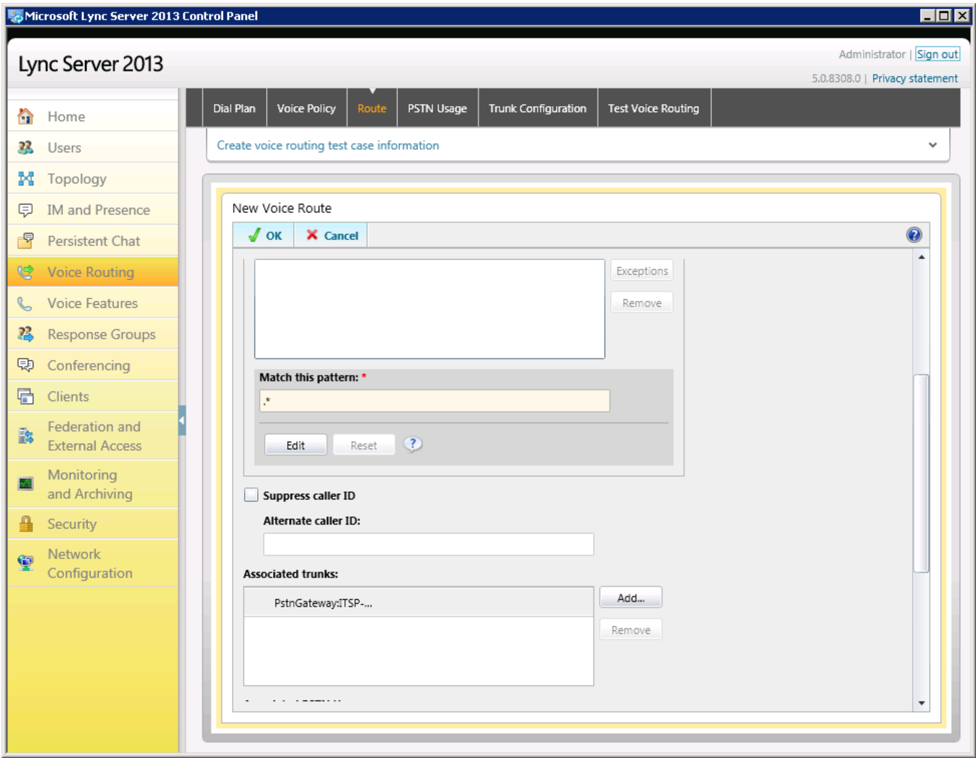
a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



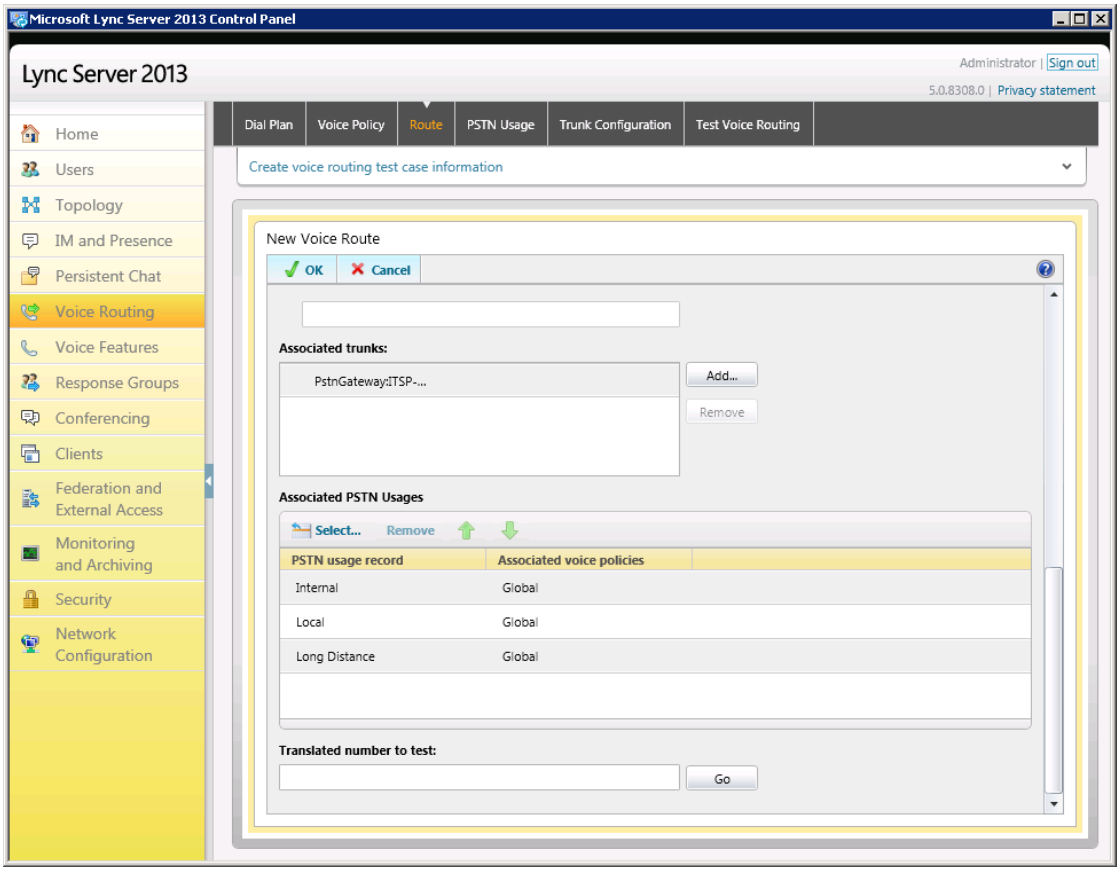
b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



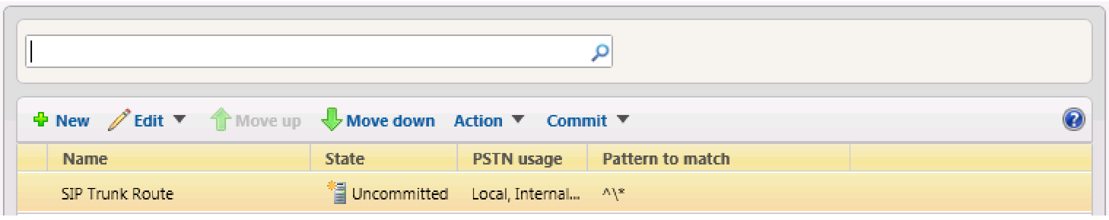
9. Associate a PSTN Usage to this route:
   a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



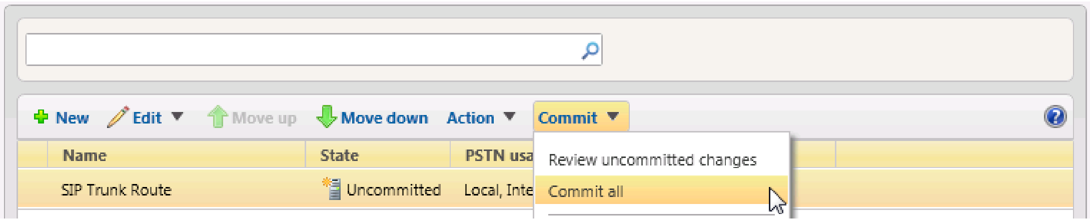
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



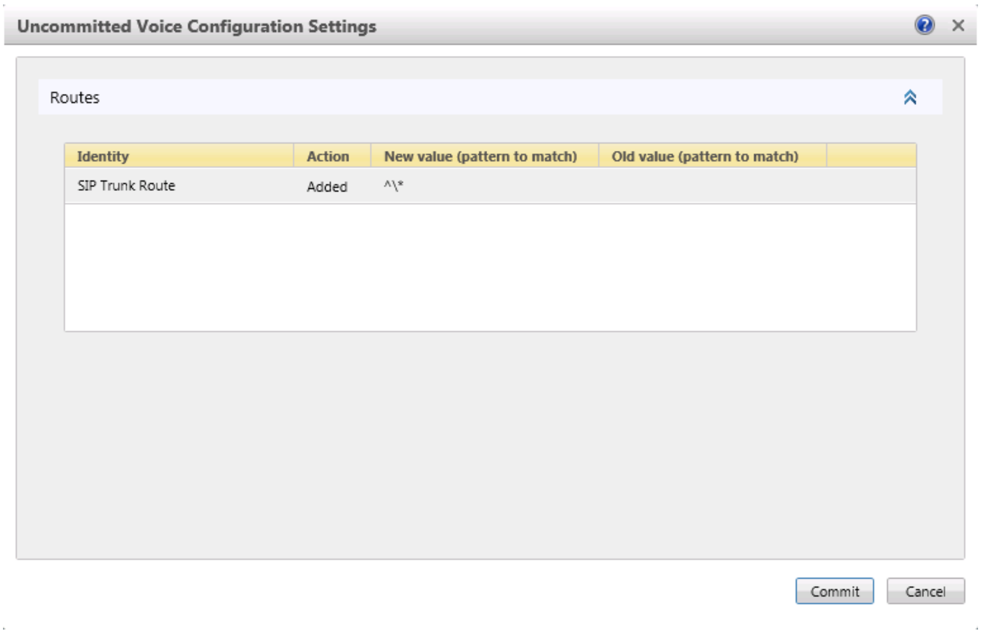
11. From the 'Commit' drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



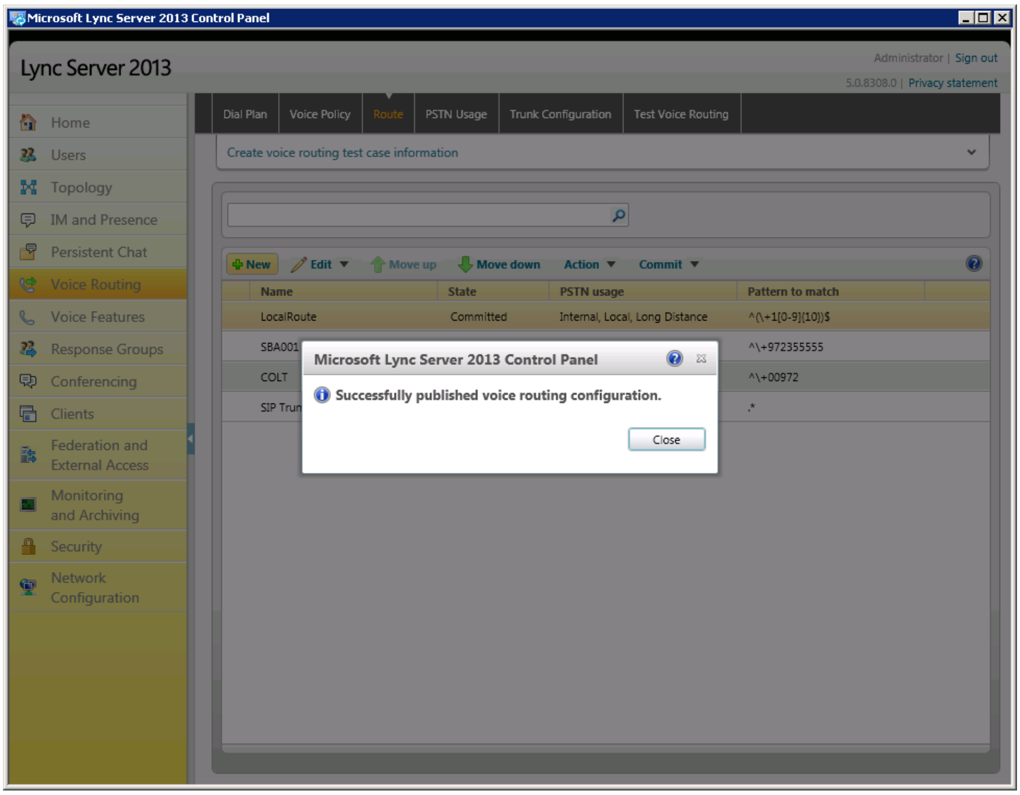
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



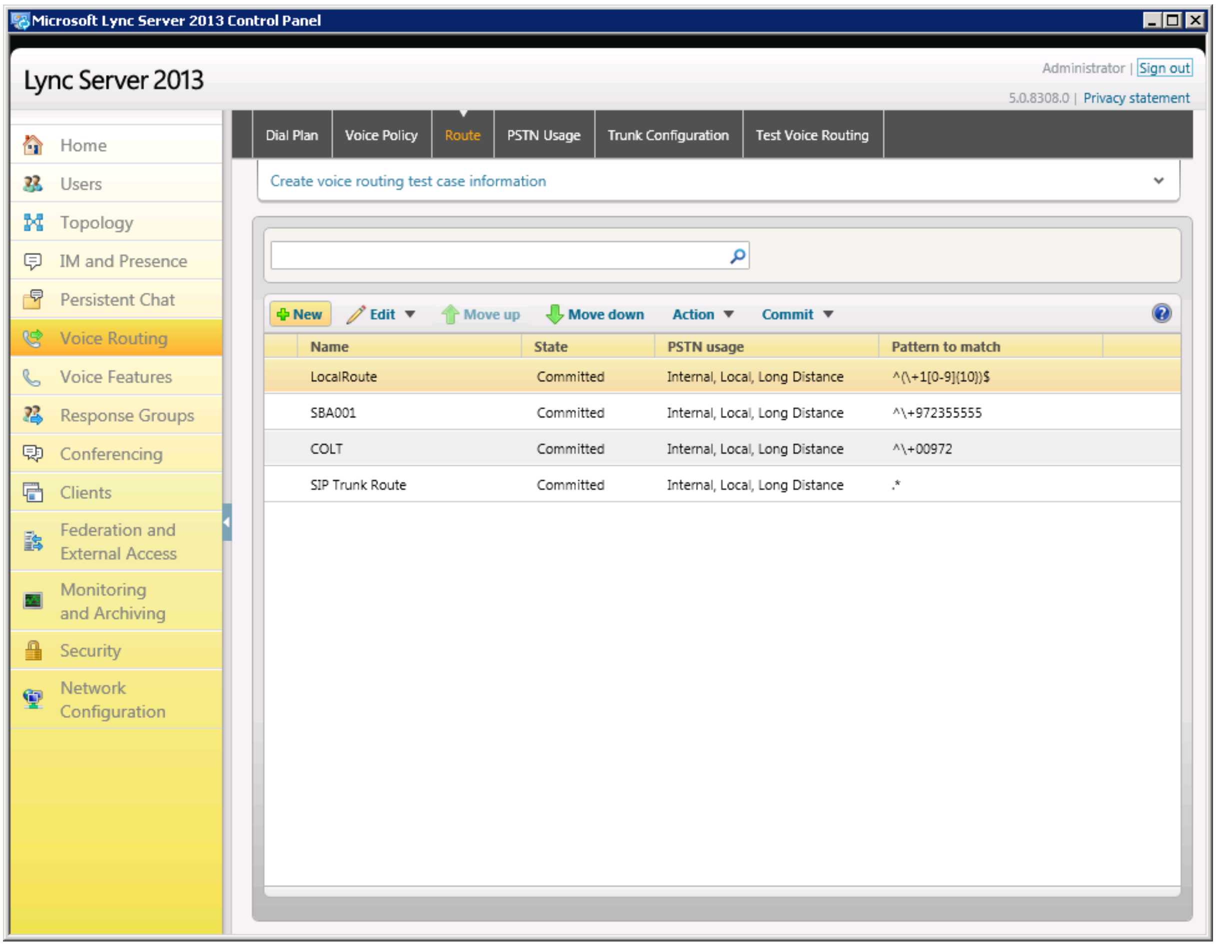
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

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

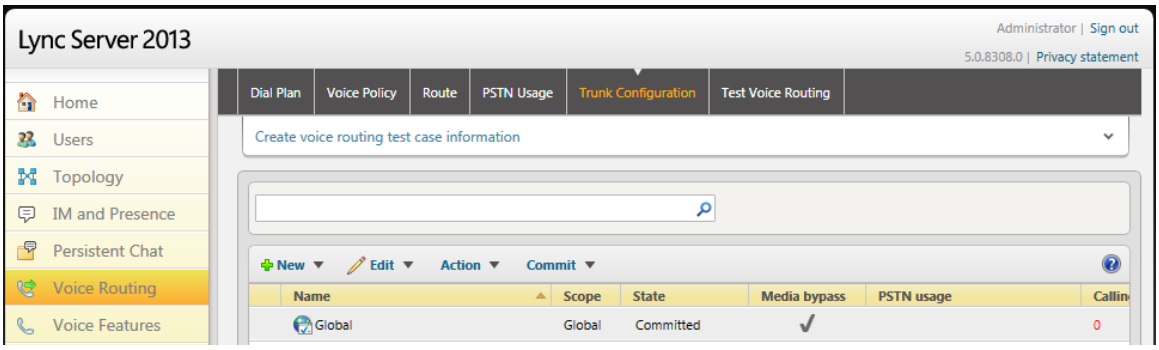


14. For ITSPs that implement a call identifier, continue with the following steps:

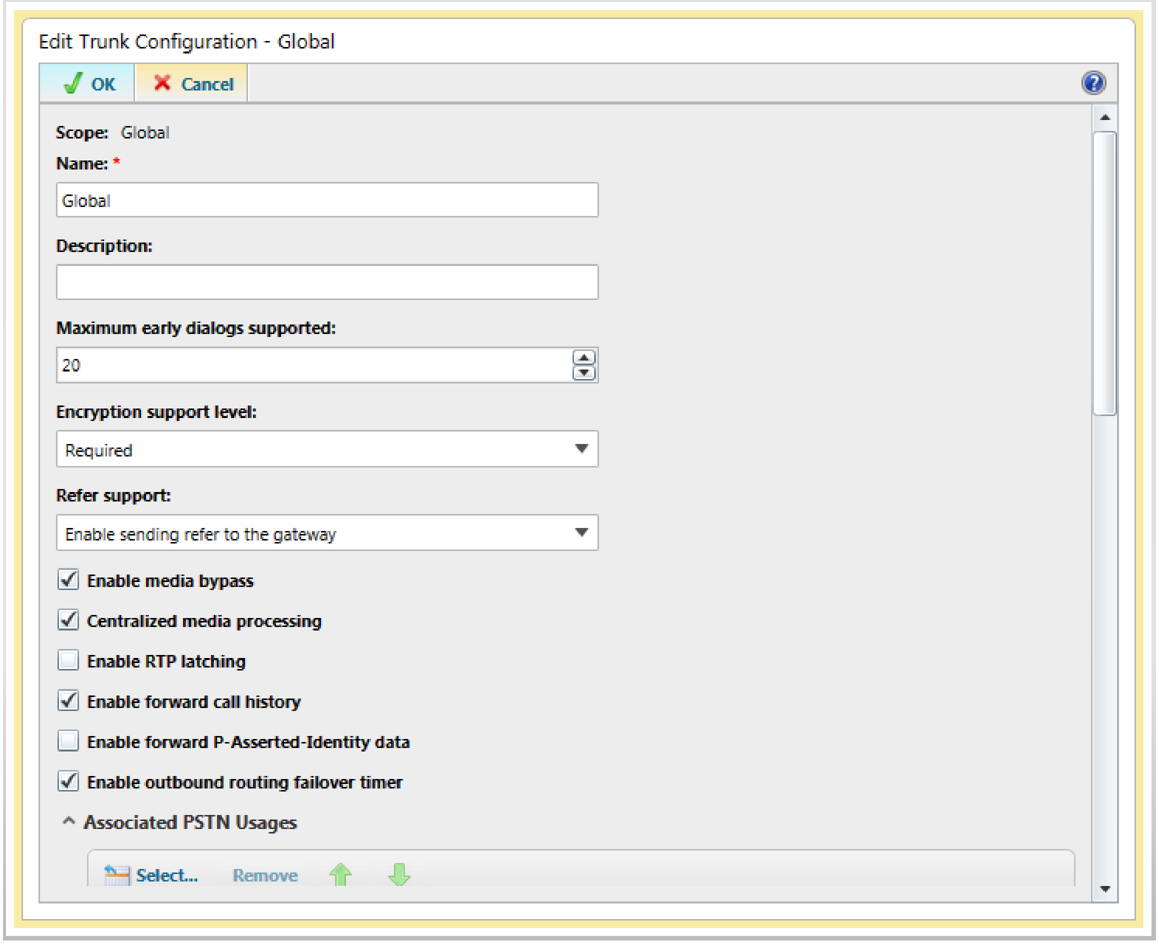
> **Note:** The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Lync user number). This ID is required by G12 SIP Trunk in the P-Asserted-Identity header. Using a Message Manipulation rule (see Section 4.13 on page 61), the device adds this ID to 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** option, and then click **OK**.

d. Repeat Steps 11 through 13 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 G12 SIP Trunk. The procedure is based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

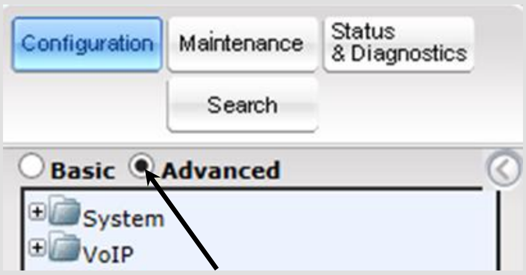
- E-SBC WAN interface - G12 SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

- To implement Microsoft Lync and G12 SIP Trunk based on the configuration described in this section, the 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 line with the enterprise'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 **Advanced** display mode, selectable as follows:



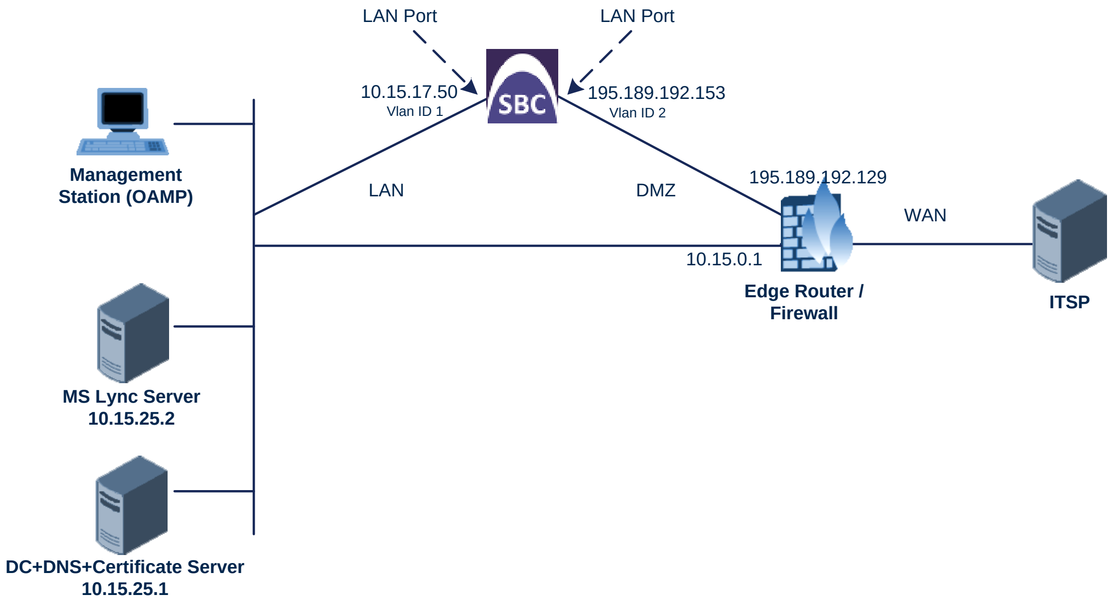
Note that when the E-SBC is reset, the navigation tree reverts to **Basic** display mode.

4.1 Step 1: Configure IP Network Interfaces

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

- E-SBC interfaces with the following IP entities:
  - Lync servers located on the LAN
  - G12 SIP Trunk located on the WAN
- E-SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure Network Interfaces

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

- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "WANSP")

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

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

Parameter	Value
IP Address	**10.15.17.55** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.25.1**
Underlying Interface	**GROUP_1** (Ethernet port group)

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

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.189.192.158** (WAN IP address)
Prefix Length	**16** (for 255.255.0.0)
Gateway	**195.189.192.129** (router's IP address)
VLAN ID	**2**
Interface Name	**WANSP**
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Interface	**GROUP_2**

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

The configured IP network interfaces are shown below:

Figure 4-2: Configured Network Interfaces in IP Interfaces Table

IP Interfaces Table

Add Index | Done

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	IPv4 Manual	10.15.17.55	16	10.15.0.1	1	Voice	10.15.25.1	0.0.0.0	GROUP_1
1	Media + Control	IPv4 Manual	195.189.192.158	25	195.189.192.129	2	WANSP	80.179.52.100	80.179.52.100	GROUP_2

4.1.2 Step 1b: Configure the Native VLAN ID

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

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

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

Figure 4-3: Configured Port 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: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Enabling SBC Application

SAS Application	Disable
SBC Application	Enable
IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for the setting to take effect (see Section 4.15 on page 71).

4.3 Step 3: Configure Signaling Routing Domains

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

The SRD comprises:

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

4.3.1 Step 3a: Configure Media Realms

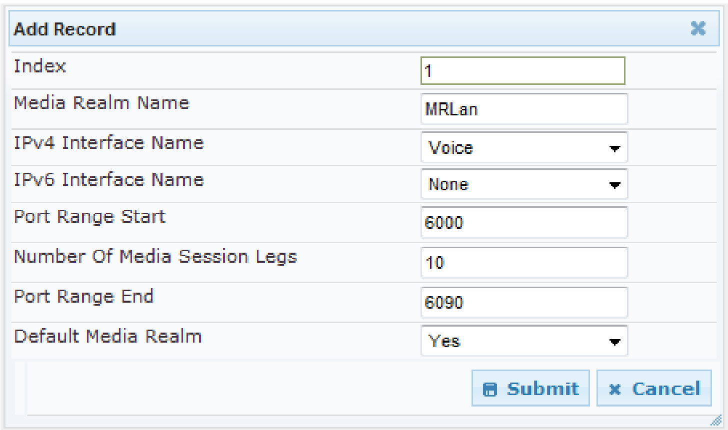
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** > **Media Realm Table**).
2. Configure a Media Realm for LAN traffic:

Parameter	Value
Index	**1**
Media Realm Name	**MRLan** (descriptive name)
IPv4 Interface Name	**Voice**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

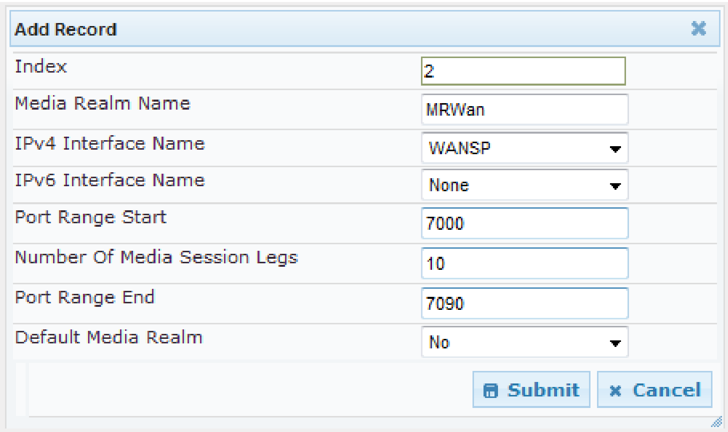
Figure 4-5: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

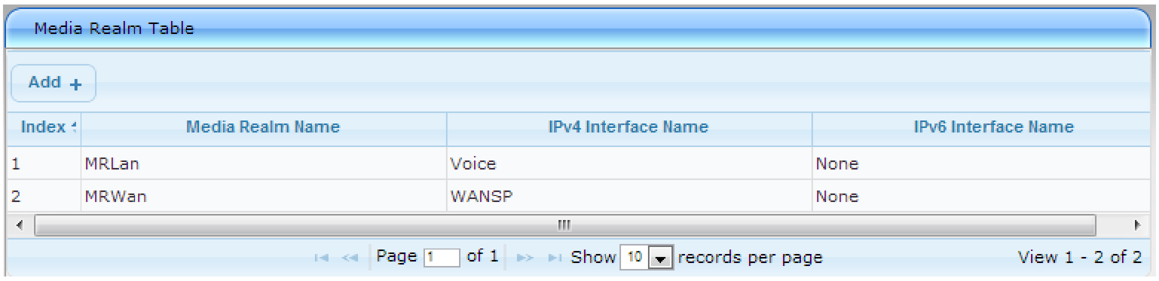
Parameter	Value
Index	**2**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**WANSP**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The figure below shows the configured Media Realms.

Figure 4-7: Configured Media Realms in Media Realm Table



4.3.2 Step 3b: Configure SRDs

This step describes how to configure the SRDs.

➢ **To configure SRDs:**

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

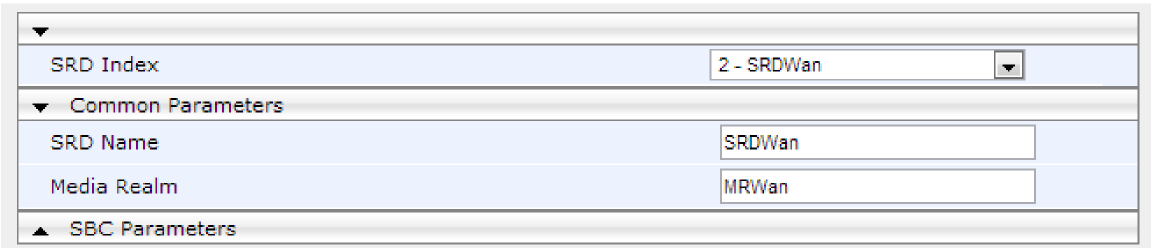
Parameter	Value
SRD Index	**1**
SRD Name	**SRDLan** (descriptive name for SRD)
Media Realm	**MRLan** (associates SRD with Media Realm)

Figure 4-8: Configuring LAN SRD

3. Configure an SRD for the E-SBC's external interface (toward the G12 SIP Trunk):

Parameter	Value
SRD Index	**2**
SRD Name	**SRDWan**
Media Realm	**MRWan**

Figure 4-9: Configuring WAN SRD



4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

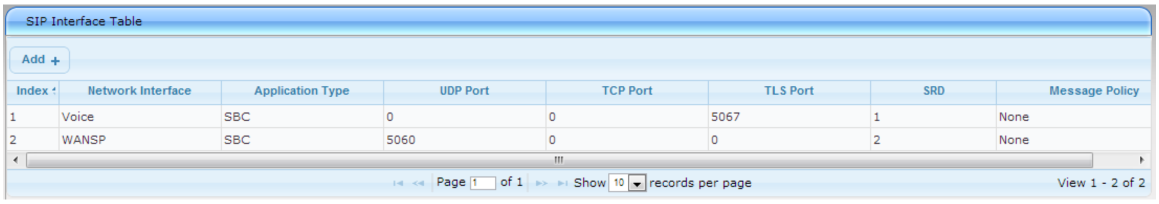
Parameter	Value
Index	**1**
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**1**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
Network Interface	**WANSP**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0**
SRD	**2**

The figure below shows the configured SIP Interfaces.

Figure 4-10: Configured SIP Interfaces in SIP Interface Table


SIP Interface Table

Add +

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

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

4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Lync Server 2013
- G12 SIP Trunk

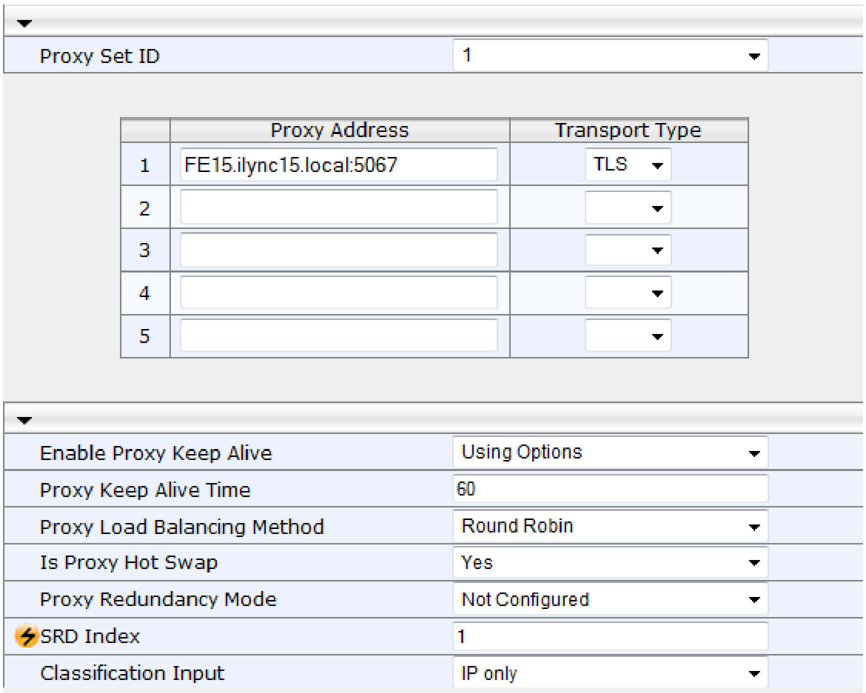
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

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

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**FE15.ilync15.local:5067** (Lync Server 2013 IP address / 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**

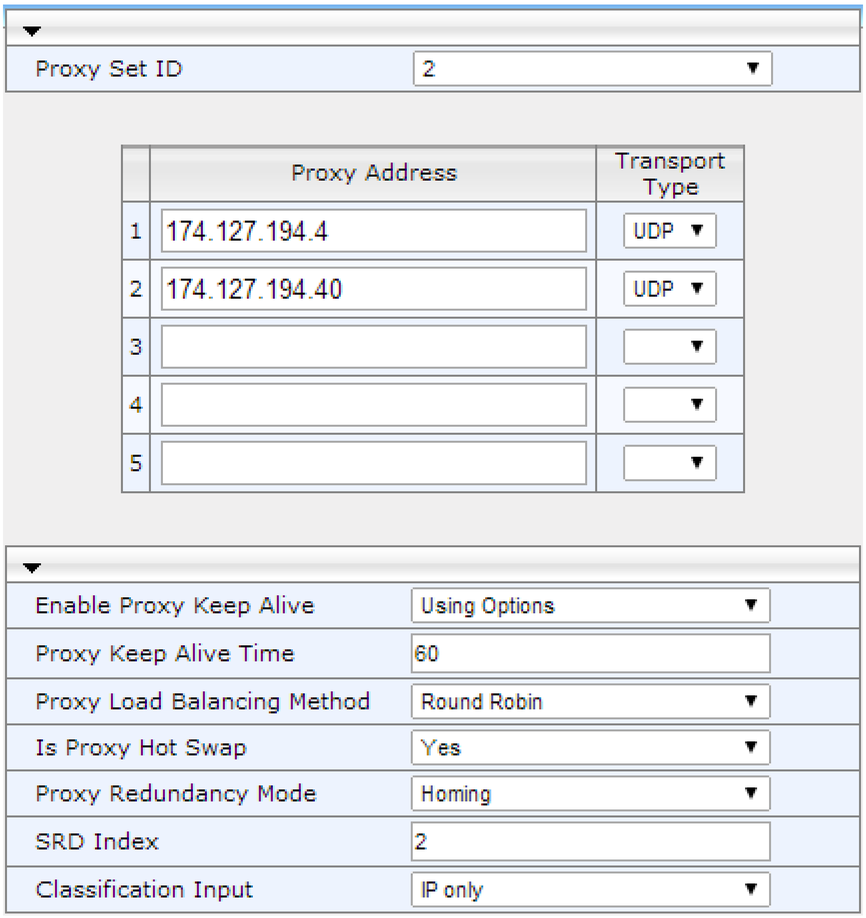
Figure 4-11: Configuring Proxy Set for Microsoft Lync Server 2013



3. Configure a Proxy Set for the G12 SIP Trunk:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**174.127.194.4** (G12 first IP address)
Transport Type	**UDP**
Proxy Address	**174.127.194.40** (G12 second IP address)
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	**2** (enables classification by Proxy Set for SRD of IP Group belonging to G12 SIP Trunk)

Figure 4-12: Configuring Proxy Set for G12 SIP Trunk



4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.15 on page 71).

4.5 Step 5: Configure IP Groups

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

In the interoperability test topology, IP Groups are configured for the following IP entities:

- Lync Server 2013 (Mediation Server) located on LAN
- G12 SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Configure an IP Group for the Lync Server 2013 Mediation Server:

Parameter	Value
Index	**1**
Type	**Server**
Description	**Lync Server** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**195.189.192.158**
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

3. Configure an IP Group for the G12 SIP Trunk:

Parameter	Value
Index	**2**
Type	**Server**
Description	**G12** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**195.189.192.158**
SRD	**2**
Media Realm Name	**MRWan**
IP Profile ID	**2**

The figure below shows the configured IP Groups:

Figure 4-13: Configured IP Groups in 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 Prof
1	Server	Lync	1	195.189.192.158			1	MRLan	1
2	Server	G12	2	195.189.192.158			2	MRWan	2

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

4.6 Step 6: Configure IP Profiles

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

In the interoperability test topology, IP Profiles are configured for these IP entities:

- Microsoft Lync Server 2013, to operate in secure mode using SRTP and TLS
- G12 SIP trunk, to operate in non-secure mode using RTP and UDP

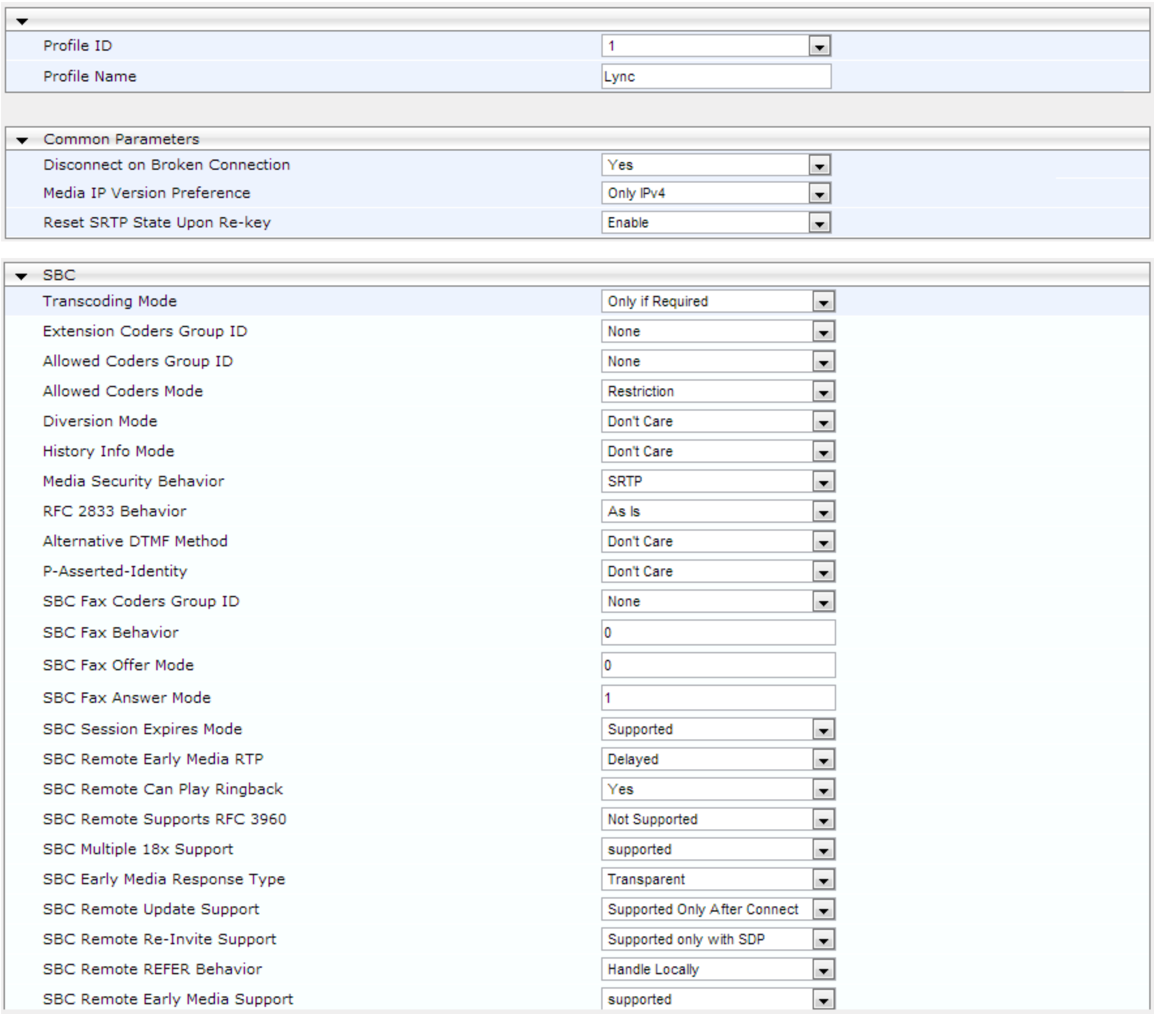
Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 41).

➢ **To configure IP Profiles:**

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

Parameter	Value
Profile ID	**1**
Reset SRTP State Upon Re-key	**Enable**
Extension Coders Group ID	**Coders Group 1**
Media Security Behavior	**SRTP**
SBC Remote Early Media RTP	**Delayed** (required as Lync Server 2013 does not immediately send RTP to the remote side when it sends a SIP 18x response)
SBC Remote Update Support	**Supported Only After Connect**
SBC Remote Re-Invite Support	**Supported Only With SDP**
SBC Remote Refer Behavior	**Handle Locally** (required as as Lync Server 2013 does not support receipt of SIP REFER)
SBC Remote 3xx Behavior	**Handle Locally** (required as as Lync Server 2013 does not support receipt of SIP 3xx responses)
SBC Remote Delayed Offer Support	**Not Supported**

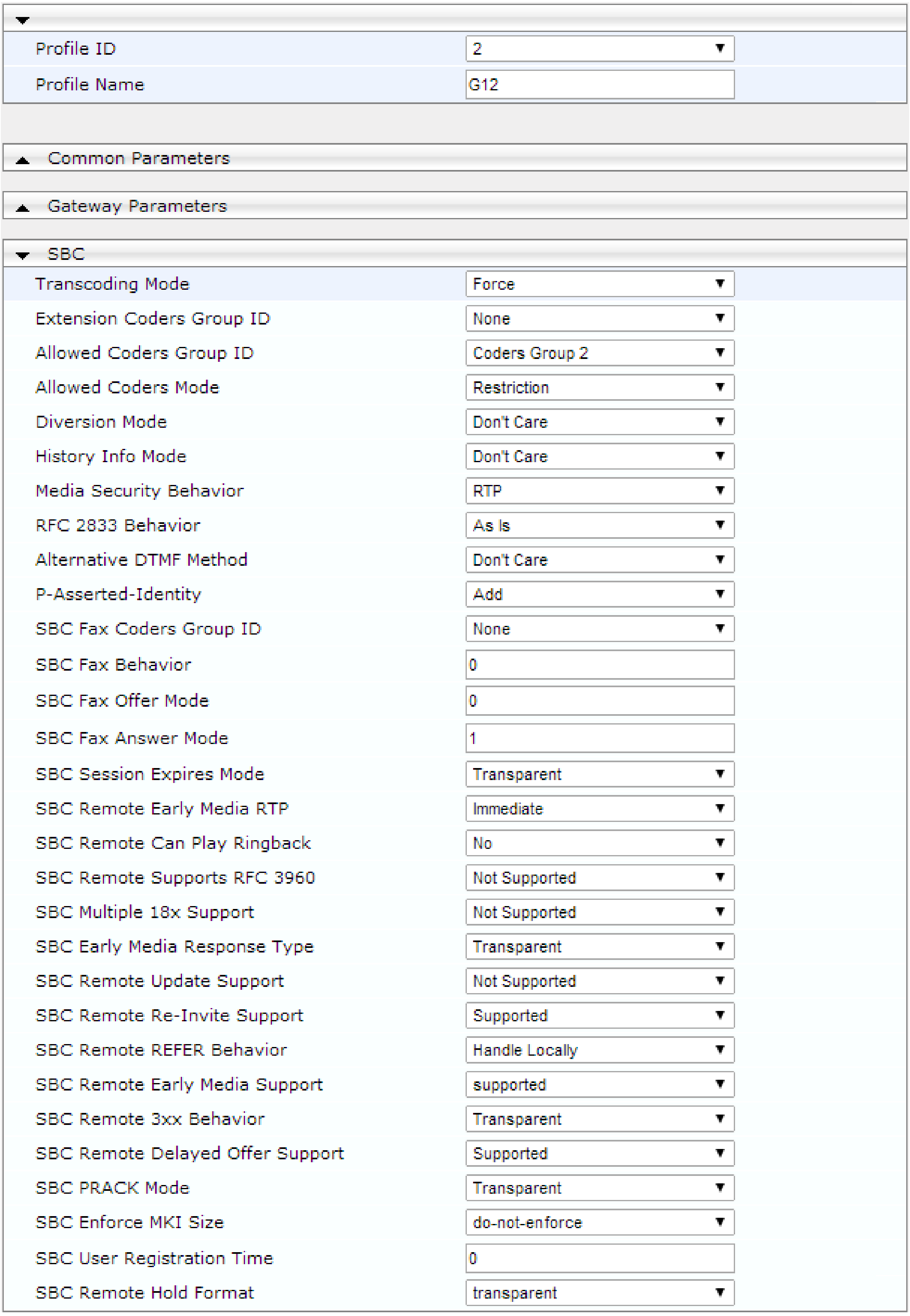
Figure 4-14: Configuring IP Profile for Lync Server 2013



3. Configure an IP Profile for the G12 SIP Trunk:

Parameter	Value
Profile ID	**2**
Transcoding Mode	**Force**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Restriction** (lists only Allowed in SDP offer)
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** (required for anonymous calls)
SBC Remote Can Play Ringback	**No** (required as Lync Server 2013 does not provide a ringback tone for incoming calls)
SBC Remote Update Support	**Not Supported**
SBC Remote Refer Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)

Figure 4-15: Configuring IP Profile for G12 SIP Trunk



4.7 Step 7: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Lync Server 2013 supports the G.711 coder while the network connection to G12 SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the G12 SIP Trunk.

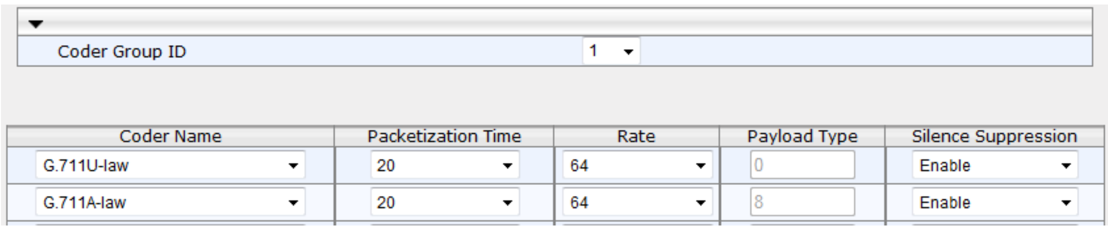
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 43).

➢ **To configure coders:**

1. Open the Coder Group Settings (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**).
2. Configure a Coder Group for Lync Server 2013:

Parameter	Value
Coder Group ID	**1**
Coder Name	▪ **G.711 U-law** ▪ **G.711 A-law**
Silence Suppression	**Enable** (for both coders)

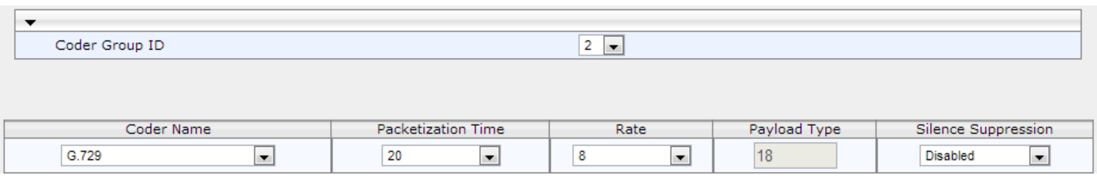
Figure 4-16: Configuring Coder Group for Lync Server 2013



3. Configure a Coder Group for G12 SIP Trunk:

Parameter	Value
Coder Group ID	**2**
Coder Name	**G.729**

Figure 4-17: Configuring Coder Group for G12 SIP Trunk



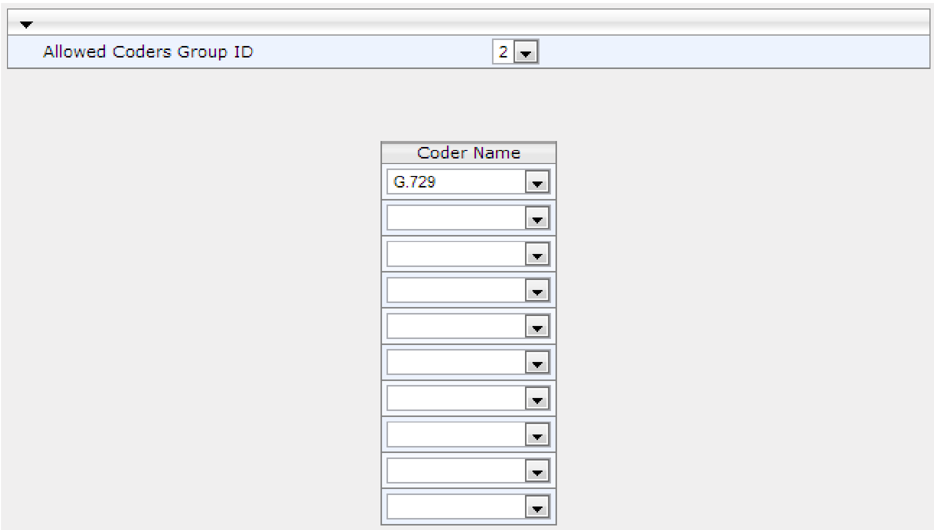
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the G12 SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the G12 SIP Trunk in the previous step (see Section 4.6 on page 43).

➢ **To set a preferred coder for the G12 SIP Trunk:**

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

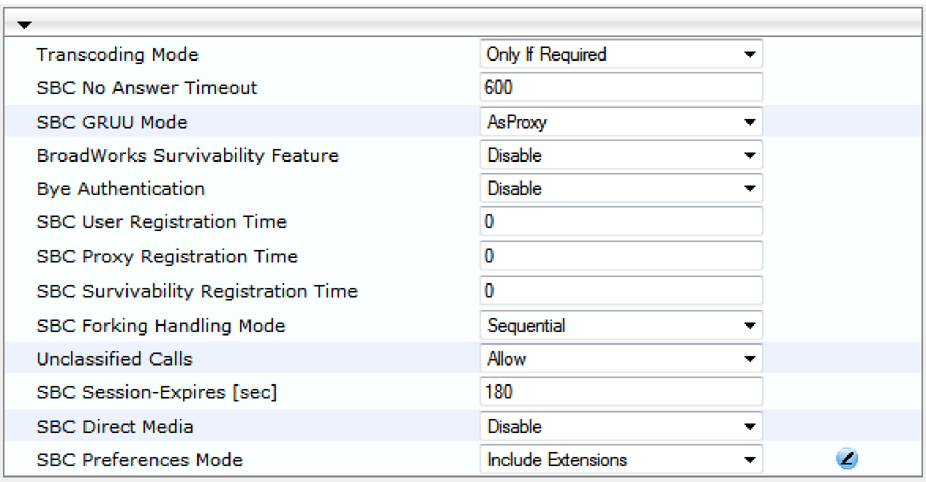
Parameter	Value
Allowed Coders Group ID	**2**
Coder Name	**G.729**

Figure 4-18: Configuring Allowed Coders Group for G12 SIP Trunk



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

Figure 4-19: SBC Preferences Mode



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

4.8 Step 8: Configure a SIP TLS Connection

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

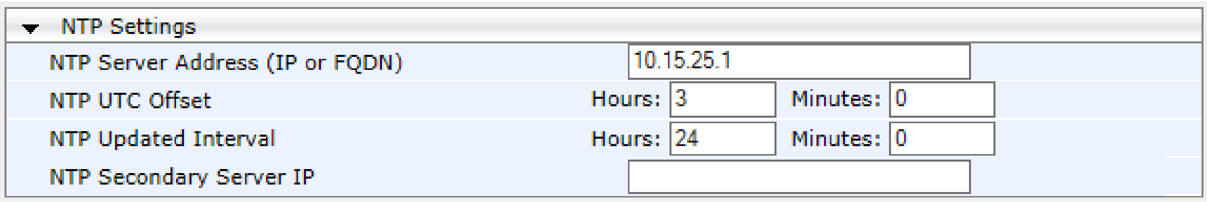
4.8.1 Step 8a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the E-SBC receives the 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., **10.15.25.1**).

Figure 4-20: Configuring NTP Server Address



3. Click **Submit**.

4.8.2 Step 8b: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Lync Server 2013.

The procedure involves these main steps:

a. Generate a Certificate Signing Request (CSR)

b. Request a Device Certificate from the CA

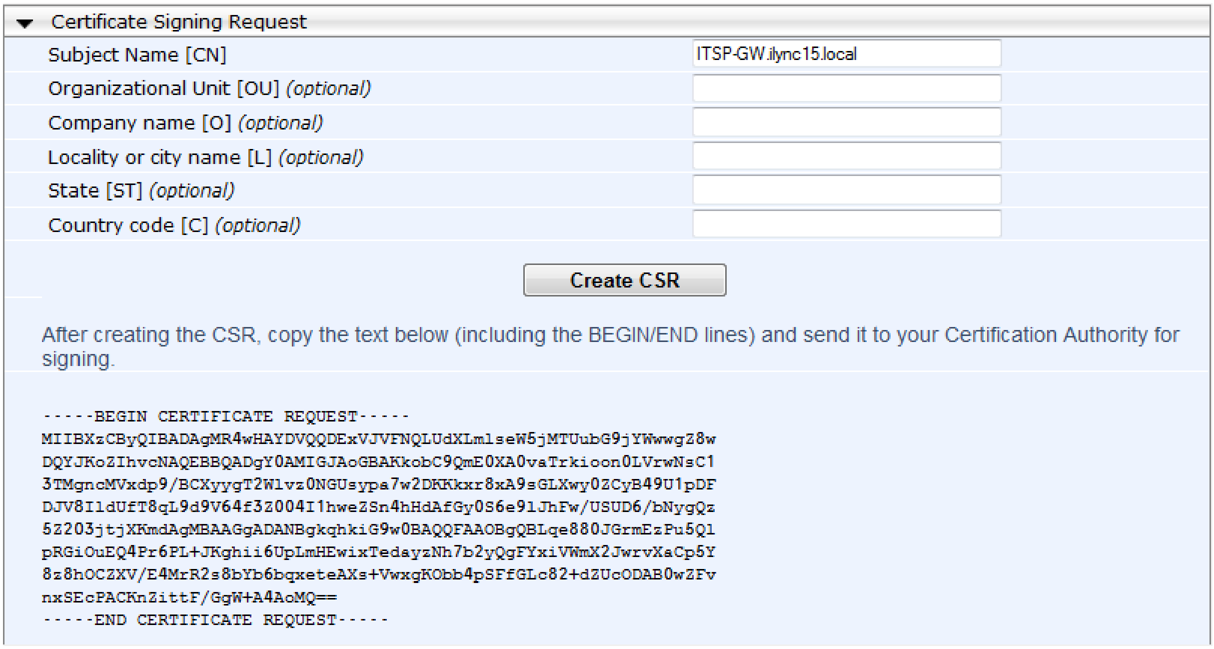
c. Obtain a Trusted Root Certificate from the CA

d. Deploy the Device and Trusted Root Certificates on the E-SBC

➢ **To configure a certificate:**

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

Figure 4-21: Certificates Page - Creating CSR



2. In the 'Subject Name' field, enter the media gateway name (e.g., **ITSP-GW.ilync15.local**).

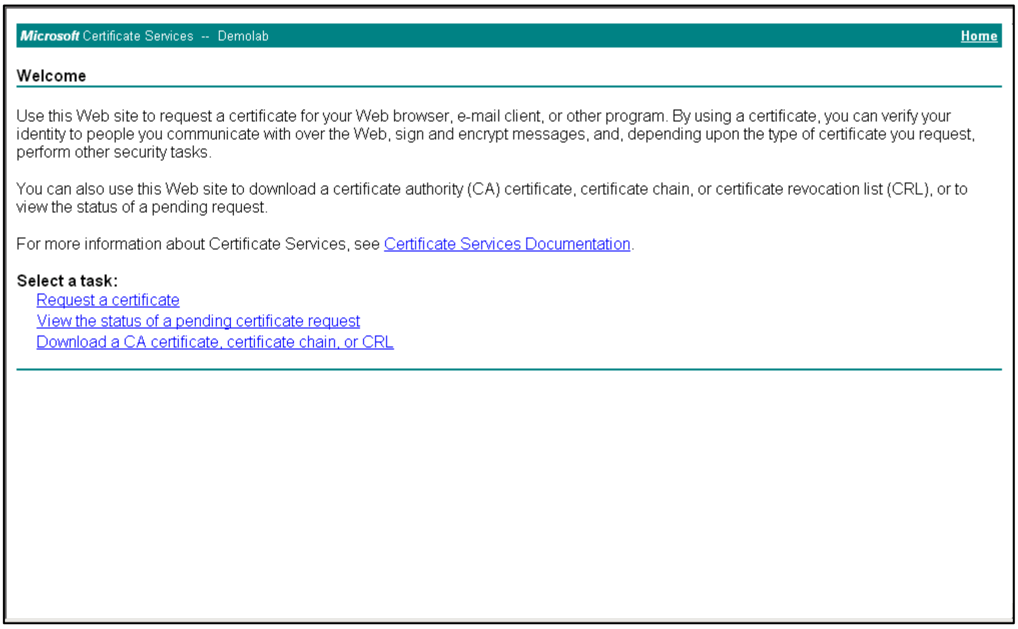
Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).

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*.

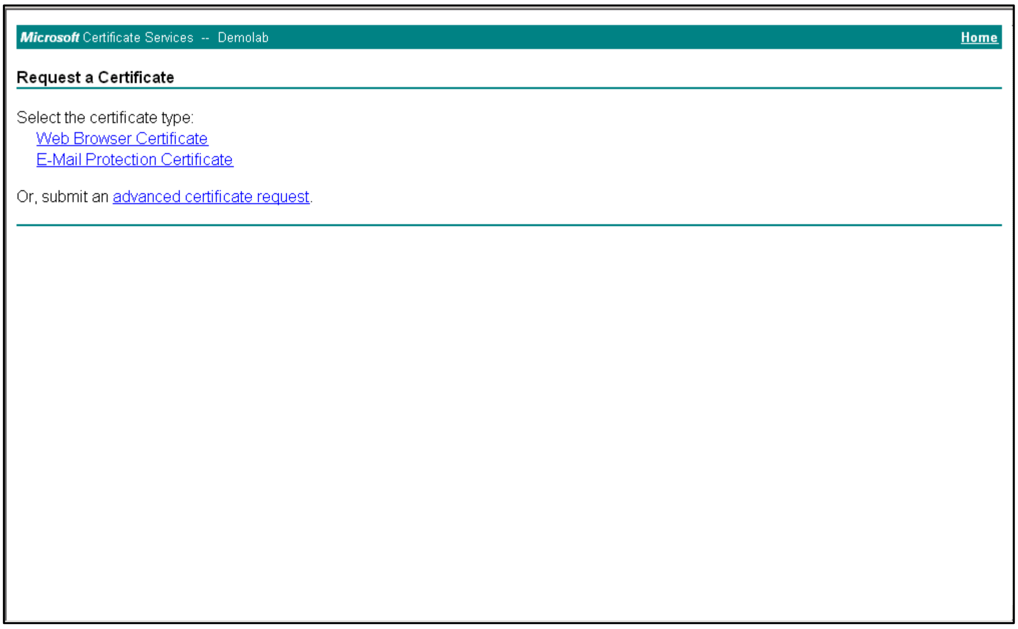
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-22: Microsoft Certificate Services Web Page



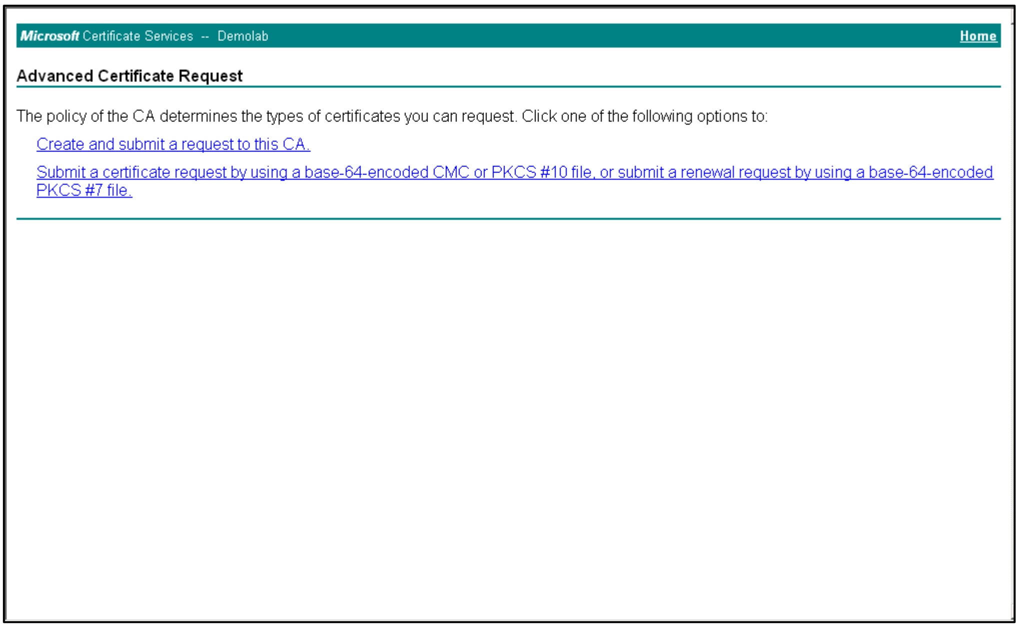
6. Click **Request a certificate**.

Figure 4-23: Request a Certificate Page



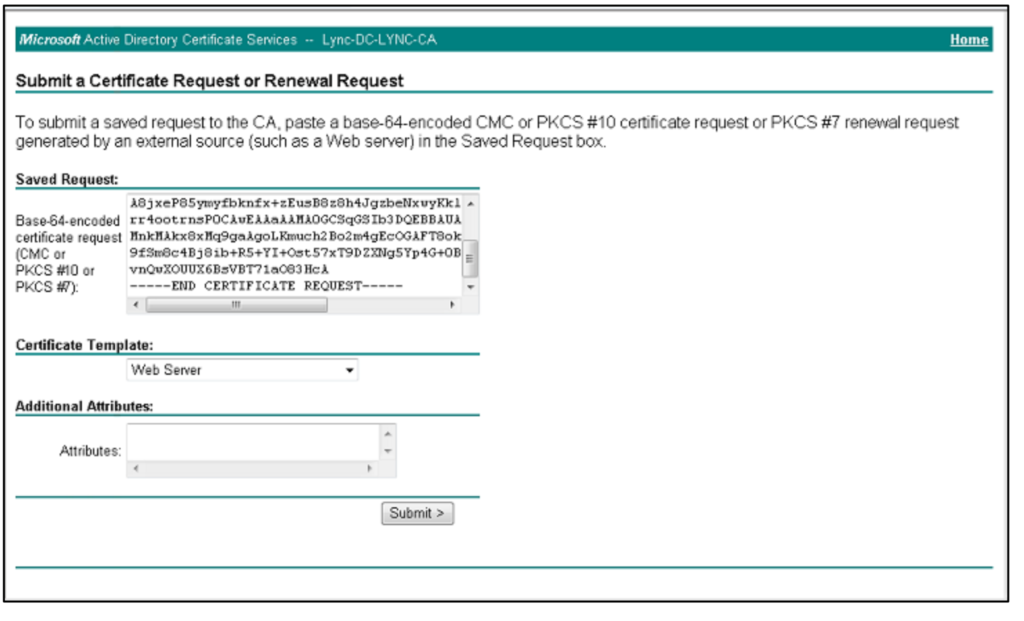
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-24: Advanced Certificate Request Page



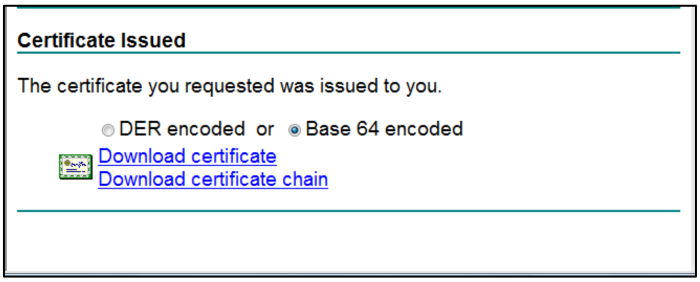
8. Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-25: Submit a Certificate Request or Renewal Request Page



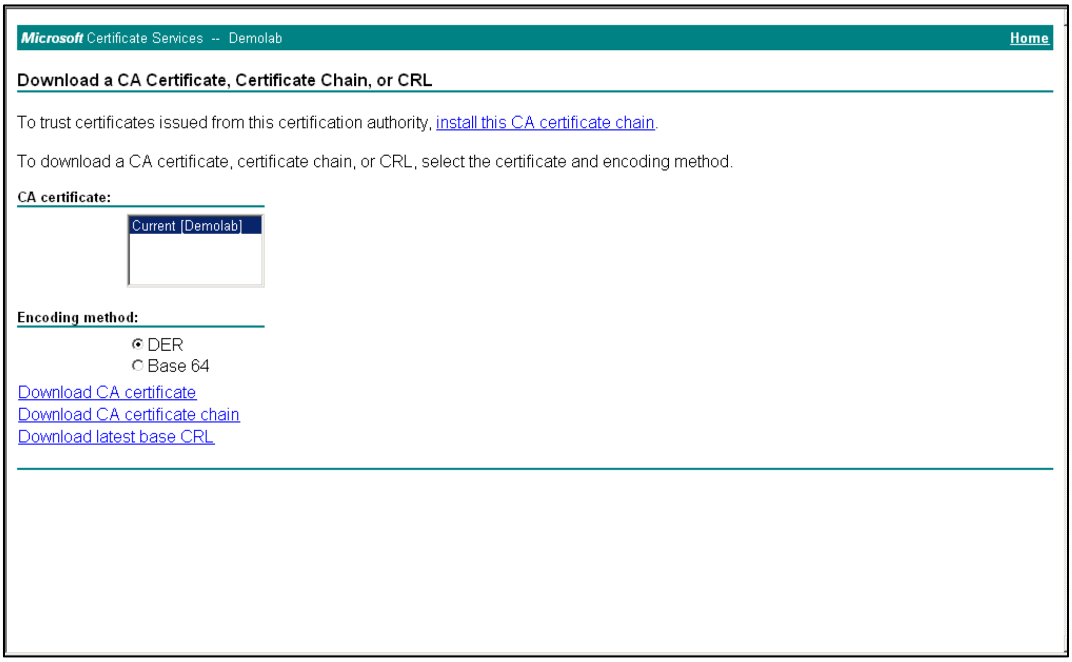
9. Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Saved Request' field.
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-26: Certificate Issued Page



12. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
13. Save the file as *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 **Download a CA certificate**, **certificate chain, or CRL**.

Figure 4-27: Download a CA Certificate, Certificate Chain, or CRL Page



16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.
18. Save the file as *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 4-28: Certificates Page (Uploading Certificate)

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 71).

4.9 Step 9: Configure SRTP

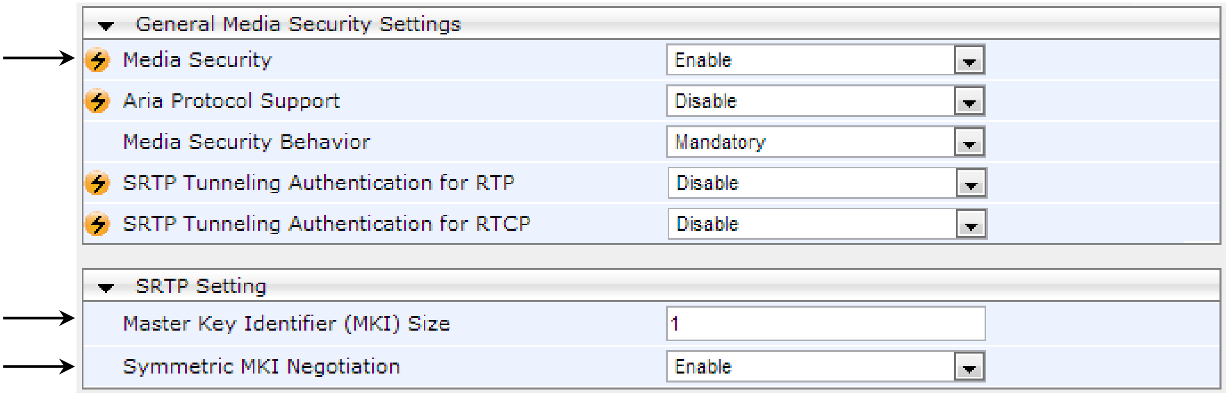
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you must configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 43).

➢ **To configure media security:**

1. Open the Media Security page (**Configuration** tab > **Media** menu > **Media Security**).
2. Configure the parameters as follows:

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

Figure 4-29: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 71).

4.10 Step 10: Configure Maximum IP Media Channels

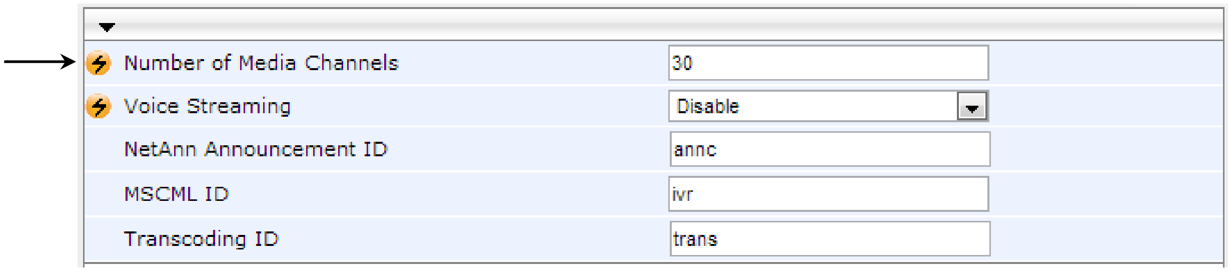
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

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

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

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

Figure 4-30: Configuring Number of IP Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 71).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 41, IP Group 1 represents Lync Server 2013, and IP Group 2 represents G12 SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules are configured to route calls between Lync Server 2013 (LAN) and G12 SIP Trunk (WAN):

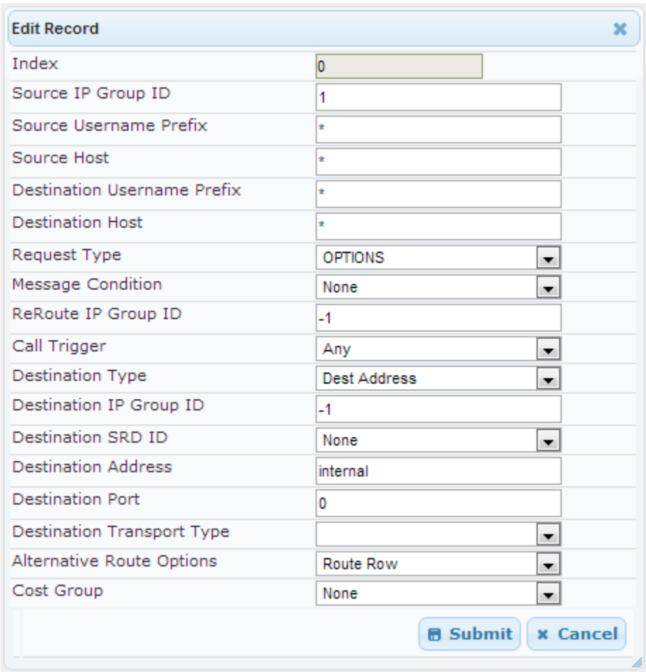
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to G12 SIP Trunk
- Calls from G12 SIP Trunk to Lync Server 2013

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

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

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

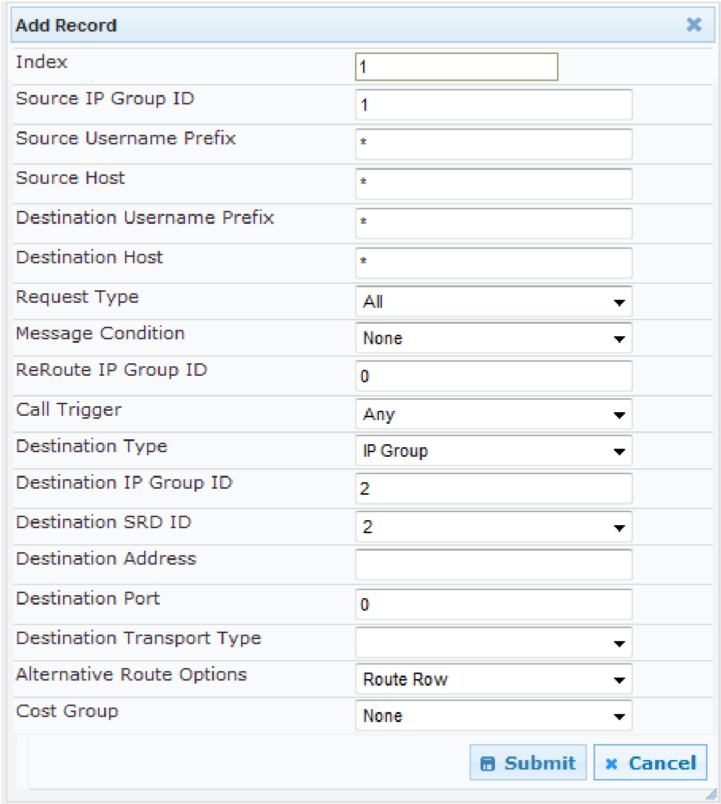
Figure 4-31: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN



3. Configure a rule to route calls from Lync Server 2013 to G12 SIP Trunk:

Parameter	Value
Index	**1**
Source IP Group ID	**1**
Destination Type	**IP Group**
Destination IP Group ID	**2**
Destination SRD ID	**2**

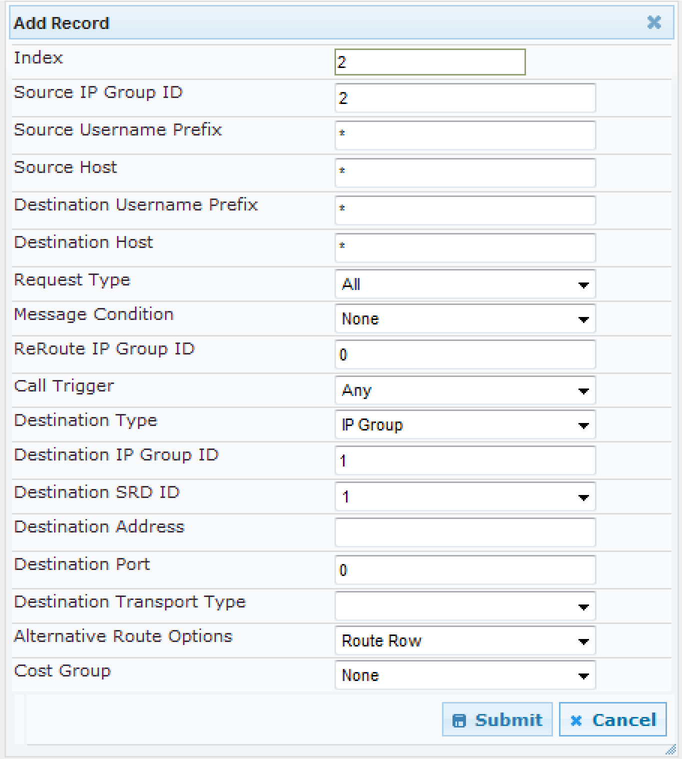
Figure 4-32: Configuring IP-to-IP Routing Rule for LAN to WAN



4. Configure a rule to route calls from G12 SIP Trunk to Lync Server 2013:

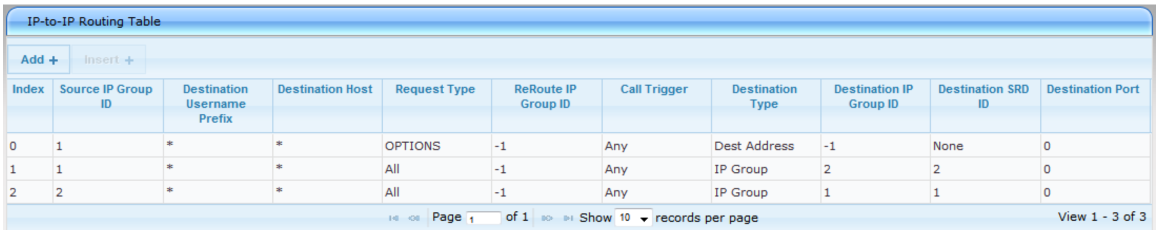
Parameter	Value
Index	**2**
Source IP Group ID	**2**
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 4-33: Configuring IP-to-IP Routing Rule for WAN to LAN



The configured routing rules are shown in the figure below:

Figure 4-34: Configured IP-to-IP Routing Rules in 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 your specific deployment topology.

4.12 Step 12: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 41, IP Group 1 represents Lync Server 2013, and IP Group 2 represents G12 SIP Trunk.

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

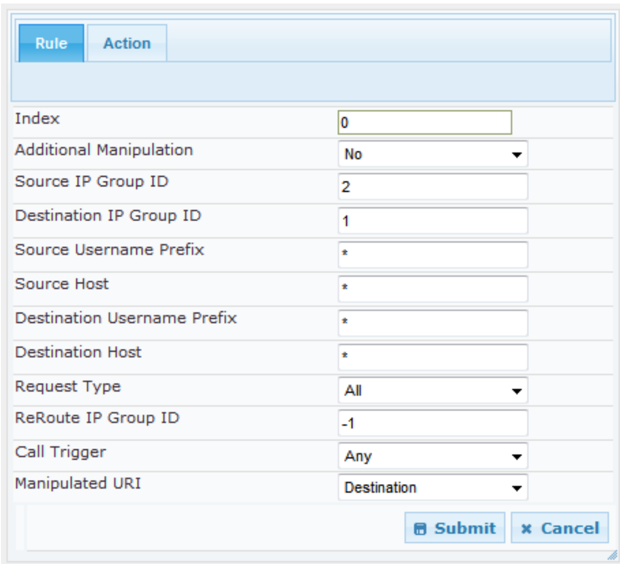
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (G12 SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

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

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

Parameter	Value
Index	**0**
Source IP Group	**2**
Destination IP Group	**1**
Destination Username Prefix	***** (asterisk sign)
Manipulated URI	**Destination**

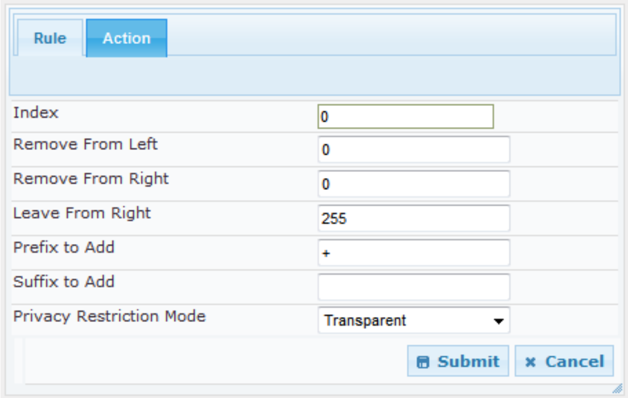
Figure 4-35: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Value
Prefix to Add	**+** (plus sign)

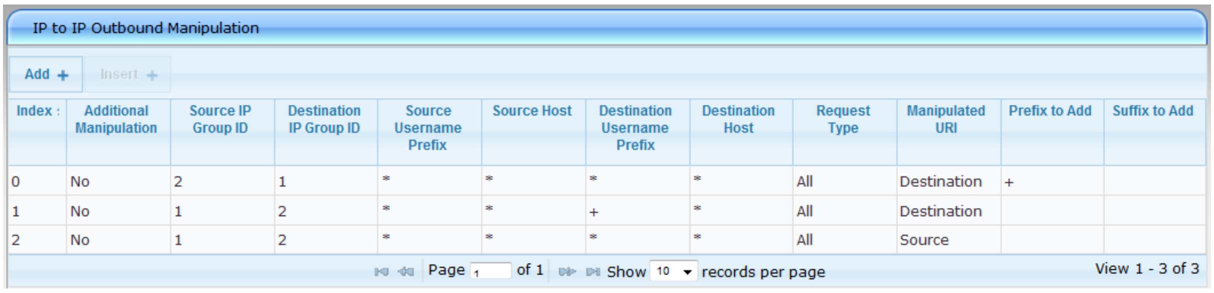
Figure 4-36: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP Group 1 (i.e., Lync Server 2013) and IP Group 2 (i.e., G12 SIP Trunk):

Figure 4-37: Example of Configured IP-to-IP Outbound Manipulation Rules



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

4.13 Step 13: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

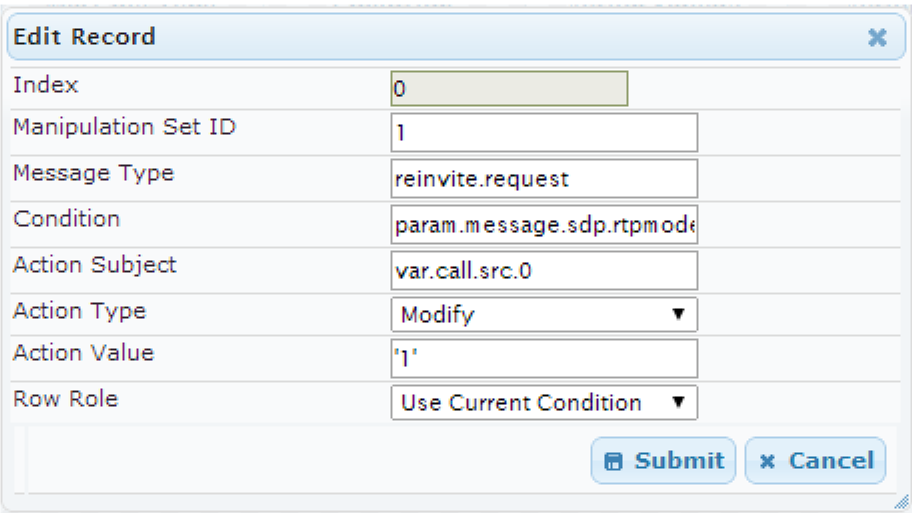
After configuring SIP message manipulation rules, you must assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-initiated Hold), create a variable and set it to **'1'**. This variable manages how the call will be handled in each state (answer, request, etc.).

Parameter	Value
Index	**0**
Manipulation Set ID	**1**
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**

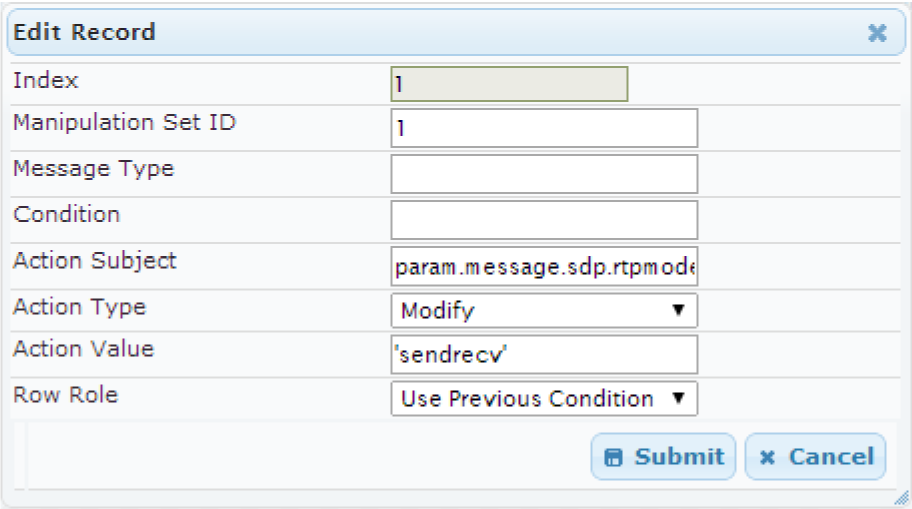
Figure 4-38: Configuring SIP Message Manipulation Rule 0 (for Microsoft Lync)



3. If the manipulation rule Index 0 (above) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to “sendonly” change it to “sendrecv”.

Parameter	Value
Index	**1**
Manipulation Set ID	**1**
Message Type	
Condition	
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**‘sendrecv’**
Row Role	**Use Previous Condition**

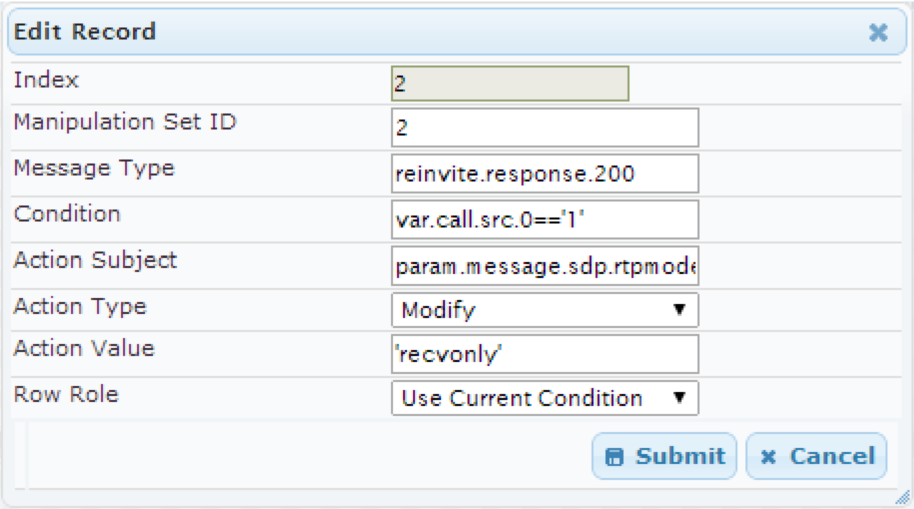
Figure 4-39: Configuring SIP Message Manipulation Rule 1 (for Microsoft Lync)



4. The following rule attempts to normalize the call processing state back to Lync 2013 for the correct reply to the initially received “sendonly”. For every SIP Re-INVITE message with the variable set to **'1'**, change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the G12 SIP Trunk to the Lync initiated Hold.

Parameter	Value
Index	**2**
Manipulation Set ID	**2**
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**

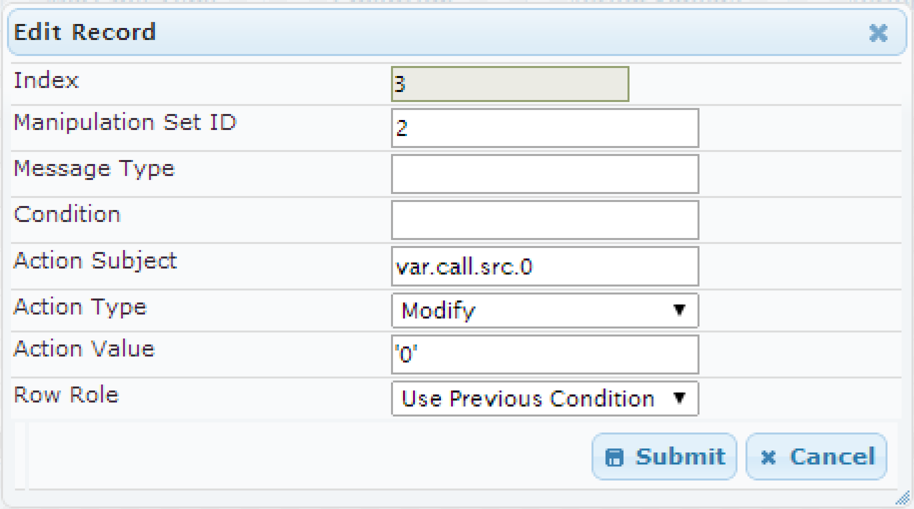
Figure 4-40: Configuring SIP Message Manipulation Rule 2 (for Microsoft Lync)



5. If the manipulation rule Index 2 (above) is executed, then the following rule is also executed. If the variable is determined to be set to **"1"** (in the previous manipulation rule), then set it to **"0"** in order to normalize the call processing state back. Lync now sends Music on Hold to the G12 SIP Trunk even without the G12 SIP Trunk knowing how to receive MoH. The call is now truly on hold with MoH.

Parameter	Value
Index	**3**
Manipulation Set ID	**2**
Message Type	
Condition	
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'0'**
Row Role	**Use Previous Condition**

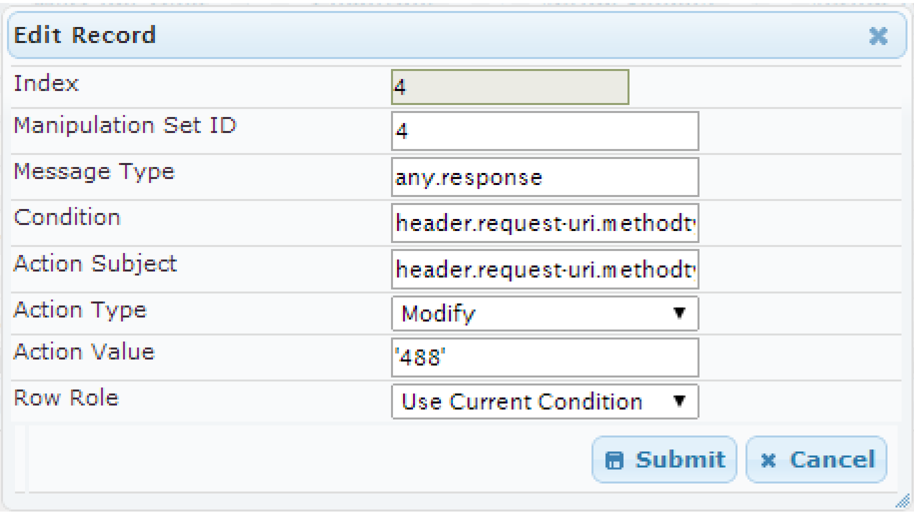
Figure 4-41: Configuring SIP Message Manipulation Rule 3 (for Microsoft Lync)



6. Configure another manipulation rule (Manipulation Set 4) for G12 SIP Trunk. This rule is applied to response messages sent to the G12 SIP Trunk (IP Group 2) for '503 Service not Available' or '480 Temporarily Unavailable' responses initiated by Lync Server 2013 (IP Group 1). This will replace method type '503' or '480' with the value '488' because the G12 SIP Trunk does not recognize '503' and '480' method types.

Parameter	Value
Index	**4**
Manipulation Set ID	**4**
Message Type	**any.response**
Condition	**header.request-uri.methodtype=='503'||'480'**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'488'**
Row Role	**Use Current Condition**

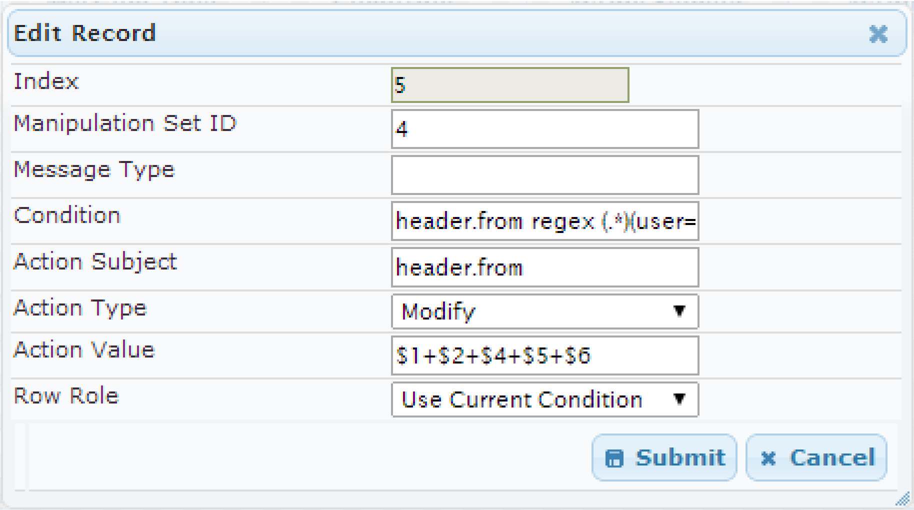
Figure 4-42: Configuring SIP Message Manipulation Rule 4 (for G12 SIP Trunk)



7. Configure another manipulation rule (Manipulation Set 4) for the G12 SIP Trunk. This rule is applied to all messages sent to the G12 SIP Trunk (IP Group 2). The G12 SIP Trunk does not recognize messages that contain the 'gruu' parameter in the From Header. This rule will remove the 'gruu' parameter from SIP From Header for all messages sent to the G12 SIP Trunk.

Parameter	Value
Index	**5**
Manipulation Set ID	**4**
Message Type	
Condition	**header.from regex (.*)(user=phone;)(.*)(.>)(;tag=)(.*)**
Action Subject	**header.from**
Action Type	**Modify**
Action Value	**$1+$2+$4+$5+$6**
Row Role	**Use Current Condition**

Figure 4-43: Configuring SIP Message Manipulation Rule 5 (for G12 SIP Trunk)



8. The G12 SIP Trunk does not send an ALLOW SIP header at all. To refresh the Session Timer from Lync, the header must be added with the value of **'UPDATE'** in all responses sent toward Lync. This is done with the following rule, which should be added for Outbound Message Manipulation Set for Lync IP Group.

Parameter	Value
Index	**6**
Manipulation Set ID	**2**
Message Type	**any.response**
Action Subject	**header.allow**
Action Type	**Add**
Action Value	**'UPDATE'**
Row Role	**Use Current Condition**

Figure 4-44: Configuring SIP Message Manipulation Rule 6 (for Microsoft Lync)

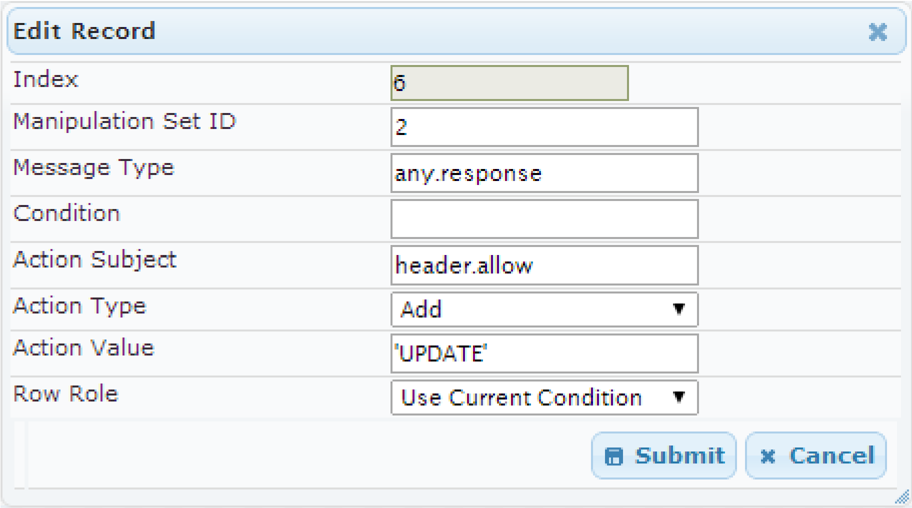
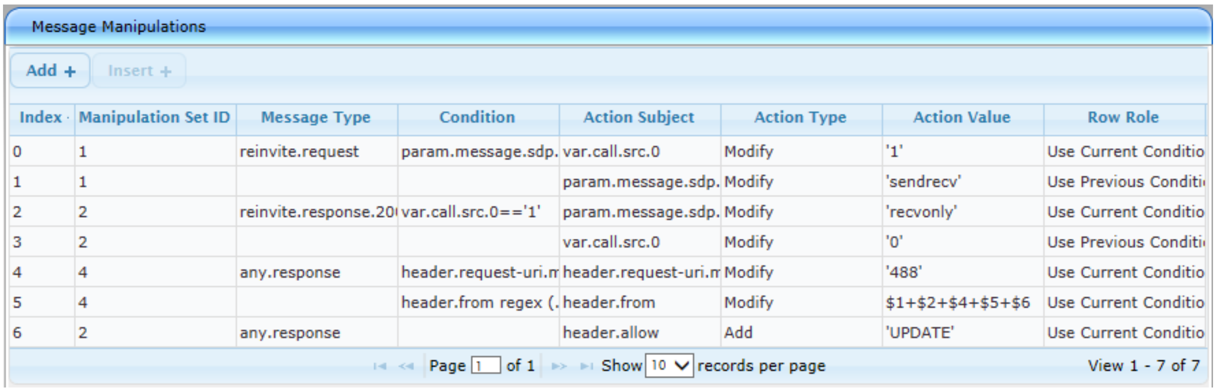


Figure 4-45: Configured SIP Message Manipulation Rules



Message Manipulations

Add + Insert +

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	1	reinvite.request	param.message.sdp.	var.call.src.0	Modify	'1'	Use Current Conditio
1	1			param.message.sdp.	Modify	'sendrecv'	Use Previous Conditi
2	2	reinvite.response.20	var.call.src.0=='1'	param.message.sdp.	Modify	'recvonly'	Use Current Conditio
3	2			var.call.src.0	Modify	'0'	Use Previous Conditi
4	4	any.response	header.request-uri.m	header.request-uri.m	Modify	'488'	Use Current Conditio
5	4		header.from regex (.	header.from	Modify	$1+$2+$4+$5+$6	Use Current Conditio
6	2	any.response		header.allow	Add	'UPDATE'	Use Current Conditio

Page 1 of 1 Show 10 records per page View 1 - 7 of 7

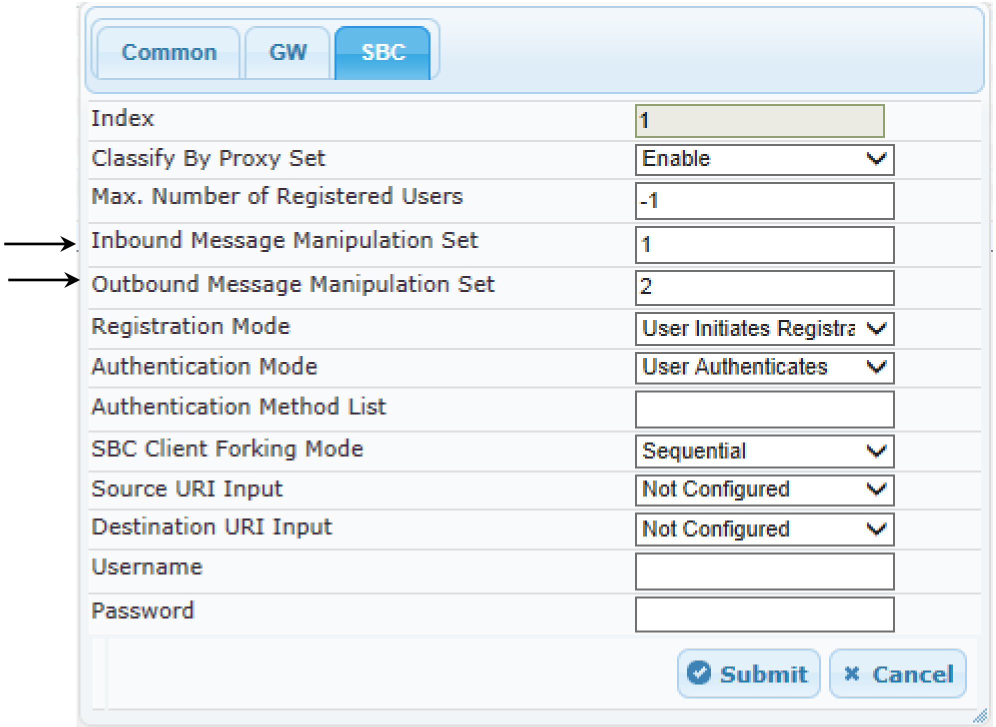
The table displayed below includes SIP message manipulation rules bound together by common Manipulation Set IDs 1, 2 and 4, which are executed for messages sent to and from the G12 SIP Trunk (IP Group 2) as well as the Lync Server 2013 (IP Group 1). These rules are specifically required to enable proper interworking between G12 SIP Trunk and Lync Server 2013. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Table 4-1: SIP Message Manipulation Rules

<table>
<tr><th>Rule Index</th><th>Rule Description</th><th>Reason for Introducing Rule</th></tr>
<tr><td>0</td><td>For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-initiated Hold), create a variable and set it to '1'. This variable manages how the call will be handled in each state (answer, request, etc.).</td><td rowspan="4">The G12 SIP Trunk only supports “inactive” format for Hold. This causes loss of the Music On Hold functionality. These four rules were applied in order to work around this limitation.</td></tr>
<tr><td>1</td><td>If the previous manipulation rule (Index 0) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to “sendonly”, change it to “sendrecv”.</td></tr>
<tr><td>2</td><td>This rule attempts to normalize the call processing state back to Lync 2013 for the correct reply to the initially received “sendonly”. For every SIP Re-INVITE message with the variable set to '1', change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the G12 SIP Trunk to the Lync initiated Hold.</td></tr>
<tr><td>3</td><td>If the manipulation rule Index 2 (above) is executed, then the following rule is also executed. If the variable is determined to be set to "1" (in the previous manipulation rule), then set it to “0” in order to normalize the call processing state back. Lync now sends Music on Hold to the G12 SIP Trunk even without the G12 SIP Trunk knowing how to receive MoH. The call is now truly on hold with MoH.</td></tr>
<tr><td>4</td><td>Configure another manipulation rule (Manipulation Set 4) for G12 SIP Trunk. This rule is applied to response messages sent to the G12 SIP Trunk (IP Group 2) for ‘503 Service not Available’ or ‘480 Temporarily Unavailable’ responses initiated by Lync Server 2013 (IP Group 1). This will replace method type ‘503’ or ‘480’ with the value ‘488’ because the G12 SIP Trunk does not recognize ‘503’ and ‘480’ method types.</td><td>G12 SIP Trunk does not recognize ‘503’ or ‘480’ method type.</td></tr>
<tr><td>5</td><td>Configure another manipulation rule (Manipulation Set 4) for the G12 SIP Trunk. This rule is applied to all messages sent to the G12 SIP Trunk (IP Group 2). The G12 SIP Trunk does not recognize messages that contain the ‘gruu’ parameter in the From Header. This rule will remove the ‘gruu’ parameter from SIP From Header for all messages sent to the G12 SIP Trunk.</td><td>The G12 SIP Trunk does not recognize messages that contain the ‘gruu’ parameter in the From Header.</td></tr>
<tr><td>6</td><td>To refresh the Session Timer from Lync, the header must be added with the value of 'UPDATE' in all responses sent toward Lync. This rule should be added for Outbound Message Manipulation Set for Lync IP Group.</td><td>The G12 SIP Trunk does not send an ALLOW SIP header at all.</td></tr>
</table>

9. Assign Manipulation Set IDs 1 and 2 to IP Group 1:
   a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP 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 **1**.
   e. Set the 'Outbound Message Manipulation Set' field to **2**.

Figure 4-46: Assigning Manipulation Sets 1 and 2 to IP Group 1



   f. Click **Submit**.

10. Assign Manipulation Set ID 4 to IP Group 2:

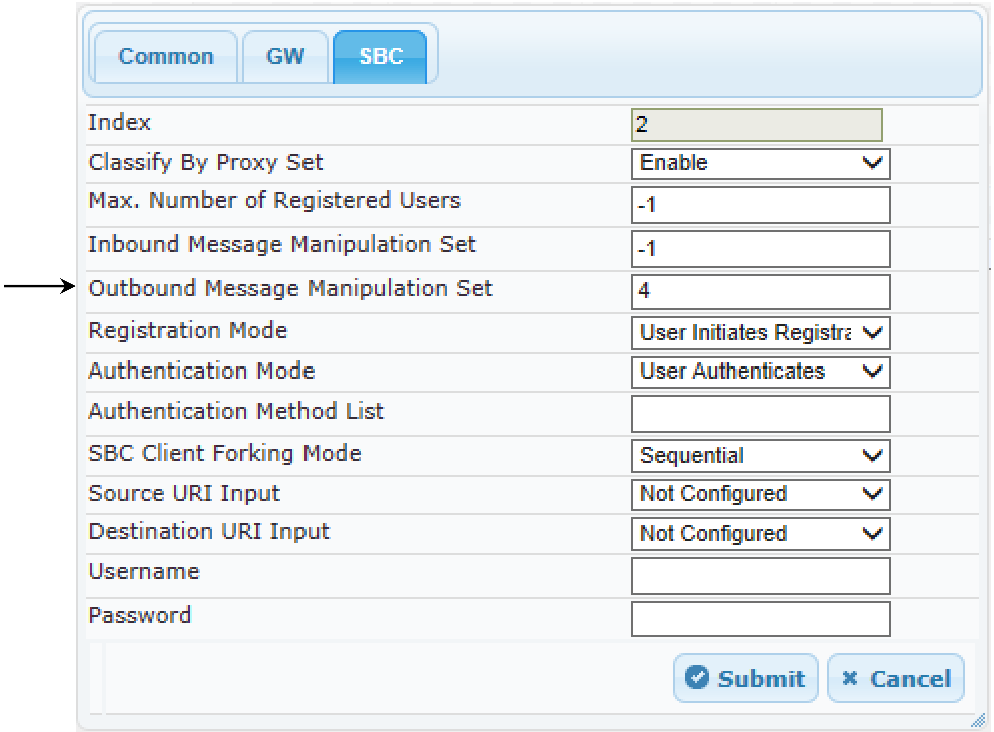
a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).

b. Select the row of IP Group 2, and then click **Edit**.

c. Click the **SBC** tab.

d. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-47: Assigning Manipulation Set 4 to IP Group 2



e. Click **Submit**.

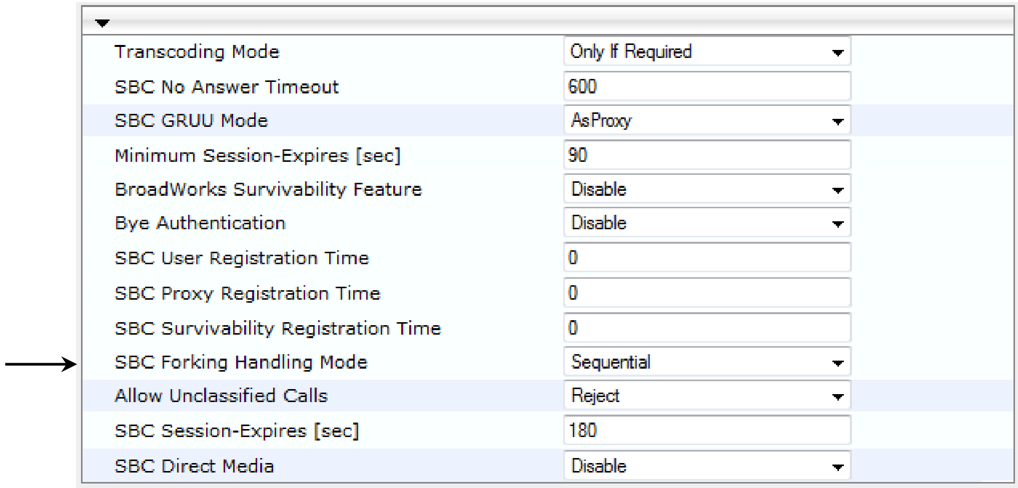
4.14 Step 14: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if 18x with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if 180 response without SDP is received. 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** menu > **SBC** > **General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-48: Configuring Forking Mode



3. Click **Submit**.

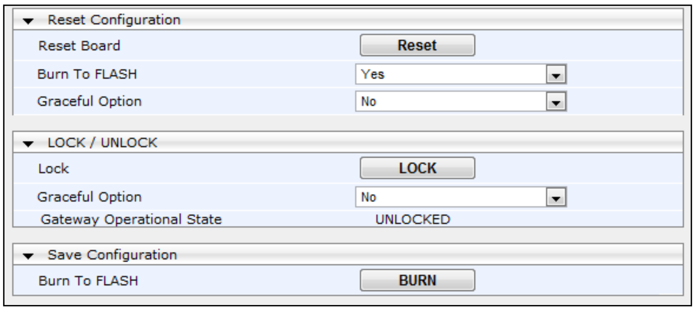
4.15 Step 15: Reset the E-SBC

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

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

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

Figure 4-49: Resetting the E-SBC



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

Reader's Notes

A AudioCodes ini File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 31, is shown below:

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

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

;Board: Mediant 850 - MSBG
;HW Board Type: 69  FK Board Type: 74
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 6.60A.250.009
;DSP Software Version: 5014AE3_R_LD => 660.23
;Board IP Address: 10.15.17.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 368M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;Key features:;Board Type: Mediant 850 - MSBG ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;Channel Type: DspCh=30
IPMediaDspCh=30 ;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 ;DSP Voice features: IpmDetector RTCP-XR
AMRPolicyManagement ;E1Trunks=1 ;T1Trunks=0 ;FXSPorts=8 ;FXOPorts=0
;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;DATA features: ;QOE features: VoiceQualityMonitoring MediaEnhancement
;Control Protocols: MSFT CLI TRANSCODING=30 FEU=100 TestCall=100 MGCP
MEGACO H323 SIP TPNCP SASurvivability SBC=50 ;Default features:;Coders:
G711 G726;

;------ Mediant 850 - MSBG HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : FXS         : 4
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
NTPServerUTCOffset = 7200
LDAPCACHEENTRYTIMEOUT = 12
NTPServerIP = '10.15.25.1'
LDAPSEARCHDNSINPARALLEL = 0
```

```
[BSP Params]

PCMLawSelect = 3

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

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

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1

[SCTP Params]


[IPsec Params]


[Audio Staging Params]
```

```
[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, GE_4_1, GE_4_2;
EtherGroupTable 1 = "GROUP_2", 2, GE_4_3, GE_4_4;

[ \EtherGroupTable ]


[ 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 = 6, 10, 10.15.17.55, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.52.100, 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", WANSP, , 7000, 10, 7090, 0;

[ \CpMediaRealm ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SRDLan", "MRLan", 0, 0, -1, 1;
SRD 2 = "SRDWan", "MRWan", 0, 0, -1, 1;

[ \SRD ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 1 = "174.127.194.4", 0, 2;
ProxyIp 2 = "174.127.194.40", 0, 2;

[ \ProxyIp ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_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", 1, 0, 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, "", 1, 0, 0, -1, 0, 1, 0, 0, 0, 0,
8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 0, 1, 1, 0, 3, 2, 1, 0, 1, 1, 1, 1,
1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0;
IpProfile 2 = "G12", 1, 0, 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, "", -1, 0, 1, 2, 0, 2, 0, 0, 1, 0,
8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 0, 2, 1, 3, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 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, 60, 1, 1, 1, 0, -1;
ProxySet 2 = 1, 60, 1, 1, 2, 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, "Lync", 1, "195.189.192.158", "", 0, -1, -1, 0, -1, 1,
"MRLan", 1, 1, -1, 1, 2, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "G12", 2, "195.189.192.158", "", 0, -1, -1, 0, -1, 2,
"MRWan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]


[ IP2IPRouting ]
```

```
FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_CostGroup;
IP2IPRouting 0 = 1, "*", "*", "*", "*", 6, , -1, 0, 1, -1, , "internal",
0, -1, 0, ;
IP2IPRouting 1 = 1, "*", "*", "*", "*", 0, , -1, 0, 0, 2, 2, "", 0, -1,
0, ;
IP2IPRouting 2 = 2, "*", "*", "*", "*", 0, , -1, 0, 0, 1, 1, "", 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 1 = "Voice", 2, 0, 0, 5067, 1, , -1, 0, 500;
SIPInterface 2 = "WANSP", 2, 5060, 0, 0, 2, , -1, 0, 500;

[ \SIPInterface ]


[ 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, 1, 0,
0, 255, "+", "", 0;
IPOutboundManipulation 1 = 0, 1, 2, "*", "*", "+", "*", 0, -1, 0, 1, 1,
0, 255, "", "", 0;
IPOutboundManipulation 2 = 0, 1, 2, "+", "*", "*", "*", 0, -1, 0, 0, 1,
0, 255, "", "", 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 = "g711Alaw64k", 20, 0, -1, 0;
CodersGroup1 1 = "g711Ulaw64k", 20, 0, -1, 0;

[ \CodersGroup1 ]


[ CodersGroup2 ]

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

[ \CodersGroup2 ]


[ AllowedCodersGroup2 ]

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

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = 1, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 1 = 1, "", "", "param.message.sdp.rtpmode", 2,
"'sendrecv'", 1;
MessageManipulations 2 = 2, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2, "'recvonly'", 0;
MessageManipulations 3 = 2, "", "", "var.call.src.0", 2, "'0'", 1;
MessageManipulations 4 = 4, "any.response", "header.request-
uri.methodtype=='503'||'480'", "header.request-uri.methodtype", 2,
"'488'", 0;
MessageManipulations 5 = 4, "", "header.from regex
(.*)(user=phone;)(.*)(.>)(;tag=)(.*)", "header.from", 2,
"$1+$2+$4+$5+$6", 0;
MessageManipulations 6 = 2, "any.response", "", "header.allow", 0,
"'UPDATE'", 0;

[ \MessageManipulations ]
```

```
[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

Reader's Notes

Configuration Note

www.audiocodes.com