

Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2013 & BT One Voice SIP Trunk using Mediant E-SBC



April 2013

Document # LTRT-12245

Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	BT One Voice SIP Trunk Version	9
2.3	Microsoft Lync Server 2013 Version	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring Lync Server 2013	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway	13
3.2	Configuring the "Route" on Lync Server 2013.....	21
4	Configuring AudioCodes E-SBC.....	29
4.1	Step 1: IP Network Interfaces Configuration	30
4.1.1	Step 1a: Configure Network Interfaces.....	31
4.2	Step 2: Enable the SBC Application	32
4.3	Step 3: Signaling Routing Domains Configuration	33
4.3.1	Step 3a: Configure Media Realms.....	33
4.3.2	Step 3b: Configure SRDs	35
4.3.3	Step 3c: Configure SIP Signaling Interfaces	36
4.4	Step 4: Configure Proxy Sets	37
4.5	Step 5: Configure IP Groups.....	39
4.6	Step 6: Configure IP Profiles	41
4.7	Step 7: Configure Coders	44
4.8	Step 8: SIP TLS Connection Configuration	46
4.8.1	Step 8a: Configure the NTP Server Address.....	46
4.8.2	Step 8b: Configure a Certificate	47
4.9	Step 9: Configure SRTP	52
4.10	Step 10: Configure Maximum IP Media Channels	53
4.11	Step 11: Configure IP-to-IP Call Routing Rules	54
4.12	Step 12: Configure IP-to-IP Manipulation Rules.....	57
4.13	Step 13: Miscellaneous Configuration.....	59
4.13.1	Step 13a: Configure Call Forking Mode	59
4.13.2	Step 13b: Configure SRTP State upon Re-key	60
4.14	Step 16: Reset the E-SBC	61
A	AudioCodes INI File	63

Reader's Notes

Notice

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

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

© Copyright 2013 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: April-02-2013

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, VolPerfect, VolPerfectHD, 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.

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 BT One Voice's SIP Trunk and Microsoft's Lync Server 2013 environment.

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.60A.0217.006
Protocol	▪ SIP/UDP (to the BT One Voice SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 BT One Voice SIP Trunk Version

Table 2-2: BT One Voice Version

Vendor/Service Provider	BT One Voice
SSW Model/Service	NOAS SIP Trunk
Software Version	NOAS SIP Trunk
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

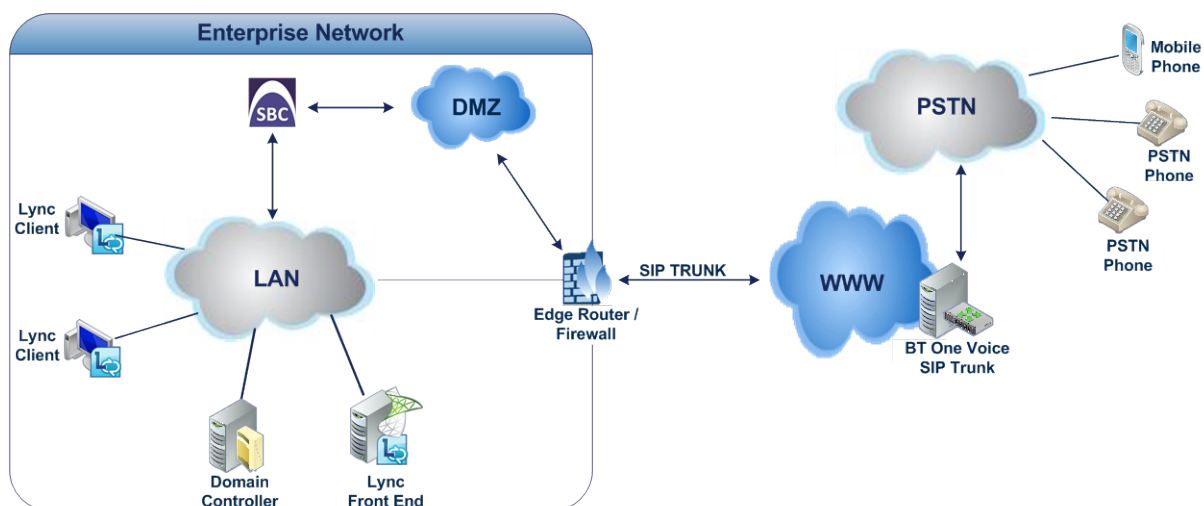
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and BT One Voice SIP Trunk with Lync 2013 was done using the following topology setup:

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

The figure below illustrates this interoperability test topology:

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



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN ▪ BT One Voice SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ BT One Voice SIP Trunk operates with SIP-over-UDP transport type or SIP over TCP this can be specified when ordering.
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ BT One Voice SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ BT One Voice SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and BT One Voice's SIP Trunk.

Reader's Notes

3 Configuring Lync Server 2013

This chapter describes how to configure Microsoft Lync Server 2013 to operate with AudioCodes E-SBC.



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

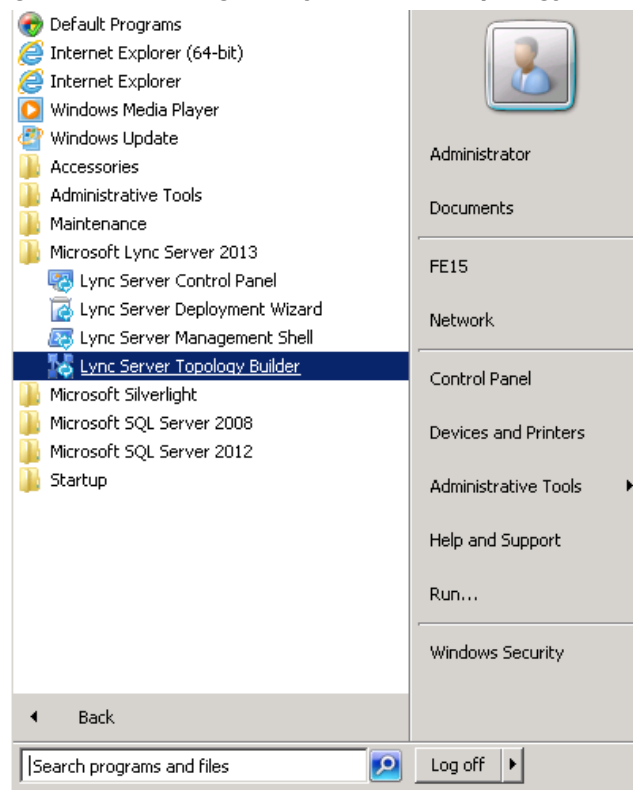
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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:**

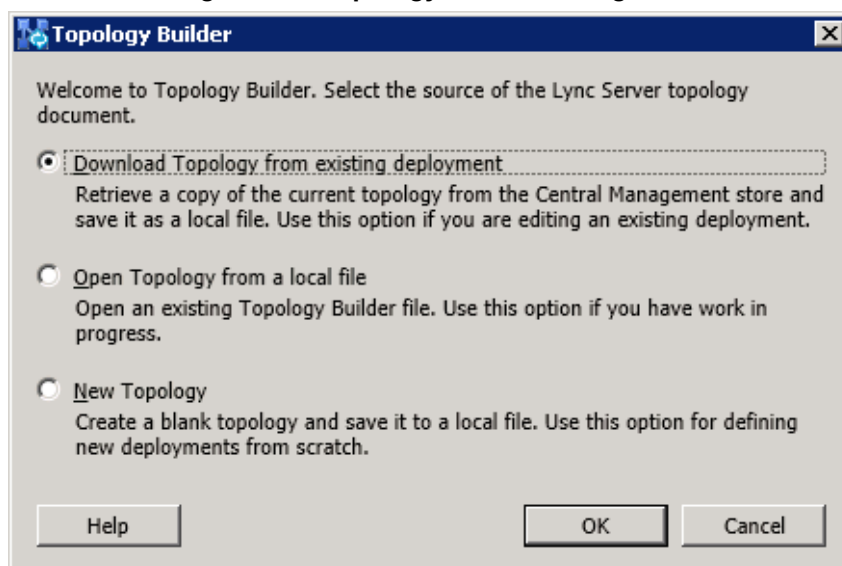
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



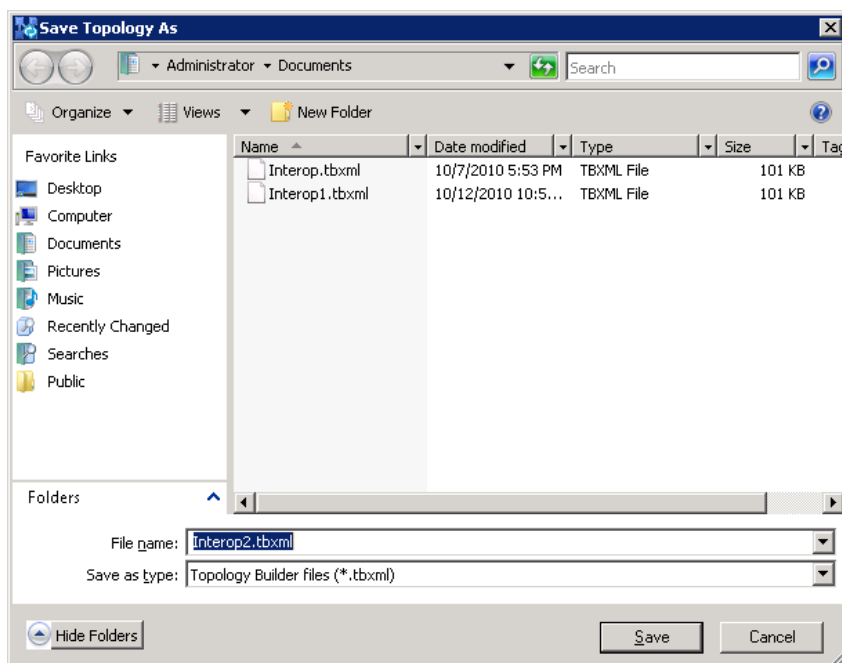
The following screen is displayed:

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:

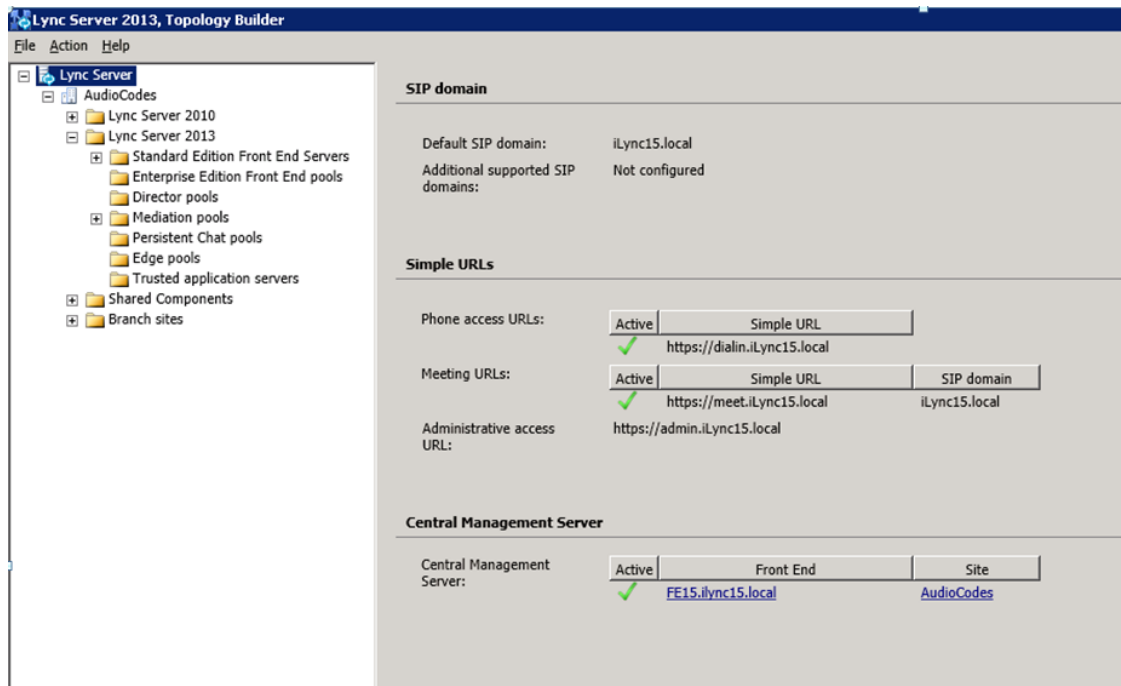
Figure 3-3: Save Topology Dialog Box



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.

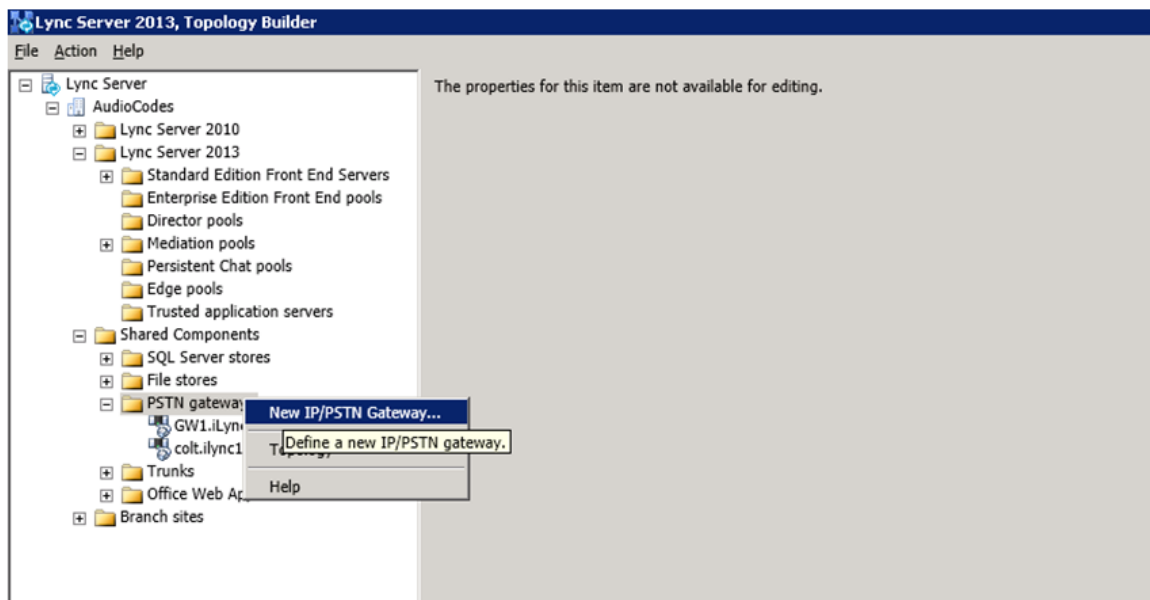
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



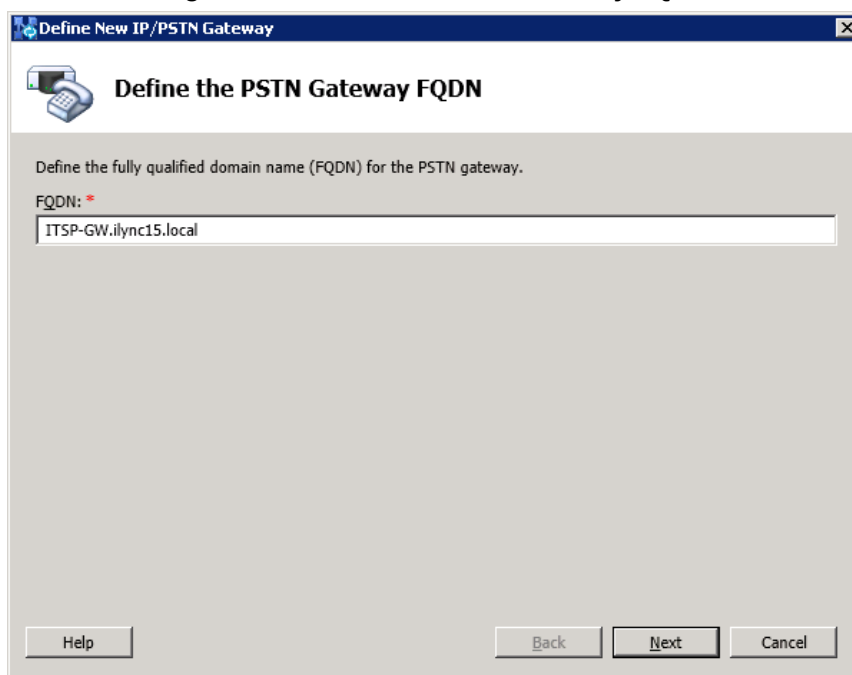
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following screen is displayed:

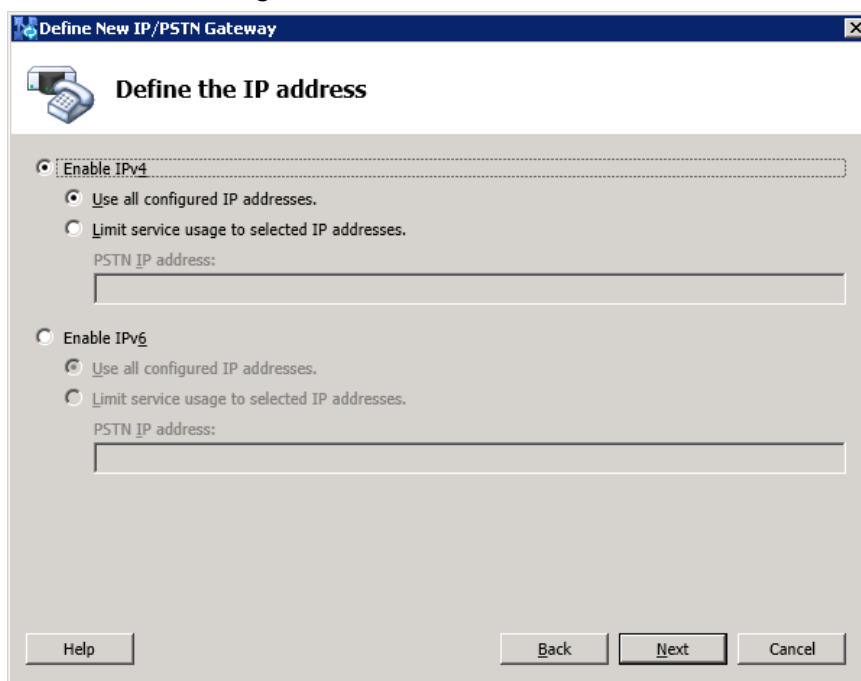
Figure 3-6: Define the PSTN Gateway FQDN



The screenshot shows a window titled "Define New IP/PSTN Gateway" with a sub-header "Define the PSTN Gateway FQDN". Below the sub-header is a text box labeled "FQDN: *" containing the text "ITSP-GW.ilync15.local". At the bottom of the window are three buttons: "Help", "Back", and "Next", and a "Cancel" button.

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



The screenshot shows a window titled "Define New IP/PSTN Gateway" with a sub-header "Define the IP address". Below the sub-header are two radio button options: "Enable IPv4" (selected) and "Enable IPv6". Each option has two sub-options: "Use all configured IP addresses." and "Limit service usage to selected IP addresses.". Below each sub-option is a text box labeled "PSTN IP address:". At the bottom of the window are three buttons: "Help", "Back", and "Next", and a "Cancel" button.

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

Define the root trunk

Trunk name: *
ITSP-GW.ilync15.local

Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
FE15.ilync15.local AudioCodes

Associated Mediation Server port: *
5067

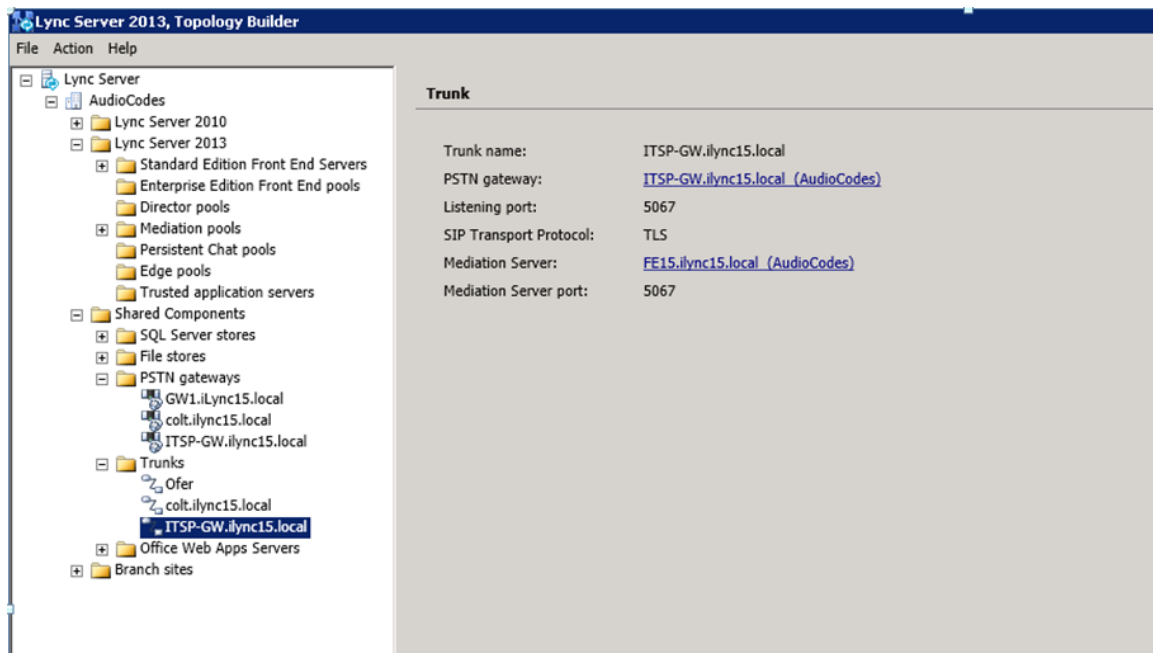
Help Back Finish Cancel

Define the following parameters:

- 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**).
- In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses.
- In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
- 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**).
- Click **Finish**.

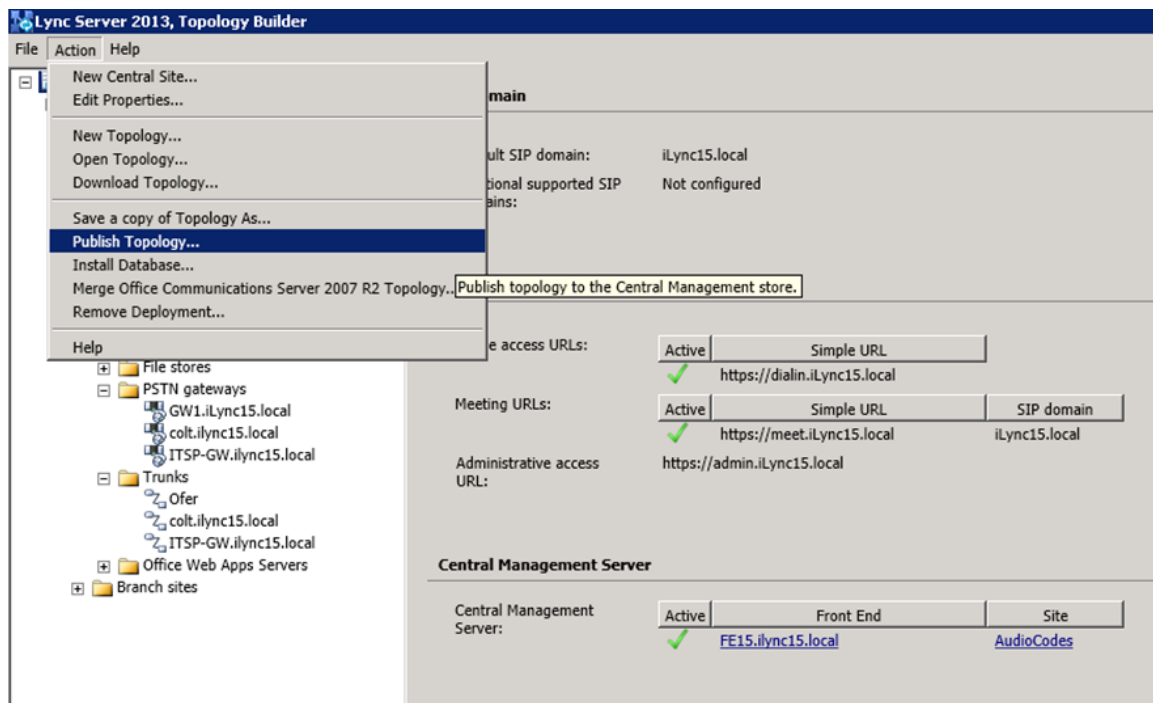
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



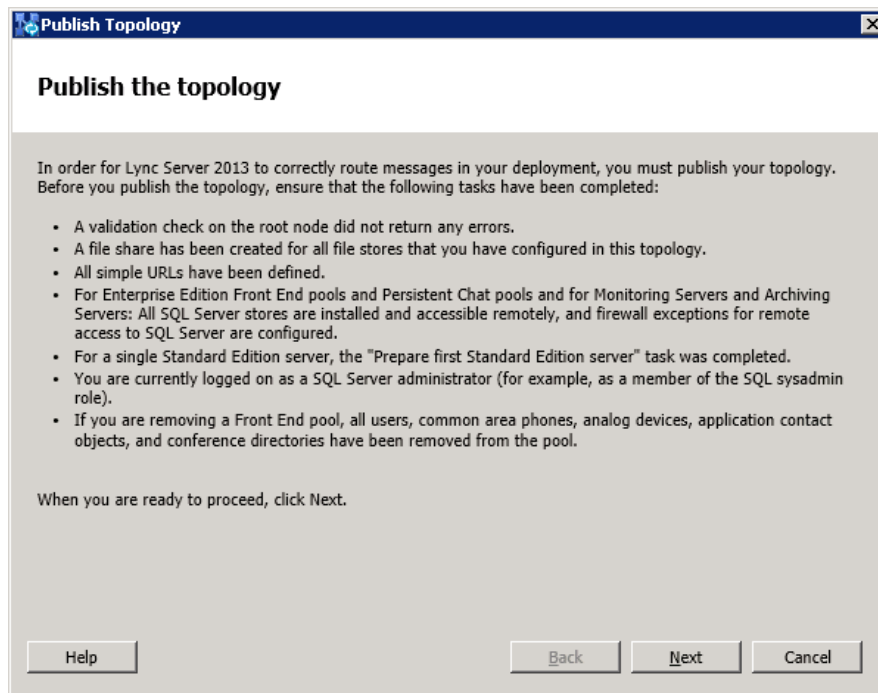
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



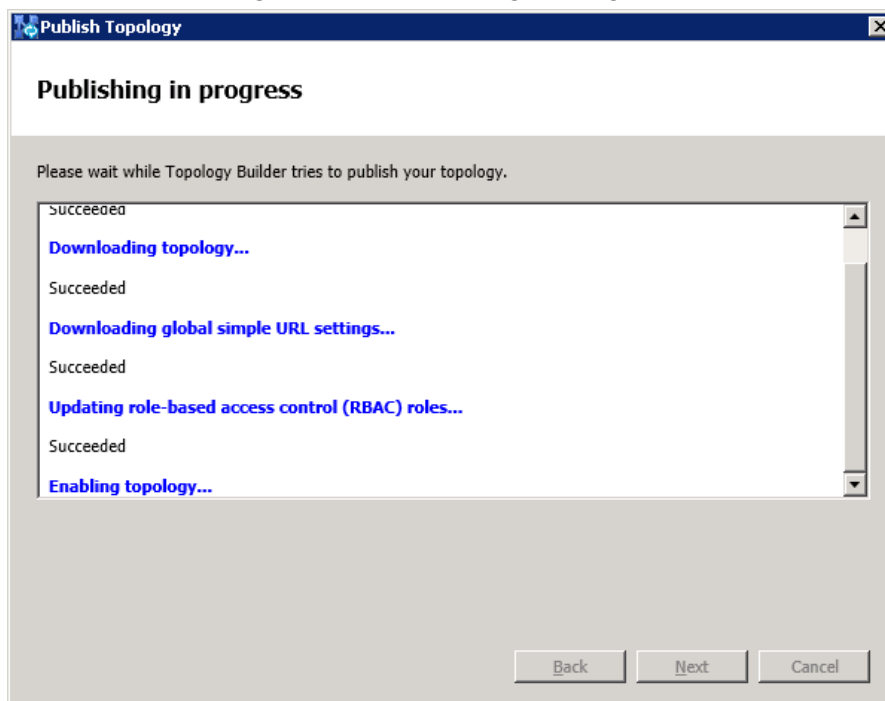
The following screen is displayed:

Figure 3-11: Publish the Topology



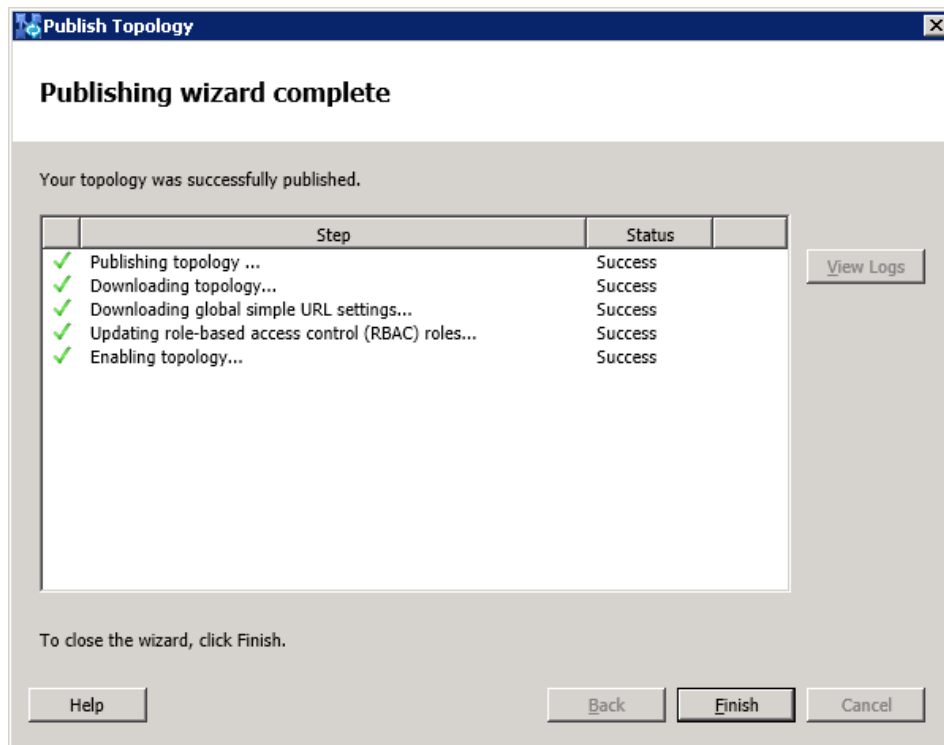
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

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**.

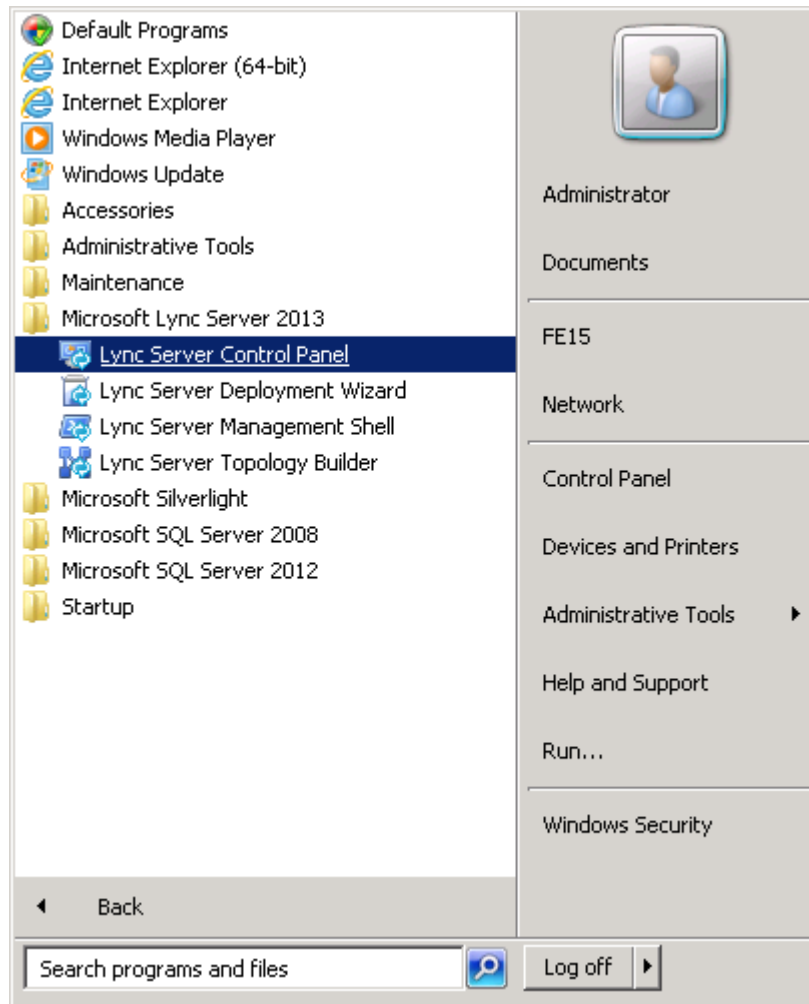
3.2 Configuring the "Route" on Lync Server 2013

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:**

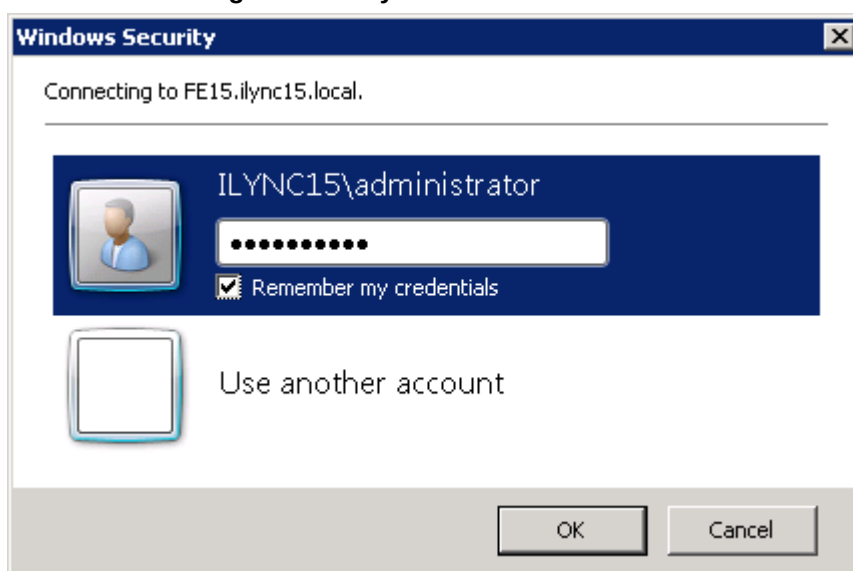
1. Start the Microsoft Lync Server 2013 Control Panel (**Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel



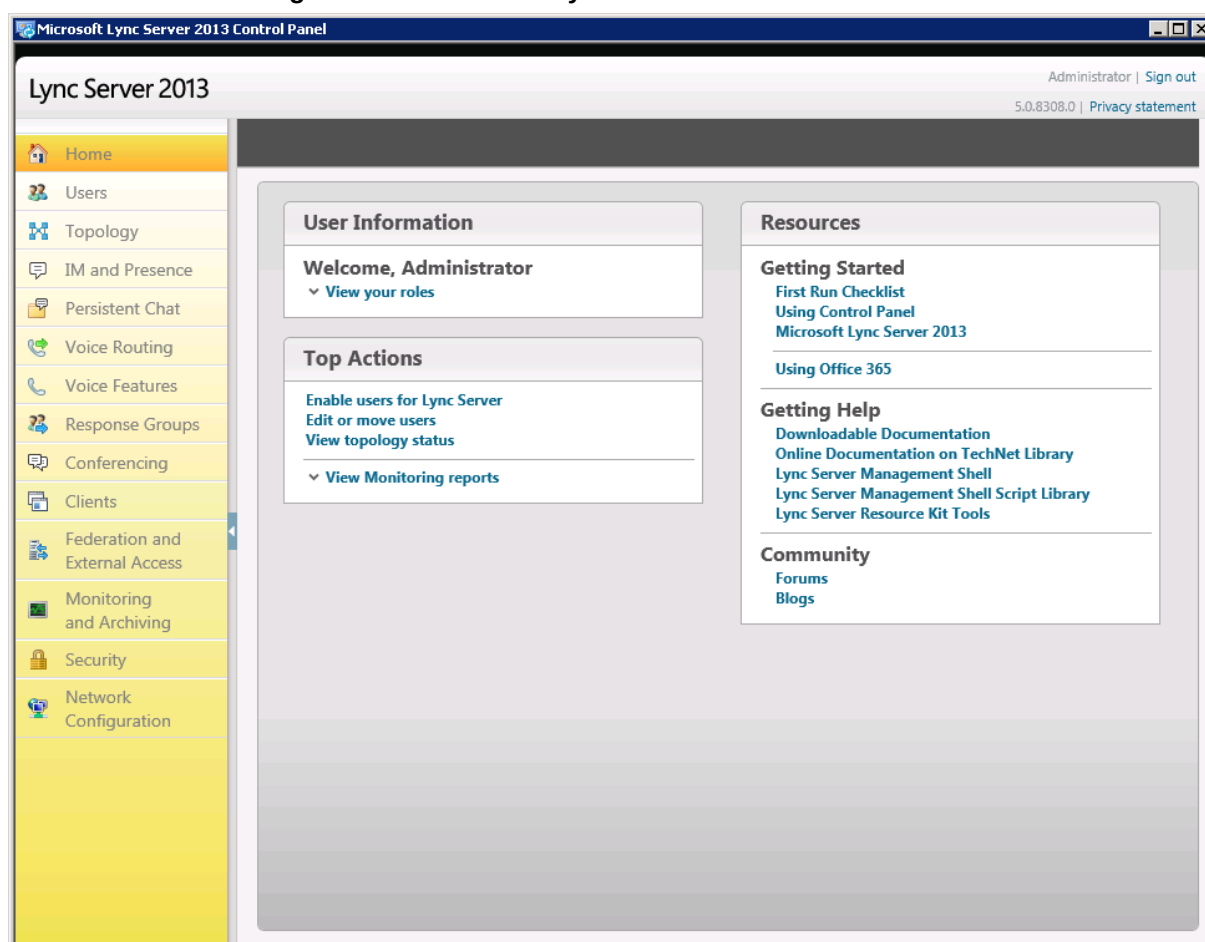
You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



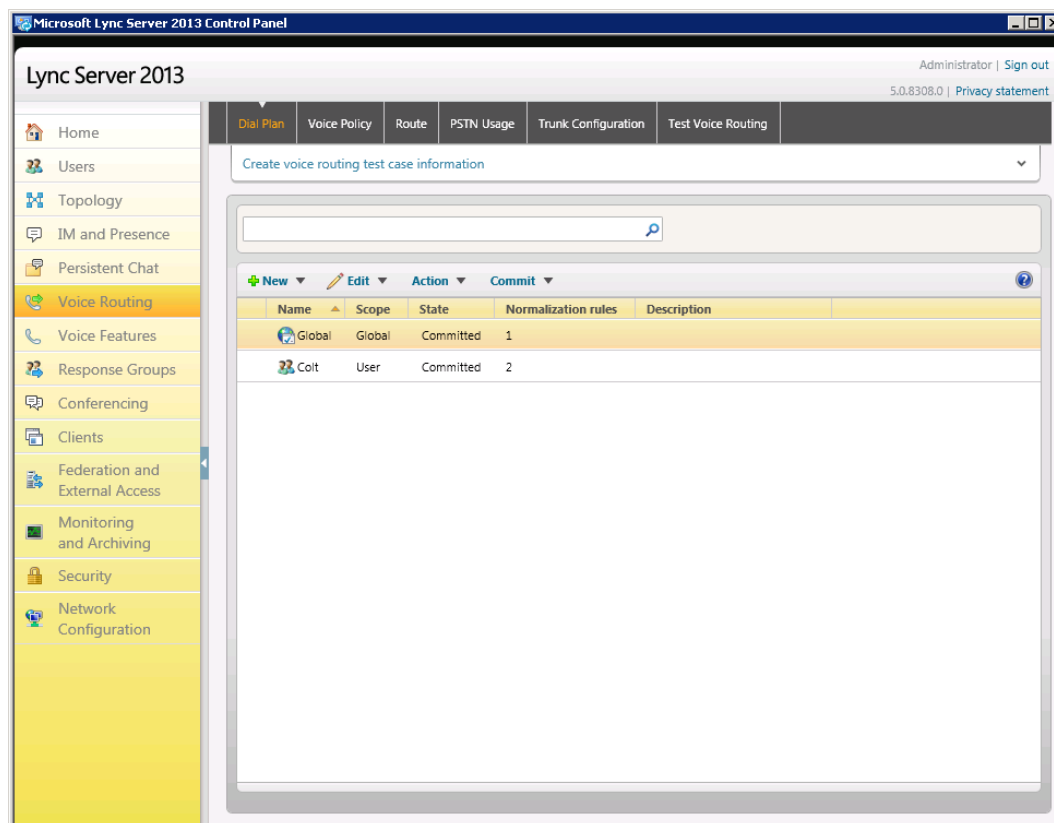
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



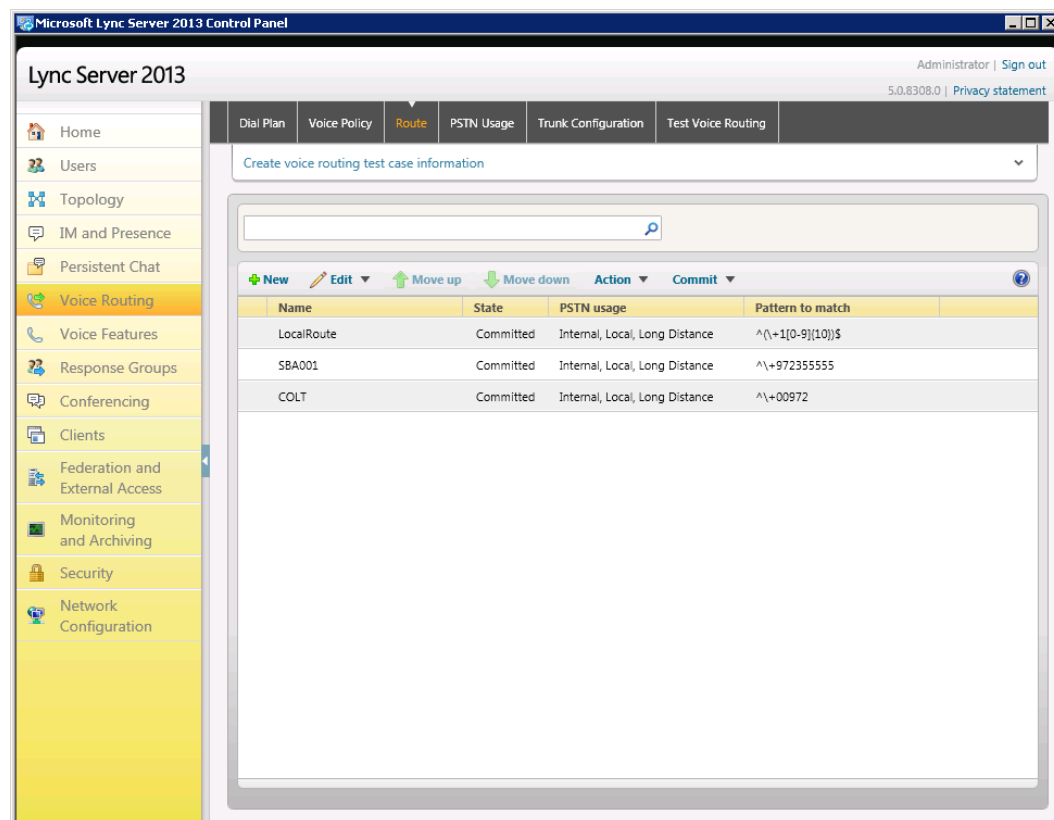
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



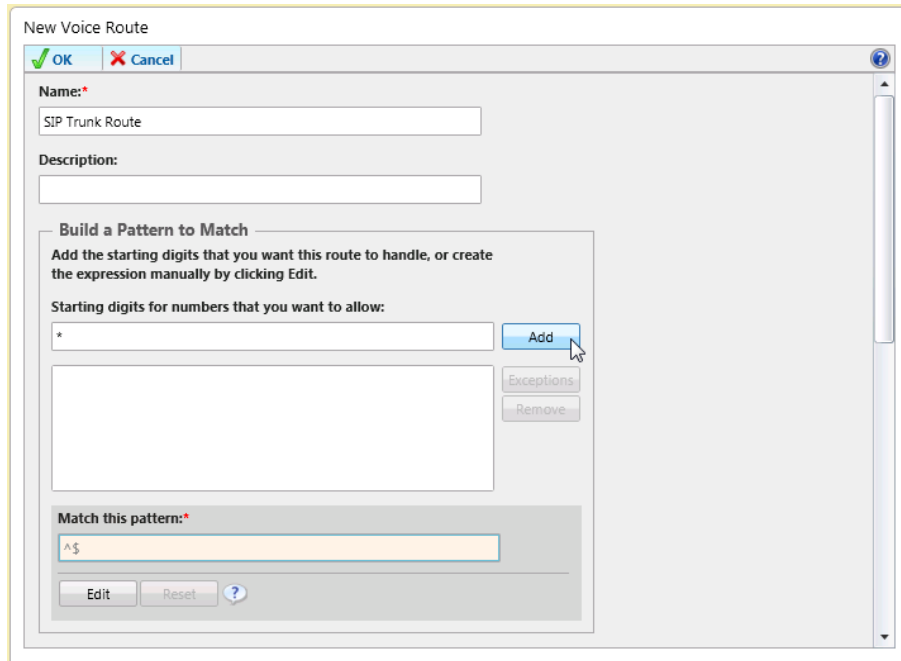
4. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



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

Figure 3-19: Adding New Voice Route



New Voice Route

OK Cancel

Name:*

SIP Trunk Route

Description:

Build a Pattern to Match

Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

Starting digits for numbers that you want to allow:

* Add

Exceptions

Remove

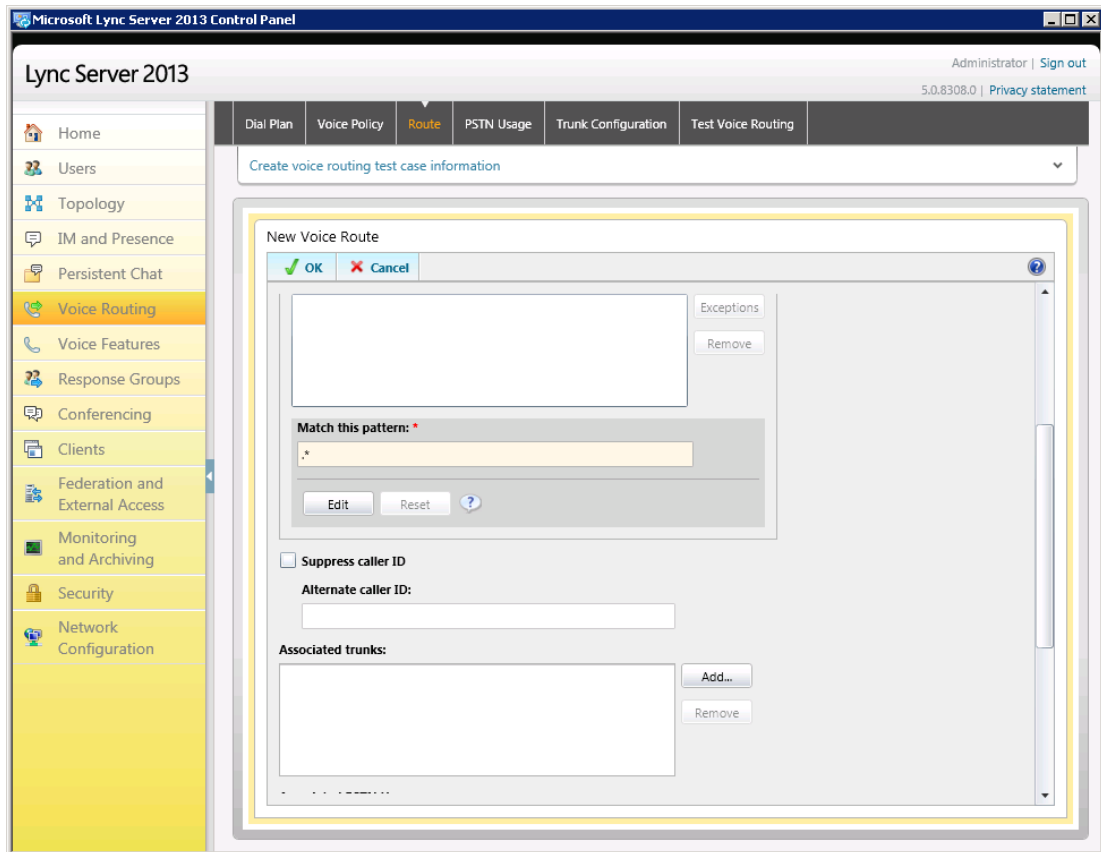
Match this pattern:*

^\$

Edit Reset ?

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



Microsoft Lync Server 2013 Control Panel

Lync Server 2013

Administrator | Sign out

5.0.8308.0 | Privacy statement

Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing

Create voice routing test case information

New Voice Route

OK Cancel

Exceptions

Remove

Match this pattern: *

* Edit Reset ?

Suppress caller ID

Alternate caller ID:

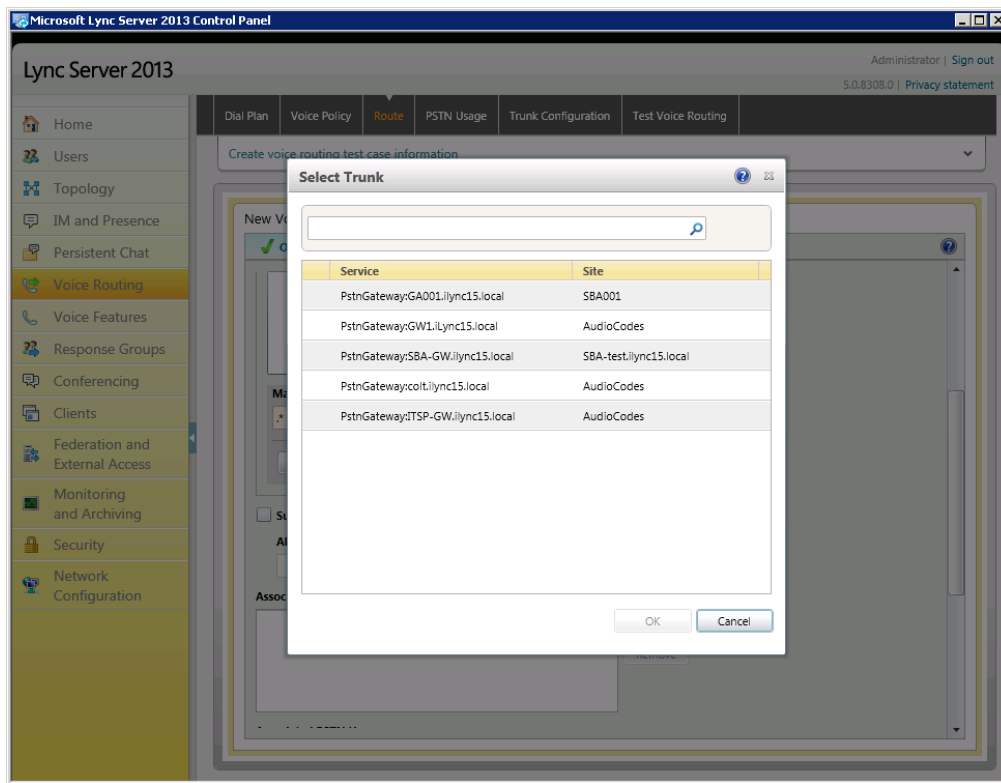
Associated trunks:

Add...

Remove

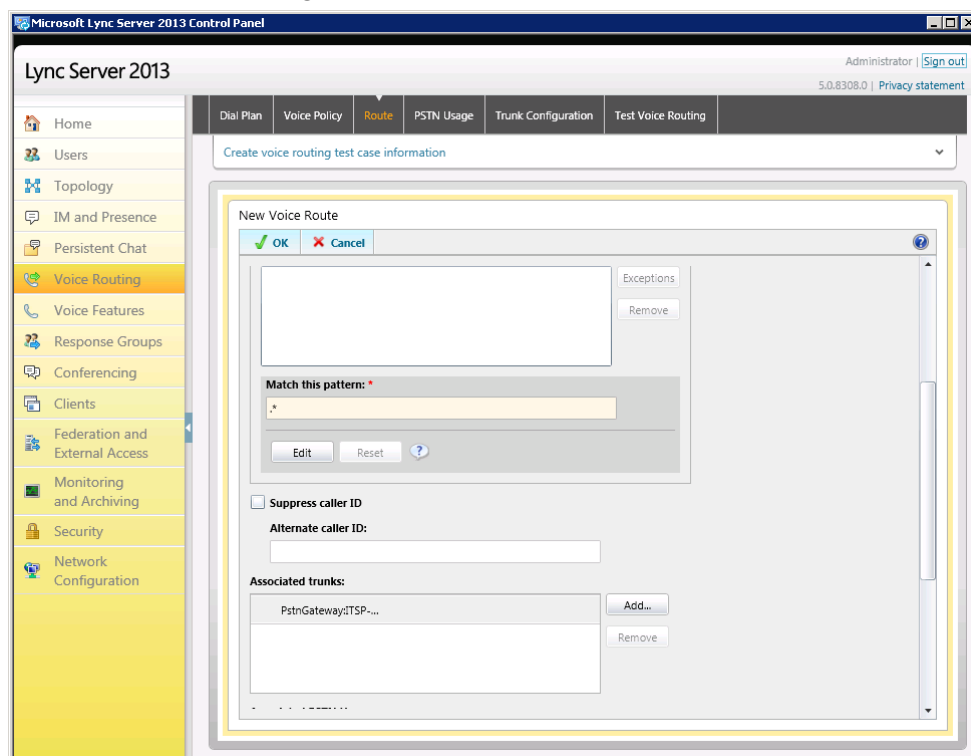
8. Associate the route with the E-SBC Trunk that you created:
 - a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



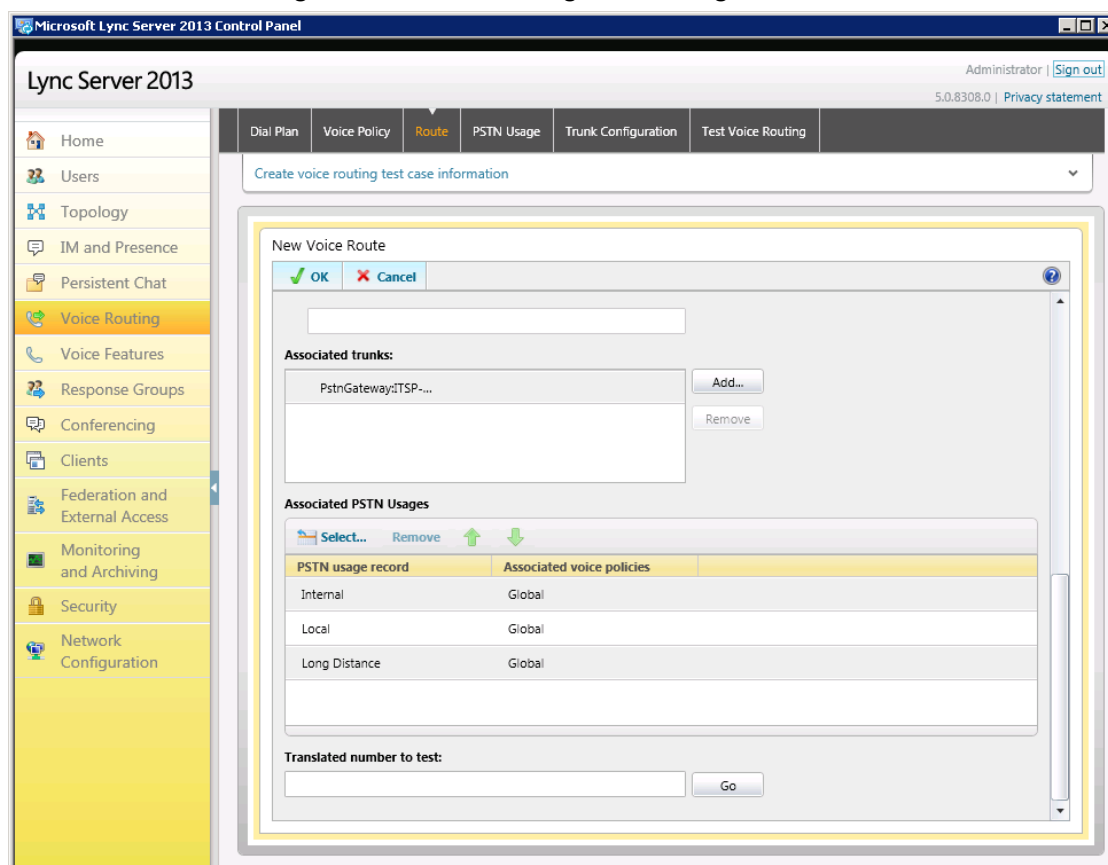
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



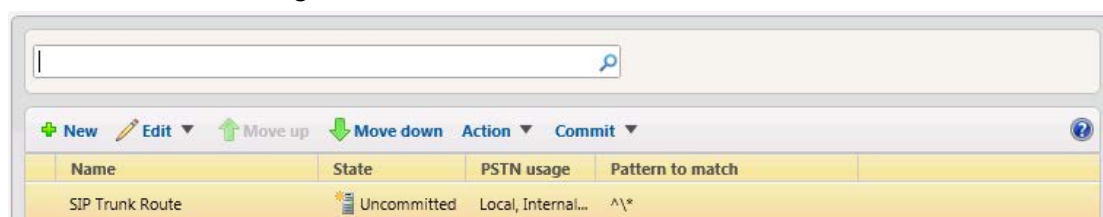
9. Associate a PSTN Usage to this route:
 - a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



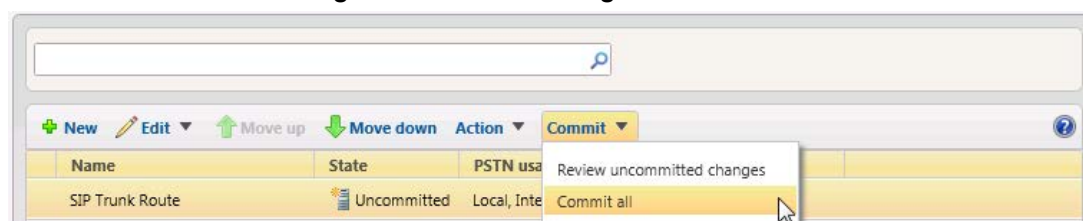
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



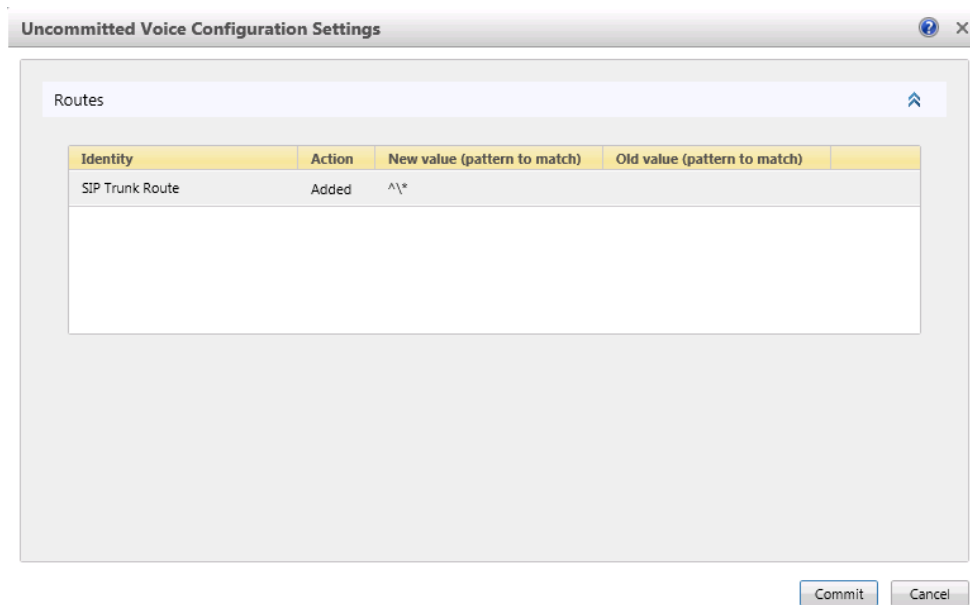
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



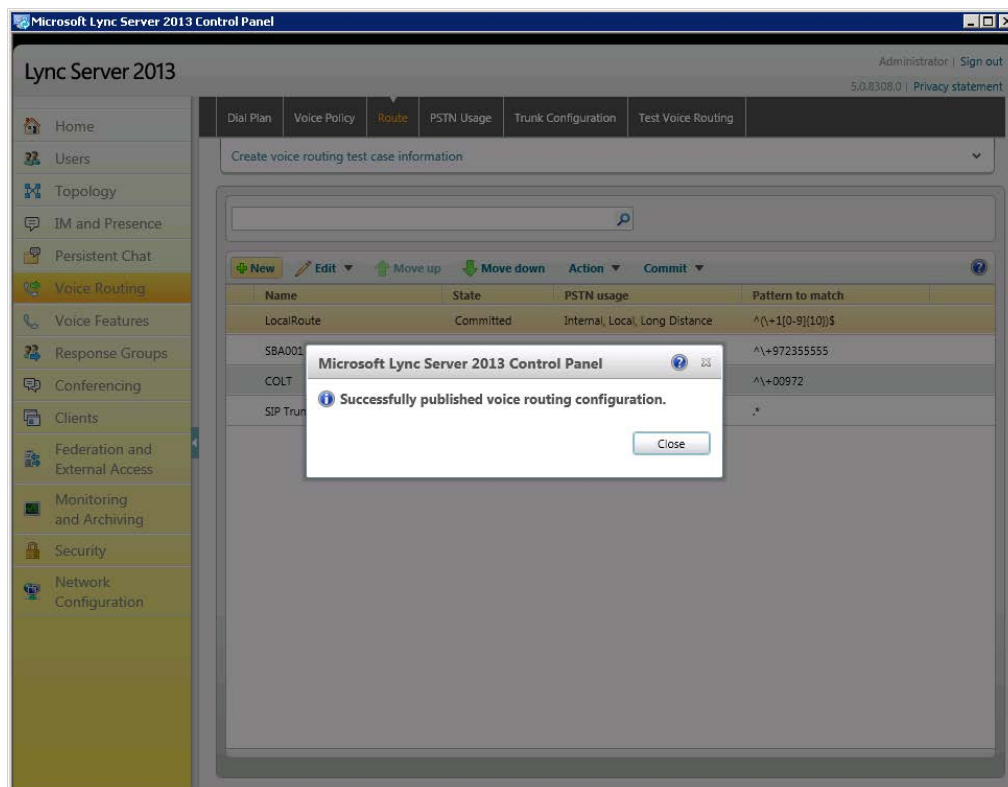
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



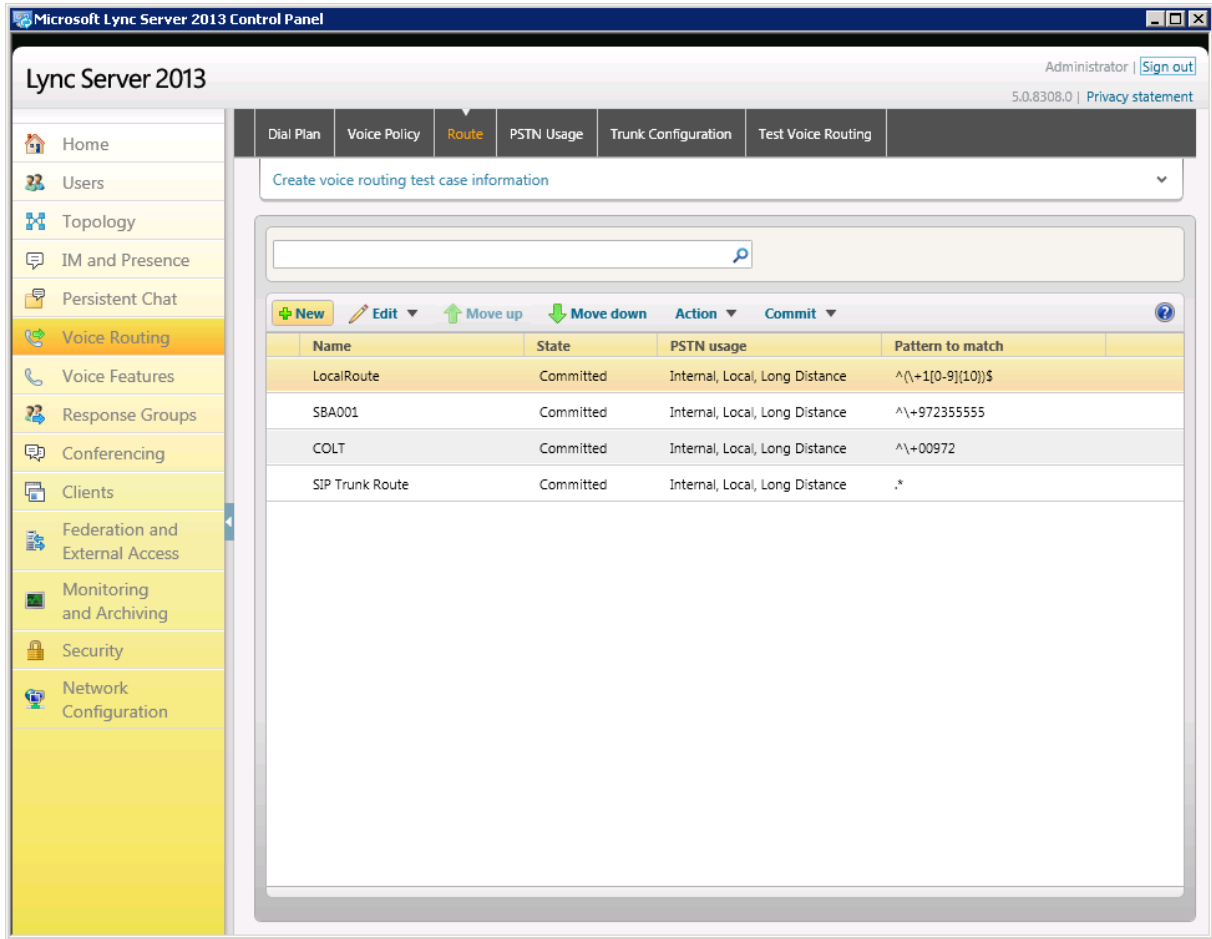
- Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

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



The screenshot shows the Microsoft Lync Server 2013 Control Panel interface. The left sidebar contains navigation links: Home, Users, Topology, IM and Presence, Persistent Chat, **Voice Routing** (highlighted), Voice Features, Response Groups, Conferencing, Clients, Federation and External Access, Monitoring and Archiving, Security, and Network Configuration. The main content area is titled 'Lync Server 2013' and includes a top navigation bar with tabs: Dial Plan, Voice Policy, **Route** (selected), PSTN Usage, Trunk Configuration, and Test Voice Routing. Below the tabs is a search bar and a 'Create voice routing test case information' dropdown. The main area displays a table of committed routes with the following data:

Name	State	PSTN usage	Pattern to match
LocalRoute	Committed	Internal, Local, Long Distance	^\+1[0-9]{10}\$
SBA001	Committed	Internal, Local, Long Distance	^\+972355555
COLT	Committed	Internal, Local, Long Distance	^\+00972
SIP Trunk Route	Committed	Internal, Local, Long Distance	.*

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the BT One Voice SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

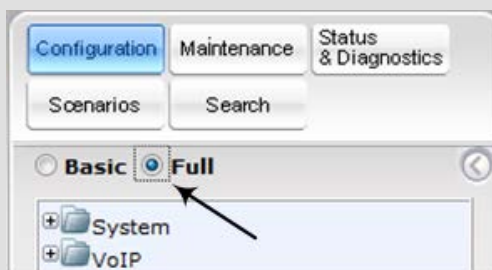
- E-SBC WAN interface - BT One Voice SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

- For implementing Microsoft Lync and BT One Voice SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
 - ✓ Microsoft
 - ✓ SBC
 - ✓ Security
 - ✓ DSP
 - ✓ RTP
 - ✓ SIP

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



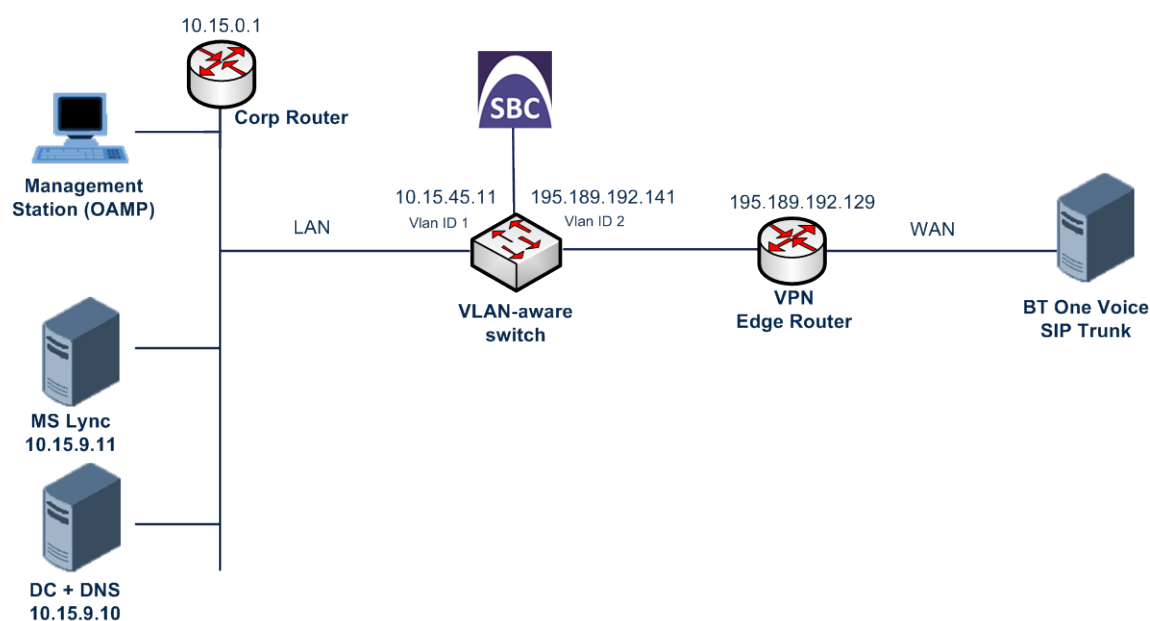
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

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

- E-SBC interfaces with the following IP entities:
 - Lync servers, located on the LAN
 - BT One Voice SIP Trunk, located on the WAN
- The E-SBC connects to the WAN through a CPE Router.
- 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, the SBC connects to the LAN and WAN using a **single** LAN port, physically connected to a VLAN-aware switch, where the E-SBC uses two logical network interfaces; one to the LAN (e.g., VLAN ID 1) and another to the WAN (e.g., VLAN ID 2).

Figure 4-1: Network Interfaces in Interoperability Test Topology



Note: It is also possible to configure physical interface separation (using separate physical ports); however the use of VLAN separation with a single LAN port is recommended by BT.

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 "BTSIP")

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

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

Parameter	Value
IP Address	10.15.45.11 (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	10.15.9.10
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	195.189.192.141 (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	BTSIP
Primary DNS Server IP Address	80.179.52.100
Secondary DNS Server IP Address	80.179.55.100
Underlying Interface	GROUP_1 (same port group as above)

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										
Note: Select row index to modify the relevant row										
1	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	QAMP + Media + Control	IPv4 Manual	10.15.45.101	16	10.15.0.1	1	Voice	10.15.0.10	0.0.0.0	GROUP_1
1	Media + Control	IPv4 Manual	195.189.192.141	25	195.189.192.129	2	BT SIP	90.179.52.100	90.179.55.100	GROUP_1

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 4-3: 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 this setting to take effect (see Section 4.14 on page 61).

4.3 Step 3: Signaling Routing Domains Configuration

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

The SRD is composed of the following:

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

4.3.1 Step 3a: Configure Media Realms

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

➤ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **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)

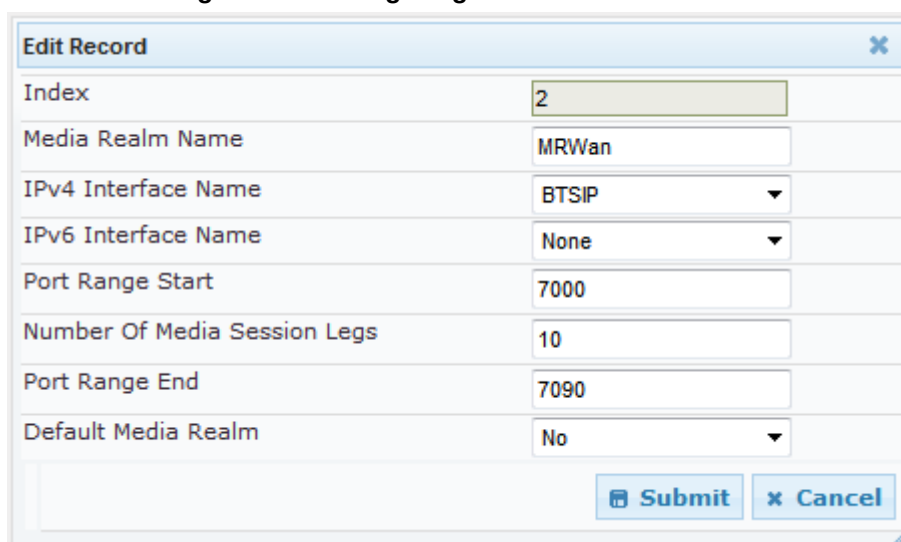
Figure 4-4: Configuring Media Realm for LAN

Add Record	
Index	1
Media Realm Name	MRLan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	10
Port Range End	6090
Default Media Realm	Yes
Submit Cancel	

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	2
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	BTSIP
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)

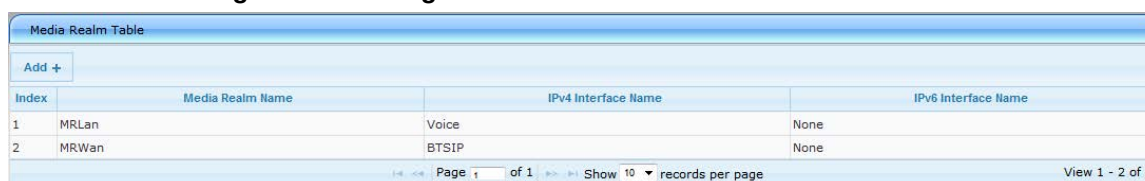
Figure 4-5: Configuring Media Realm for WAN



Edit Record	
Index	2
Media Realm Name	MRWan
IPv4 Interface Name	BTSIP
IPv6 Interface Name	None
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	7090
Default Media Realm	No
Submit Cancel	

The configured Media Realms are shown in the figure below:

Figure 4-6: Configured Media Realms in Media Realm Table



Media Realm Table			
Add +			
Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
1	MRLan	Voice	None
2	MRWan	BTSIP	None

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

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 4-7: Configuring LAN SRD

▼

SRD Index 1 - SRDLan ▼

▼ Common Parameters

SRD Name SRDLan

Media Realm MRLan

▲ SBC Parameters

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

Parameter	Value
SRD Index	2
SRD Name	SRDWan
Media Realm	MRWan

Figure 4-8: Configuring WAN SRD

▼

SRD Index 2 - SRDWan ▼

▼ Common Parameters

SRD Name SRDWan

Media Realm MRWan

▲ SBC Parameters

4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➤ **To configure SIP Interfaces:**

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

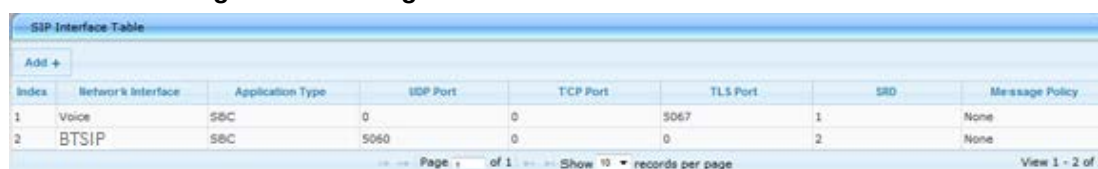
Parameter	Value
Index	1
Network Interface	Voice
Application Type	SBC
TLS Port	5067
TCP and UDP	0
SRD	1

3. Configure a SIP interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

Figure 4-9: Configured SIP Interfaces in SIP Interface Table



Index	Network's Interface	Application Type	SDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	0	0	5067	1	None
2	BTSIP	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 need to be configured for the following IP entities:

- Microsoft Lync Server 2013
- BT One Voice 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 4-10: Configuring Proxy Set for Microsoft Lync Server 2013

Proxy Set ID

1

	Proxy Address	Transport Type
1	FE15.ilync15.local:5067	TLS
2		
3		
4		
5		

Enable Proxy Keep Alive

Using Options

Proxy Keep Alive Time

60

Proxy Load Balancing Method

Round Robin

Is Proxy Hot Swap

Yes

Proxy Redundancy Mode

Not Configured

⚡ SRD Index

1

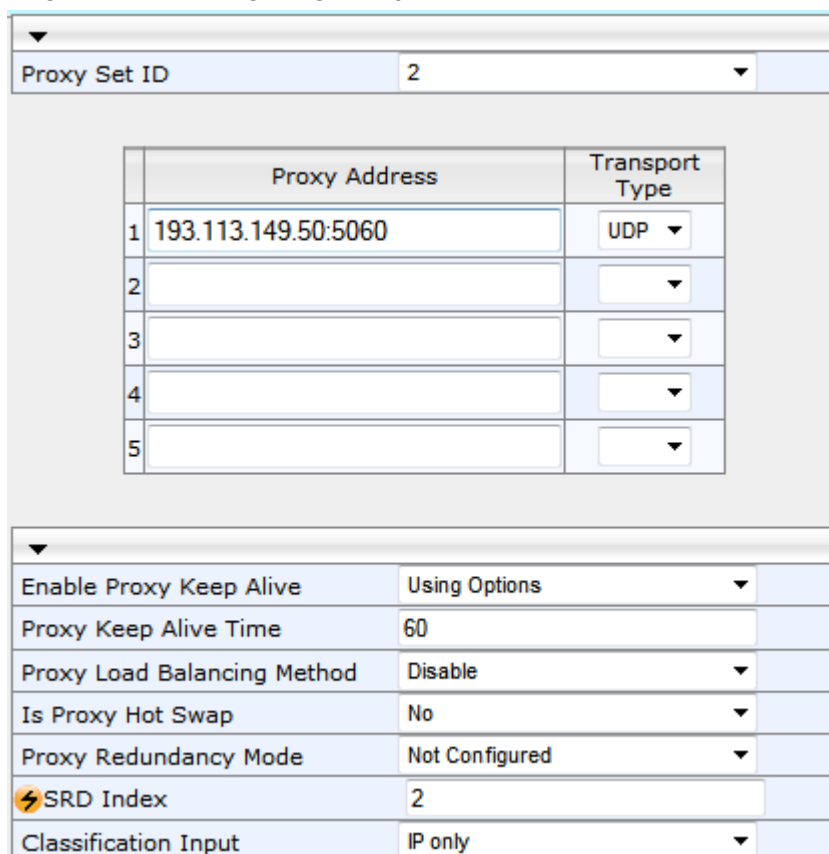
Classification Input

IP only

3. Configure a Proxy Set for the BT One Voice SIP Trunk:

Parameter	Value
Proxy Set ID	2
Proxy Address	193.113.149.50:5060 (BT One Voice IP address / FQDN and destination port)
Transport Type	UDP
Enable Proxy Keep Alive	Using Options
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to BT One Voice SIP Trunk)

Figure 4-11: Configuring Proxy Set for BT One Voice SIP Trunk



	Proxy Address	Transport Type
1	193.113.149.50:5060	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	2
Classification Input	IP only

4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.14 on page 61).

4.5 Step 5: Configure IP Groups

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

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

- Lync Server 2013 (Mediation Server) located on LAN
- BT One Voice 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
SRD	1
Media Realm Name	MRLan
IP Profile ID	1

3. Configure an IP Group for the BT One Voice SIP Trunk:

Parameter	Value
Index	2
Type	Server
Description	BT One Voice (arbitrary descriptive name)
Proxy Set ID	2
SRD	2
Media Realm Name	MRWan
IP Profile ID	2

The configured IP Groups are shown in the figure below:

Figure 4-12: 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 Profile ID
1	Server	Lync	1				1	MRLan	1
2	Server	BT One Voice	2				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 this interoperability test topology, IP Profiles need to be configured for the following IP entities:

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



Note: The IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 39).

➤ **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
Extension Coders Group ID	Coders Group 1
Media Security Behavior	SRTP
SBC Remote Early Media RTP	Delayed (required, as Lync Server 2013 does not send RTP immediately to 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 Lync Server 2013 does not support receipt of SIP REFER)
SBC Remote 3xx Behavior	Handle Locally (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
SBC Remote Delayed Offer Support	Not Supported
SBC PRACK mode	Optional (required, the E-SBC performs the PRACK process on behalf of the Sip Trunk. "Supported:100rel" header is required to enable receiving Early Media from the Lync side)
SBC Remote Hold Format	Inactive (required, as when SIP Trunk sends a SIP 200 response, it does not send attributes (e.g., a=inactive), the E-SBC will add one on behalf of the Sip Trunk)

Figure 4-13: Configuring IP Profile for Lync Server 2013

Profile ID	1	
Profile Name	Lync	
SBC		
Transcoding Mode	Only if Required	
Extension Coders Group ID	Coders Group 1	
Allowed Coders Group ID	None	
Allowed Coders Mode	Restriction	
Diversion Mode	Don't Care	
History Info Mode	Don't Care	
Media Security Behavior	SRTP	
RFC 2833 Behavior	As Is	
Alternative DTMF Method	Don't Care	
P-Asserted-Identity	Don't Care	
SBC Fax Coders Group ID	None	
SBC Fax Behavior	0	
SBC Fax Offer Mode	0	
SBC Fax Answer Mode	1	
SBC Session Expires Mode	Transparent	
SBC Remote Early Media RTP	Delayed	
SBC Remote Can Play Ringback	Yes	
SBC Remote Supports RFC 3960	Not Supported	
SBC Multiple 18x Support	supported	
SBC Early Media Response Type	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	Optional	
SBC Enforce MKI Size	do-not-enforce	
SBC User Registration Time	-1	
SBC Remote Hold Format	inactive	

3. Configure an IP Profile for the BT One Voice SIP Trunk:

Parameter	Value
Profile ID	2
Transcoding Mode	Force (required, as Lync Server 2013 does not send RTP packets when negotiated coder is G.711)
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer) Restrict (enables the received SDP offer to list Allowed coders only) (e.g., only G.729)
Media Security Behavior	RTP
SBC Remote Refer Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)

Figure 4-14: Configuring IP Profile for BT One Voice SIP Trunk

▼	
Profile ID	2 ▼
Profile Name	BT Onevoice
▼ SBC	
Transcoding Mode	Force ▼ 
Extension Coders Group ID	Coders Group 2 ▼ 
Allowed Coders Group ID	Coders Group 2 ▼ 
Allowed Coders Mode	Preference ▼ 
Diversion Mode	Don't Care ▼
History Info Mode	Don't Care ▼
Media Security Behavior	RTP ▼ 
RFC 2833 Behavior	As Is ▼
Alternative DTMF Method	Don't Care ▼
P-Asserted-Identity	Don't Care ▼
SBC Fax Coders Group ID	None ▼
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent ▼
SBC Remote Early Media RTP	Immediate ▼
SBC Remote Can Play Ringback	Yes ▼
SBC Remote Supports RFC 3960	Not Supported ▼

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 BT One Voice 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 BT One Voice SIP Trunk.

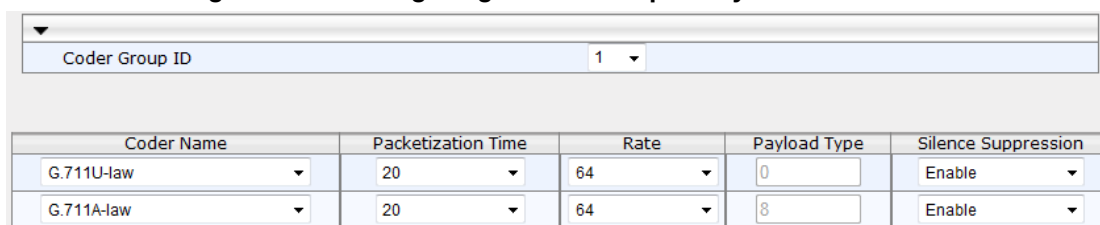
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 41).

➤ **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 4-15: Configuring Coder Group for Lync Server 2013

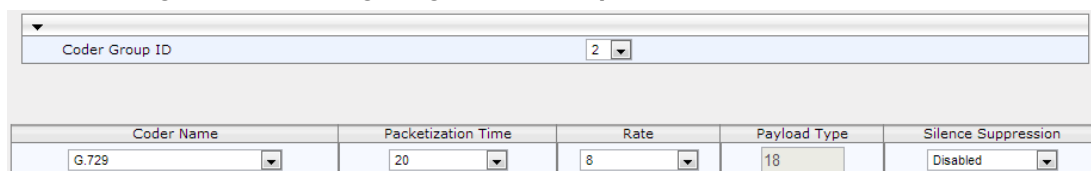


Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-law	20	64	0	Enable
G.711A-law	20	64	8	Enable

3. Configure a Coder Group for BT One Voice SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	G.729

Figure 4-16: Configuring Coder Group for BT One Voice SIP Trunk



Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729	20	8	18	Disabled

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the BT One Voice SIP Trunk uses the G.729 codec whenever possible. Note that this Allowed Coders Group ID (and its preference) was assigned to the IP Profile belonging to the BT One Voice SIP Trunk in the previous step (see Section 4.6 on page 41). BT One Voice will select the higher bandwidth codecs when available. The preferred bandwidth is determined by the purchased bandwidth.

➤ **To set a preferred coder for the BT One Voice 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 4-17: Configuring Allowed Coders Group for BT One Voice SIP Trunk

➤ **To set the preferred coder as the first coder offered :**

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

Figure 4-18: SBC Preferences Mode

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

4.8 Step 8: SIP TLS Connection Configuration

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.

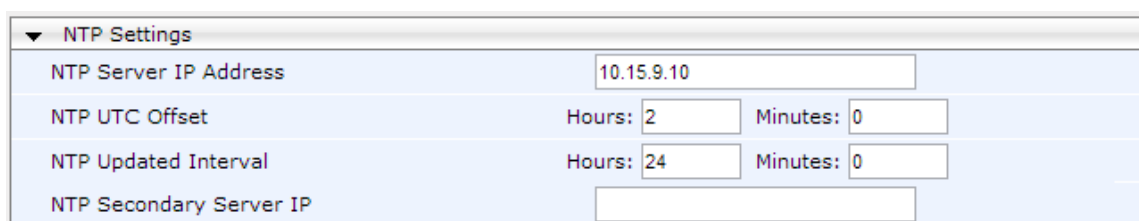
4.8.1 Step 8a: Configure the NTP Server Address

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., **10.15.9.10**).

Figure 4-19: Configuring NTP Server Address



NTP Settings			
NTP Server IP Address	10.15.9.10		
NTP UTC Offset	Hours: 2	Minutes: 0	
NTP Updated Interval	Hours: 24	Minutes: 0	
NTP Secondary Server IP			

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 the following main steps:

- a. Generating a Certificate Signing Request (CSR).
- b. Requesting Device Certificate from CA.
- c. Obtaining Trusted Root Certificate from CA.
- d. Deploying Device and Trusted Root Certificates on E-SBC.

➤ **To configure a certificate:**

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

Figure 4-20: Certificates Page - Creating CSR

▼ Certificate Signing Request

Subject Name [CN]

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLmlseW5jMTUubG9jYWwz8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCKxytgT2W1vz0NGUstypa7w2DKKkxr8x8A9sGLXwy0ZCyB49U1pDF
DJV8IldUfT8qL9d9V64f3z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBqQBLqe880JGrmEzFu5Q1
pRGiOuEQ4Pr6PL+JKghii6UpLmHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y
8z8hOCZXV/E4MrR2s8bYb6bqxeteAXs+VwxgKObb4pSFfGLc82+dZUcODAB0wZFv
nxSEcPACKnZittF/GgW+A4AoMQ==
-----END CERTIFICATE REQUEST-----
```

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

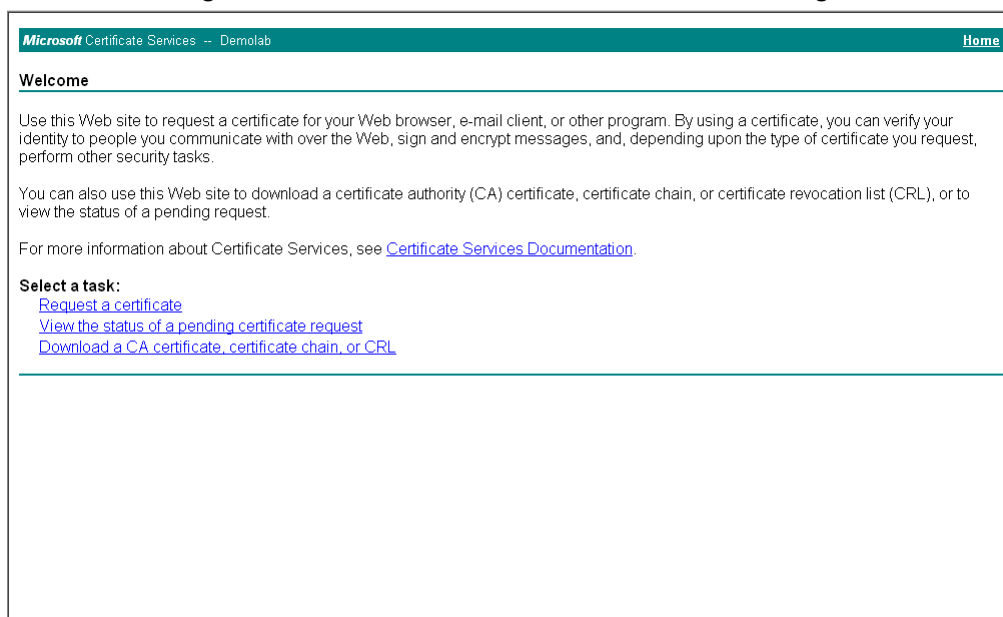


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).

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*.

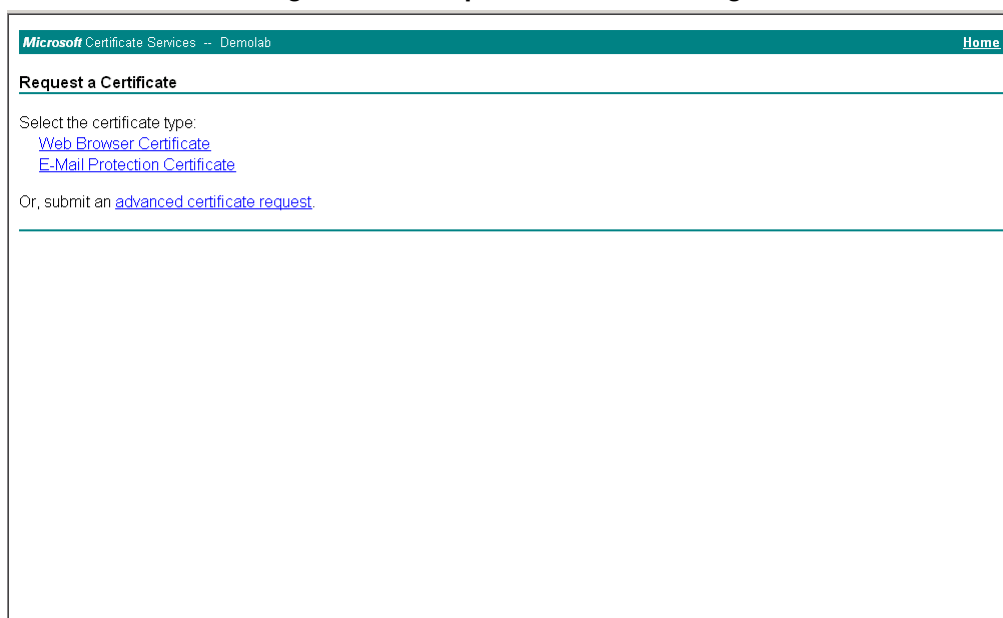
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-21: Microsoft Certificate Services Web Page



6. Click **Request a certificate**.

Figure 4-22: Request a Certificate Page



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

Figure 4-23: Advanced Certificate Request Page

Microsoft Certificate Services -- Demolab [Home](#)

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

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

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

Microsoft Active Directory Certificate Services -- Lync-DC-LYNC-CA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

λ8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxvyKt1
rr4ootrnsPOCAvEAAaAAHAOGCSqGSIb3DQEBBAUA
HnkHAKx8xHq9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj8ib+R5+YI+Ost57xT9DZXNg5Yp4G+OB
vnQuXOUUX6BeVBT71aO83HcA
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

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

Figure 4-25: Certificate Issued Page

Certificate Issued

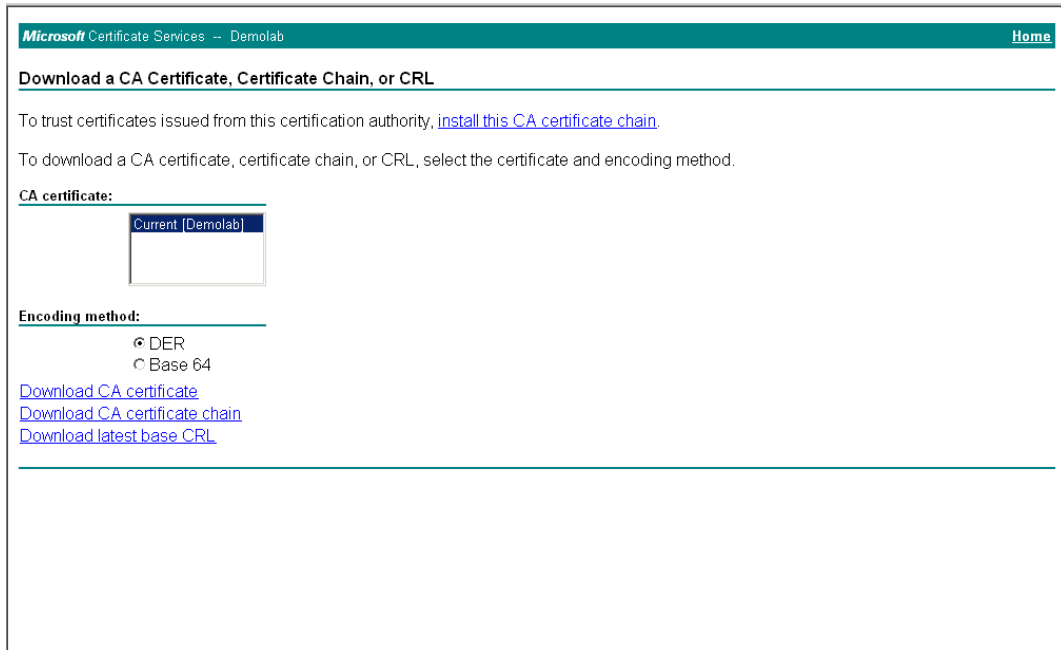
The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

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



Microsoft Certificate Services -- Demolab [Home](#)

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate chain](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Demolab]

Encoding method:

☒ DER
☐ Base 64

[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)

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 4-27: Certificates Page (Uploading Certificate)

The screenshot shows a web interface titled "Upload certificate files from your computer". It contains three main sections for uploading certificates:

- Private key pass-phrase (optional):** A text input field containing "audc".
- Send Private Key file from your computer to the device:** A section with instructions "The file must be in either PEM or PFX (PKCS#12) format." and buttons for "Browse..." and "Send File".
- Send Device Certificate file from your computer to the device:** A section with instructions "The file must be in textual PEM format." and buttons for "Browse..." and "Send File".
- Send "Trusted Root Certificate Store" file from your computer to the device:** A section with instructions "The file must be in textual PEM format." and buttons for "Browse..." and "Send File".

A note is present: "Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link."

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.14 on page 61).

4.9 Step 9: Configure SRTP

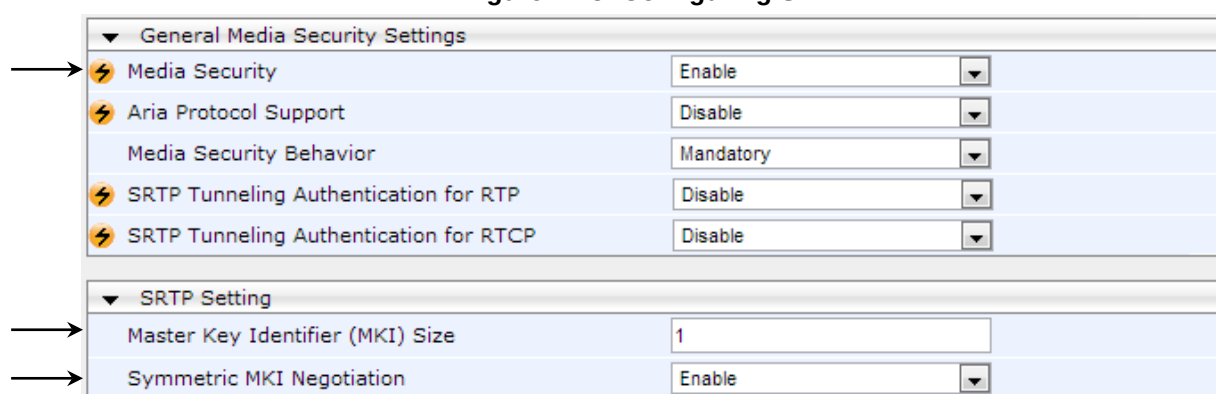
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 41).

➤ **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 4-28: Configuring SRTP



General Media Security Settings

- Media Security: Enable
- Aria Protocol Support: Disable
- Media Security Behavior: Mandatory
- SRTP Tunneling Authentication for RTP: Disable
- SRTP Tunneling Authentication for RTCP: Disable

SRTP Setting

- 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 4.14 on page 61).

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 4-29: Configuring Number of IP Media Channels

⚡ Number of Media Channels	30
⚡ Voice Streaming	Disable
NetAnn Announcement ID	annc
MSCML ID	ivr
Transcoding ID	trans

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 [4.14](#) on page [61](#)).

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 39, IP Group 1 represents Lync Server 2013, and IP Group 2 represents BT One Voice SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Lync Server 2013 (LAN) and BT One Voice SIP Trunk (WAN):

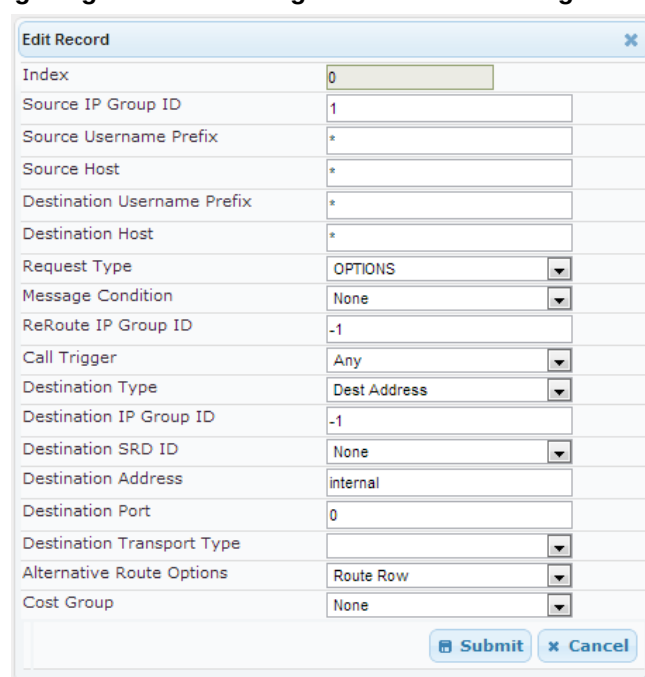
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to BT One Voice SIP Trunk
- Calls from BT One Voice SIP Trunk to Lync Server 2013

➤ 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 4-30: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN



Edit Record	
Index	0
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Cost Group	None
Submit Cancel	

3. Configure a rule to route calls from Lync Server 2013 to BT One Voice 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 4-31: Configuring IP-to-IP Routing Rule for LAN to WAN

The 'Add Record' dialog box is shown with the following configuration:

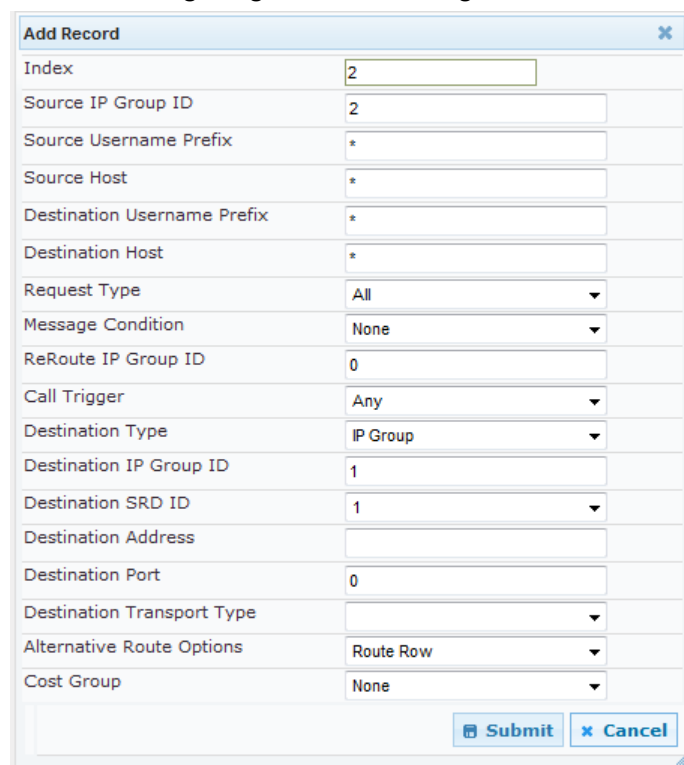
- Index: 1
- Source IP Group ID: 1
- Source Username Prefix: *
- Source Host: *
- Destination Username Prefix: *
- Destination Host: *
- Request Type: All
- Message Condition: None
- ReRoute IP Group ID: 0
- Call Trigger: Any
- Destination Type: IP Group
- Destination IP Group ID: 2
- Destination SRD ID: 2
- Destination Address: (empty)
- Destination Port: 0
- Destination Transport Type: (empty)
- Alternative Route Options: Route Row
- Cost Group: None

Buttons at the bottom: Submit, Cancel.

4. Configure a rule to route calls from BT One Voice 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 4-32: Configuring IP-to-IP Routing Rule for WAN to LAN



Index	2
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	0
Call Trigger	Any
Destination Type	IP Group
Destination IP Group ID	1
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Cost Group	None

The configured routing rules are shown in the figure below:

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



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



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 39, IP Group 1 represents Lync Server 2013, and IP Group 2 represents BT One Voice SIP Trunk.



Note: Adapt the manipulation table according to you 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 (BT One Voice 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

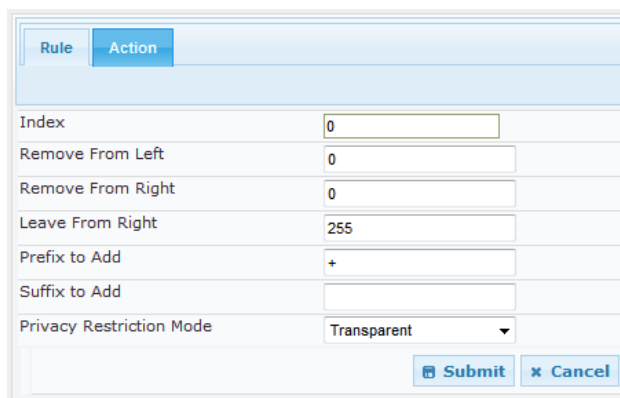
Figure 4-34: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Rule	
Index	0
Additional Manipulation	No
Source IP Group ID	2
Destination IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
ReRoute IP Group ID	-1
Call Trigger	Any
Manipulated URI	Destination
Submit Cancel	

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

Parameter	Value
Prefix to Add	+ (plus sign)

Figure 4-35: 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., BT One Voice SIP Trunk):

Figure 4-36: Example of Configured IP-to-IP Outbound Manipulation Rules

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 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 "+" 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: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

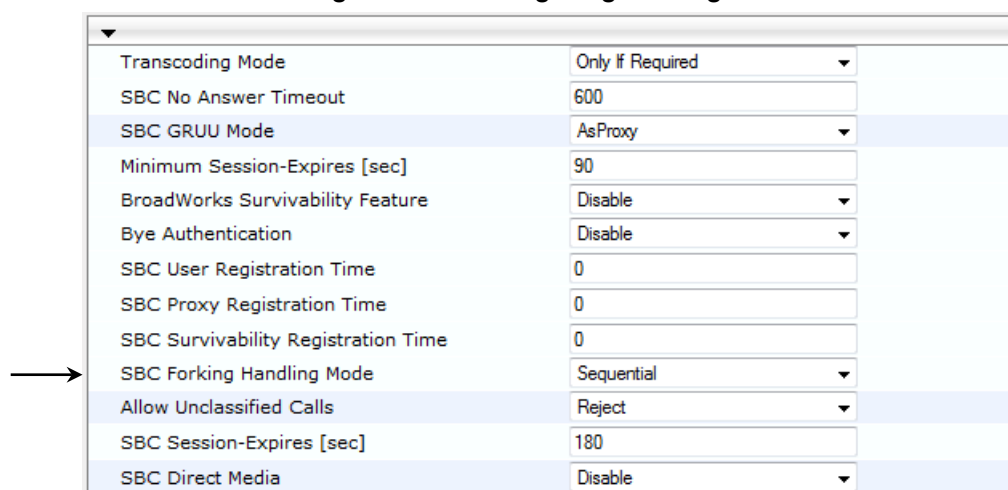
4.13.1 Step 13a: Configure Call Forking Mode

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 4-37: Configuring Forking Mode



Transcoding Mode	Only If Required
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
Bye Authentication	Disable
SBC User Registration Time	0
SBC Proxy Registration Time	0
SBC Survivability Registration Time	0
SBC Forking Handling Mode	Sequential
Allow Unclassified Calls	Reject
SBC Session-Expires [sec]	180
SBC Direct Media	Disable

3. Click **Submit**.

4.13.2 Step 13b: Configure SRTP State upon Re-key

This step describes how to configure the E-SBC to reset its SRTP state upon a re-key generation.

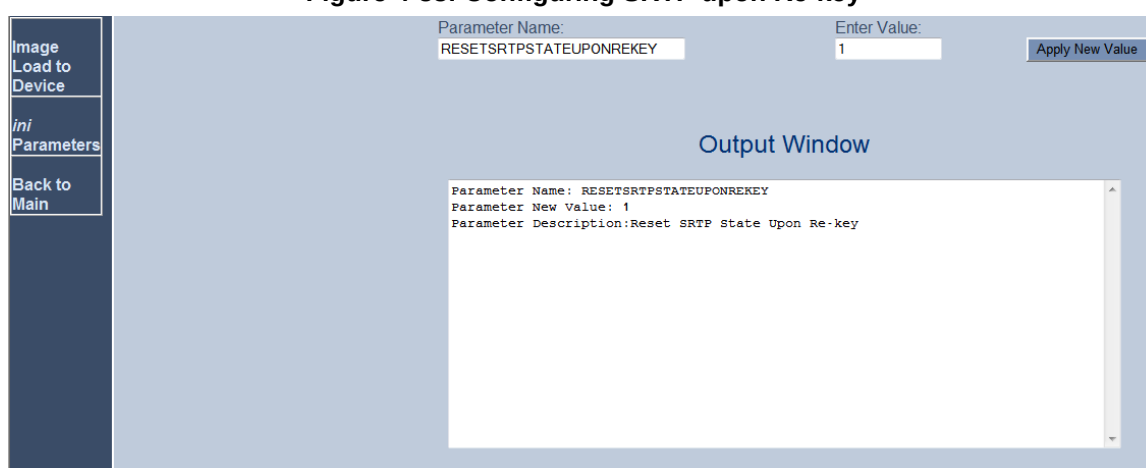
➤ **To configure SRTP upon re-key:**

1. Open the Admin page, by appending the suffix "AdminPage" (case-sensitive) to the E-SBC's IP address in the Web browser's URL field (e.g., <http://10.15.45.11/AdminPage>).
2. In the left pane, click **ini Parameters**.
3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
RESETSRTPSTATEUPONREKEY	1

4. Click **Apply New Value** for each field.

Figure 4-38: Configuring SRTP upon Re-key



The screenshot shows the 'ini Parameters' configuration page. On the left is a navigation pane with links: 'Image Load to Device', 'ini Parameters' (selected), and 'Back to Main'. The main area has two input fields: 'Parameter Name:' with the value 'RESETSRTPSTATEUPONREKEY' and 'Enter Value:' with the value '1'. An 'Apply New Value' button is to the right. Below these fields is an 'Output Window' displaying the following text:

```
Parameter Name: RESETSRTPSTATEUPONREKEY
Parameter New Value: 1
Parameter Description: Reset SRTP State Upon Re-key
```

4.14 Step 16: Reset the E-SBC

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

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

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

Figure 4-39: Resetting the E-SBC

The screenshot displays a web-based configuration interface for an E-SBC. It is organized into three main sections, each with a dropdown arrow on the left:

- Reset Configuration:** Contains three rows. The first row is 'Reset Board' with a 'Reset' button. The second row is 'Burn To FLASH' with a dropdown menu set to 'Yes'. The third row is 'Graceful Option' with a dropdown menu set to 'No'.
- LOCK / UNLOCK:** Contains three rows. The first row is 'Lock' with a 'LOCK' button. The second row is 'Graceful Option' with a dropdown menu set to 'No'. The third row is 'Gateway Operational State' with the text 'UNLOCKED'.
- Save Configuration:** Contains one row: 'Burn To FLASH' with a 'BURN' button.

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 29, is shown below:

```

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

;Board: BT Media Gateway
;Board Type: 47
;Serial Number: 3220947
;Slot Number: 1
;Software Version: 6.60A.217.006
;DSP Software Version: 624AE3 => 660.07
;Board IP Address: 10.15.45.11
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 495M Flash size: 64M
;Num of DSP Cores: 13 Num DSP Channels: 76
;Num of physical LAN ports: 3
;Profile: NONE
;Key features;;Board Type: 67 ;Channel Type: RTP DspCh=240
IPMediaDspCh=240 ;IP Media: Conf VXML VoicePromptAnnounc(H248.9)
ExtVoicePrompt=1MB ;E1Trunks=4 ;T1Trunks=4 ;Coders: G723 G729 GSM-
FR G727 ILBC ;PSTN Protocols: ISDN IUA=4 CAS ;DSP Voice features:
IpmDetector ;DATA features: Routing FireWall&VPN Wan-Rate=271Mbps
WIFI-5GHz WIFI-COUNTRY-CODE=0xff07 ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Control
Protocols: MGCP MEGACO SIP SASurvivability SBC=30 MSFT ;Default
features;;Coders: G711 G726;

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

[SYSTEM Params]
SyslogServerIP = 10.15.45.200
EnableSyslog = 1
NTPServerUTCOffset = 7200
TLSPkeySize = 1024
NTPServerIP = '10.15.9.10'
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
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]
LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]
MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
MEDIASECURITYBEHAVIOUR = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCPREFERENCESEXAMPLEMODE = 1
SBCFORKINGHANDLINGMODE = 1
RESETSRTPSTATEUPONREKEY = 1

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]
SNMPManagerIsUsed_0 = 1
SNMPManagerIsUsed_1 = 0
SNMPManagerIsUsed_2 = 0
```

```

SNMPManagerIsUsed_3 = 0
SNMPManagerIsUsed_4 = 0
SNMPManagerTableIP_0 = 10.7.2.17
SNMPManagerTableIP_1 = 0.0.0.0
SNMPManagerTableIP_2 = 0.0.0.0
SNMPManagerTableIP_3 = 0.0.0.0
SNMPManagerTableIP_4 = 0.0.0.0

[ PhysicalPortsTable ]
FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_0_1", 1, 1, 4, "User Port #0",
"GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 1, 4, "User Port #1",
"GROUP_1", "Redundant";
[ \PhysicalPortsTable ]

[ EtherGroupTable ]
FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1,
EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, GE_0_1, GE_0_2;
[ \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, 10.15.45.11, 16, 10.15.0.1, 1, "Voice",
10.15.9.10, , GROUP_1;
InterfaceTable 1 = 5, 10, 195.189.192.141, 25, 195.189.192.129, 2,
"BTSIP", 80.179.52.100, 80.179.55.100, GROUP_1;
[ \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", BTSIP, , 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 = "FE-Lync.Lync.local:5067", 2, 1;
ProxyIp 1 = " 193.113.149.50:5060 ", 0, 2;
[ \ProxyIp ]

[ IpProfile ]
FORMAT IpProfile_Index = IpProfile_ProfileName,
IpProfile_IpPreference, IpProfile_CodersGroupID,
IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay,
IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ,
IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDTMFOption, IpProfile_SecondTxDTMFOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_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 1 = "Lync", 1, 0, 0, 10, 10, 0, 0, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 3, -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, 3, 0, 2, 2, 1,
0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, -1;
IpProfile 2 = "BT Onevoice", 1, 3, 2, 10, 10, 46, 24, 0, 0, 0, 0,
2, 0, 0, 1, 1, -1, 1, 0, 3, -1, 1, 4, -1, 1, 1, 0, 0, "", 3, 0, 0,
3, 0, 2, 1, 0, 0, 0, 8, 300, 400, 0, -1, 0, -1, 0, 0, 1, 1, 3, 2,
2, 1, 3, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, -1, 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, 0, 0, 1, 0, -1;
ProxySet 2 = 0, 60, 0, 0, 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_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "Lync Server", 1, "", "", 0, -1, -1, 0, -1, 1,
"MRLan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "BT One Voice", 2, "", "", 0, -1, -1, 0, -1, 2,
"MRWan", 1, 2, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
[ \IPGroup ]

[ IP2IPRouting ]
FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress,
IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,
IP2IPRouting_AltRouteOptions, IP2IPRouting_CostGroup;
IP2IPRouting 0 = 1, "", "", "", "", 6, , -1, 0, 0, -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 1 = "Voice", 2, 0, 0, 5067, 1, , -1;
SIPInterface 2 = "BTSIP", 2, 5060, 0, 0, 2, , -1;
[ \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 1 = 0, 2, 1, "*", "*", "*", "*", 0, -1, 0,
1, 0, 0, 255, "+", "", 0;
IPOutboundManipulation 2 = 0, 1, 2, "*", "*", "+44", "*", 0, -1,
0, 1, 1, 0, 255, "", "", 0;
IPOutboundManipulation 3 = 0, 1, 2, "*", "*", "+", "*", 0, -1, 0,
1, 1, 0, 255, "00", "", 0;
IPOutboundManipulation 4 = 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, 0, -1, 0;
[ \CodersGroup0 ]

[ CodersGroup1 ]
FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = "g711Alaw64k", 20, 0, -1, 1;
CodersGroup1 1 = "g711Ul原因64k", 20, 0, -1, 1;
[ \CodersGroup1 ]

[ CodersGroup2 ]

```

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

[ AllowedCodersGroup2 ]
FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
[ \AllowedCodersGroup2 ]

[ RoutingRuleGroups ]
FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength,
RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;
[ \RoutingRuleGroups ]

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

[ \CpMediaRealm ]
```




Configuration Note