

Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

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



Microsoft Partner
Gold Communications



tIPicall
CONNECT WITH THE WORLD



Version 6.8

December 2013

Document # LTRT-39335

Table of Contents

1	Introduction	9
1.1	Intended Audience	9
1.2	About AudioCodes E-SBC Product Series.....	9
2	Component Information.....	11
2.1	AudioCodes E-SBC Version	11
2.2	tlPicall SIP Trunking Version	11
2.3	Microsoft Lync Server 2013 Version	11
2.4	Interoperability Test Topology	12
2.4.1	Environment Setup	13
2.4.2	Known Limitations.....	13
3	Configuring Lync Server 2013	15
3.1	Configuring the E-SBC as an IP / PSTN Gateway	15
3.2	Configuring the "Route" on Lync Server 2013.....	23
4	Configuring AudioCodes E-SBC.....	33
4.1	Step 1: IP Network Interfaces Configuration	34
4.1.1	Step 1a: Configure VLANs.....	35
4.1.2	Step 1b: Configure Network Interfaces.....	36
4.1.3	Step 1c: Configure the Native VLAN ID.....	37
4.2	Step 2: Enable the SBC Application	38
4.3	Step 3: Signaling Routing Domains Configuration	39
4.3.1	Step 3a: Configure Media Realms.....	39
4.3.2	Step 3b: Configure SRDs	41
4.3.3	Step 3c: Configure SIP Signaling Interfaces	43
4.4	Step 4: Configure Proxy Sets	44
4.5	Step 5: Configure IP Groups.....	46
4.6	Step 6: Configure IP Profiles	48
4.7	Step 7: SIP TLS Connection Configuration	54
4.7.1	Step 7a: Configure the NTP Server Address.....	54
4.7.2	Step 7b: Configure a Certificate	55
4.8	Step 8: Configure SRTP	59
4.9	Step 9: Configure IP-to-IP Call Routing Rules	60
4.10	Step 10: Configure IP-to-IP Manipulation Rules.....	65
4.11	Step 11: Configure Message Manipulation Rules	67
4.12	Step 12: Miscellaneous Configuration.....	77
4.12.1	Step 12a: Configure Call Forking Mode	77
4.13	Step 13: Reset the E-SBC	78
A	AudioCodes INI File	79
B	Configuring Transcoding from G.729 to G.711.....	89
B.1	Step 1: Configure Maximum IP Media Channels	89
B.2	Step 2: Configure Coders	90
B.3	Step 3: Configure Coders in the IP Profiles	93

List of Figures

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Lync with tIPicall SIP Trunk	12
Figure 3-1: Starting the Lync Server Topology Builder	15
Figure 3-2: Topology Builder Dialog Box.....	16
Figure 3-3: Save Topology Dialog Box.....	16
Figure 3-4: Downloaded Topology	17
Figure 3-5: Choosing New IP/PSTN Gateway	17
Figure 3-6: Define the PSTN Gateway FQDN.....	18
Figure 3-7: Define the IP Address	18
Figure 3-8: Define the Root Trunk.....	19
Figure 3-9: E-SBC added as IP/PSTN Gateway and Trunk Created.....	20
Figure 3-10: Choosing Publish Topology	20
Figure 3-11: Publish the Topology	21
Figure 3-12: Publishing in Progress	21
Figure 3-13: Publishing Wizard Complete.....	22
Figure 3-14: Opening the Lync Server Control Panel	23
Figure 3-15: Lync Server Credentials.....	24
Figure 3-16: Microsoft Lync Server 2013 Control Panel	24
Figure 3-17: Voice Routing Page	25
Figure 3-18: Route Tab	25
Figure 3-19: Adding New Voice Route	26
Figure 3-20: Adding New Trunk	26
Figure 3-21: List of Deployed Trunks	27
Figure 3-22: Selected E-SBC Trunk.....	27
Figure 3-23: Associating PSTN Usage to Route	28
Figure 3-24: Confirmation of New Voice Route	28
Figure 3-25: Committing Voice Routes	29
Figure 3-26: Uncommitted Voice Configuration Settings	29
Figure 3-27: Confirmation of Successful Voice Routing Configuration	29
Figure 3-28: Voice Routing Screen Displaying Committed Routes	30
Figure 3-29: Voice Routing Screen – Trunk Configuration Tab	30
Figure 4-1: Network Interfaces in Interoperability Test Topology.....	34
Figure 4-2: Configured VLAN IDs in Ethernet Device Table.....	35
Figure 4-3: Configured Network Interfaces in IP Interfaces Table	37
Figure 4-4: Configured Port Native VLAN	37
Figure 4-5: Enabling SBC Application	38
Figure 4-6: Configuring Media Realm for LAN	39
Figure 4-7: Configuring Media Realm for WAN.....	40
Figure 4-8: Configured Media Realms in Media Realm Table	40
Figure 4-9: Configuring LAN SRD	41
Figure 4-10: Configuring WAN SRD.....	42
Figure 4-11: Configured SIP Interfaces in SIP Interface Table	43
Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013.....	44
Figure 4-13: Configuring Proxy Set for tIPicall SIP Trunk.....	45
Figure 4-14: Configured IP Groups in IP Group Table	47
Figure 4-15: Configuring IP Profile for Lync Server 2013 – Common Tab	48
Figure 4-16: Configuring IP Profile for Lync Server 2013 – SBC Tab.....	50
Figure 4-17: Configuring IP Profile for tIPicall SIP Trunk – Common Tab	51
Figure 4-18: Configuring IP Profile for tIPicall SIP Trunk – SBC Tab	53
Figure 4-19: Configuring NTP Server Address.....	54
Figure 4-20: Certificates Page - Creating CSR	55
Figure 4-21: Microsoft Certificate Services Web Page	56
Figure 4-22: Request a Certificate Page	56
Figure 4-23: Advanced Certificate Request Page	57
Figure 4-24: Submit a Certificate Request or Renewal Request Page	57
Figure 4-25: Certificate Issued Page	57
Figure 4-26: Download a CA Certificate, Certificate Chain, or CRL Page	58
Figure 4-27: Certificates Page (Uploading Certificate).....	58

Figure 4-28: Configuring SRTP	59
Figure 4-29: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab	61
Figure 4-30: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab	61
Figure 4-31: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab	62
Figure 4-32: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab	63
Figure 4-33: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab	63
Figure 4-34: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab	64
Figure 4-35: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table	64
Figure 4-36: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab	65
Figure 4-37: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab	66
Figure 4-38: Example of Configured IP-to-IP Outbound Manipulation Rules	66
Figure 4-39: Configuring SIP Message Manipulation Rule 0 (for Lync Server 2013)	67
Figure 4-40: Configuring SIP Message Manipulation Rule 1 (for Lync Server 2013)	68
Figure 4-41: Configuring SIP Message Manipulation Rule 2 (for tIPicall SIP Trunk)	69
Figure 4-42: Configuring SIP Message Manipulation Rule 3 (for tIPicall SIP Trunk)	70
Figure 4-43: Configuring SIP Message Manipulation Rule 4 (for tIPicall SIP Trunk)	71
Figure 4-44: Configuring SIP Message Manipulation Rule 5 (for tIPicall SIP Trunk)	72
Figure 4-45: Configuring SIP Message Manipulation Rule 6 (for tIPicall SIP Trunk)	73
Figure 4-46: Configured SIP Message Manipulation Rules	73
Figure 4-47: Assigning Manipulation Sets 1 and 2 to IP Group 1	75
Figure 4-48: Assigning Manipulation Set 4 to IP Group 2	76
Figure 4-49: Configuring Forking Mode	77
Figure 4-50: Resetting the E-SBC	78
Figure 4-51: Configuring Number of IP Media Channels	89
Figure 4-52: Configuring Coder Group for Lync Server 2013	90
Figure 4-53: Configuring Coder Group for tIPicall SIP Trunk	90
Figure 4-54: Configuring Allowed Coders Group for tIPicall SIP Trunk	91
Figure 4-55: Configuring Allowed Coders Group for tIPicall SIP Trunk	92
Figure 4-56: SBC Preferences Mode	92
Figure 4-57: Configuring Coders in IP Profile for Lync Server 2013 – SBC Tab	93
Figure 4-58: Configuring IP Profile for tIPicall SIP Trunk – Common Tab	93

List of Tables

Table 2-1: AudioCodes E-SBC Version	11
Table 2-2: tIPicall Version	11
Table 2-3: Microsoft Lync Server 2013 Version	11
Table 2-4: Environment Setup	13
Table 4-1: SIP Message Manipulation Rules	74

Reader's Notes

Notice

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

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

© Copyright 2013 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: December-15-2013

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Reader's Notes

1 Introduction

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

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_F6.80A.009.005
Protocol	▪ SIP/UDP (to the tIPicall SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 tIPicall SIP Trunking Version

Table 2-2: tIPicall Version

Vendor/Service Provider	tIPicall
SSW Model/Service	Kamailio
Software Version	3.0.4
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

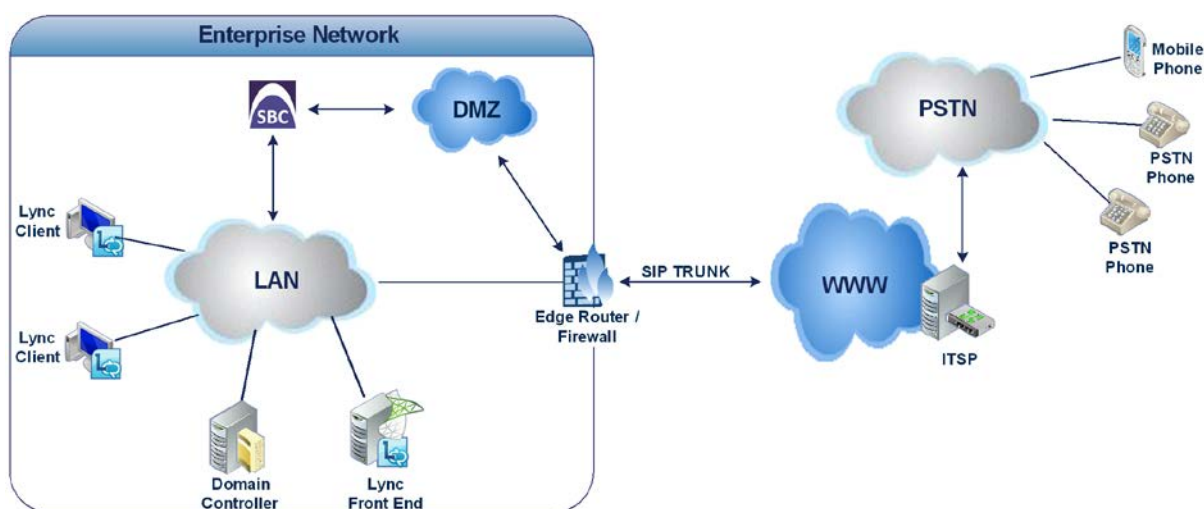
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and tIPicall 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 tIPicall's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border between Lync Server 2013 network in the Enterprise LAN and tIPicall'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 tIPicall 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 ▪ tIPicall SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ tIPicall SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ tIPicall SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ tIPicall 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 tIPicall'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.

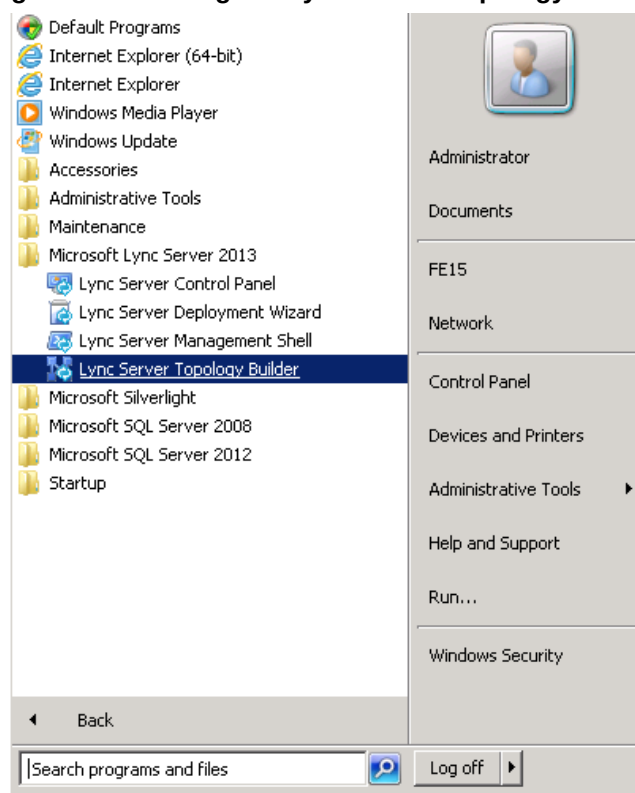
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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:**

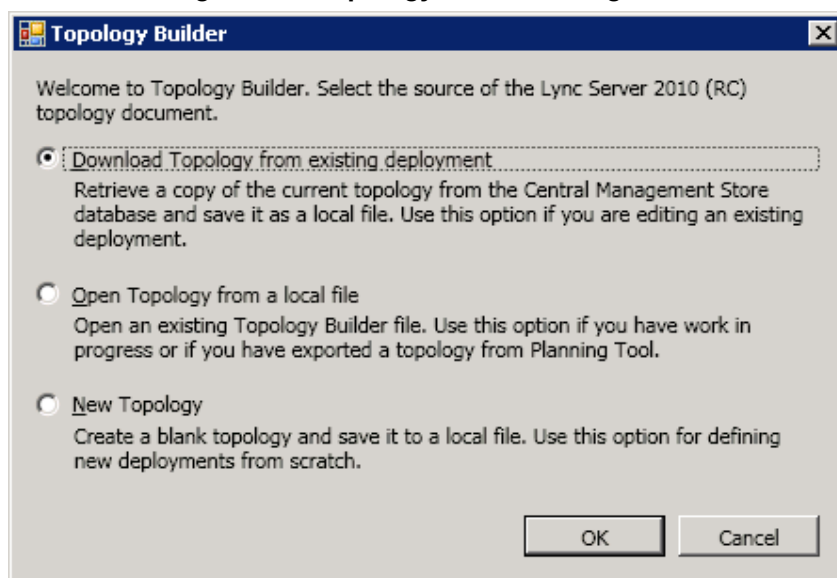
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



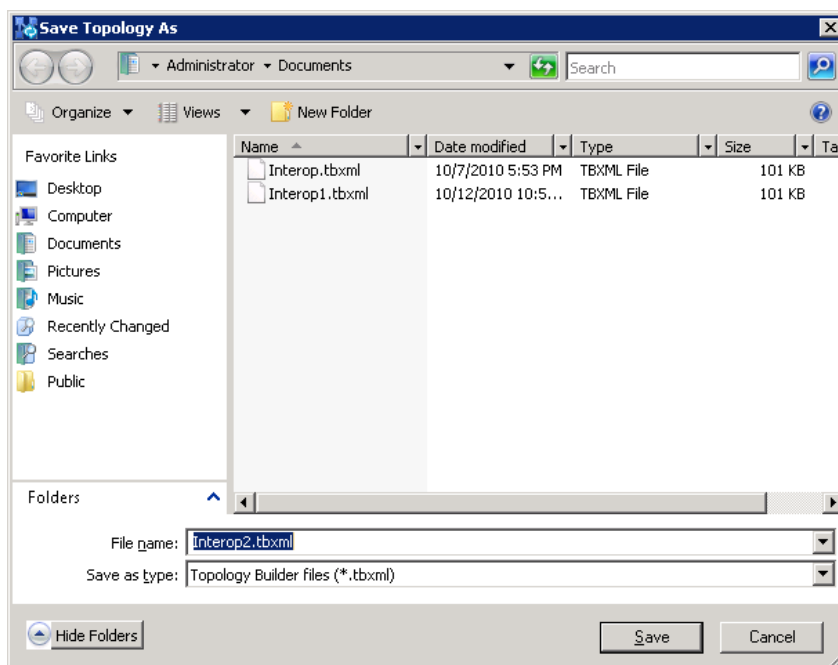
The following is displayed:

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:

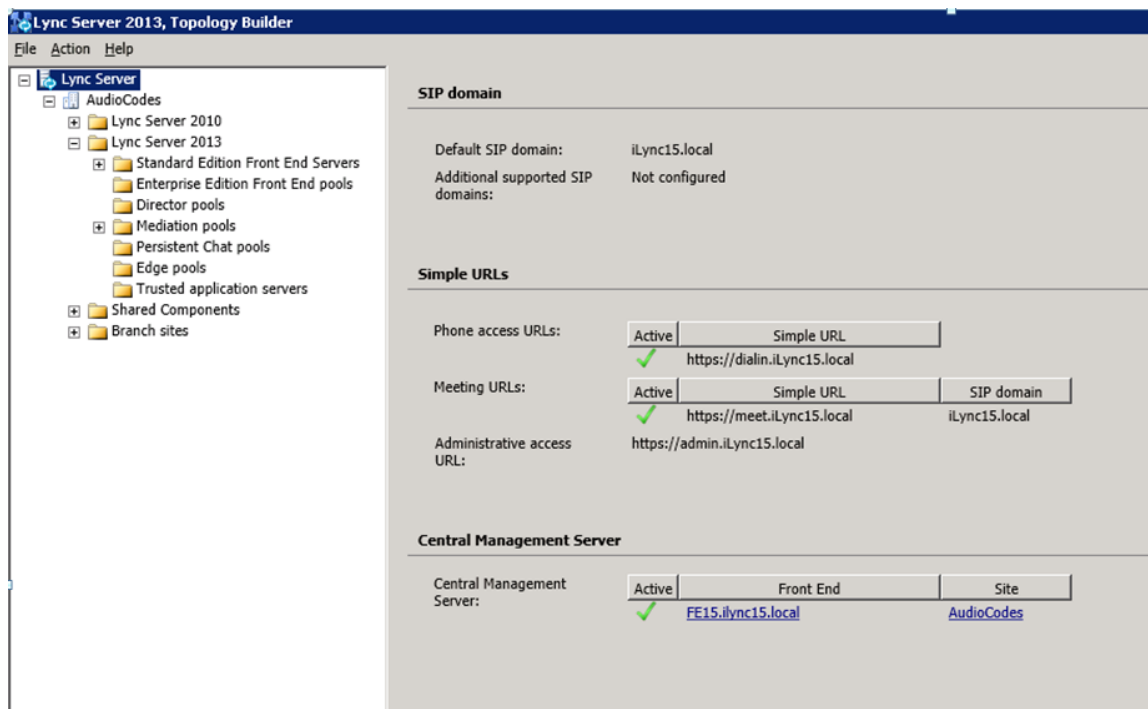
Figure 3-3: Save Topology Dialog Box



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.

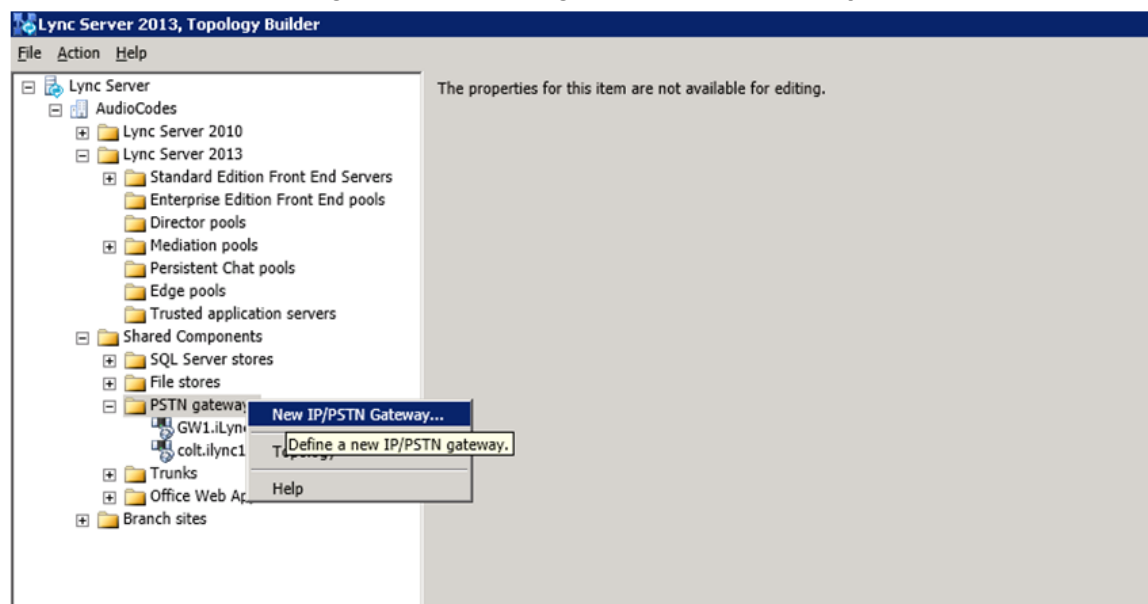
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



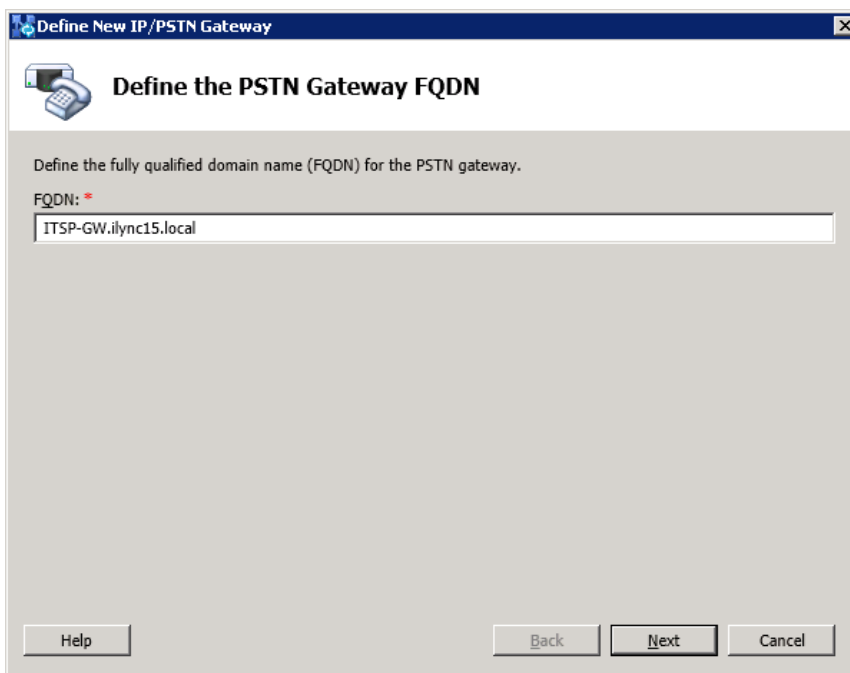
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

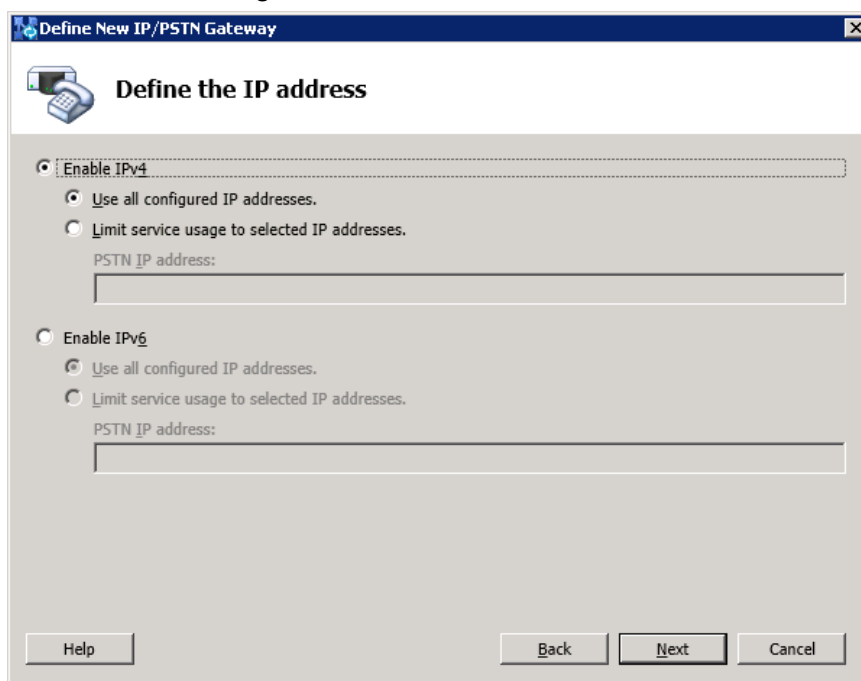
Figure 3-6: Define the PSTN Gateway FQDN



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

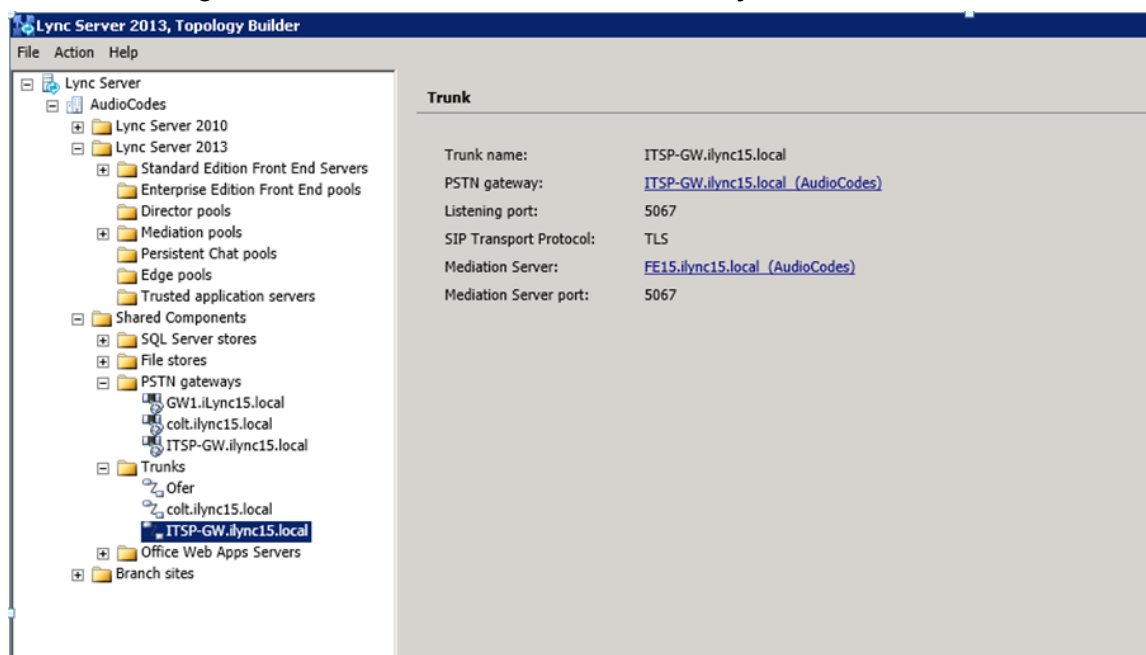
Associated Mediation Server port: *
5067

Help Back Finish Cancel

- 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**.

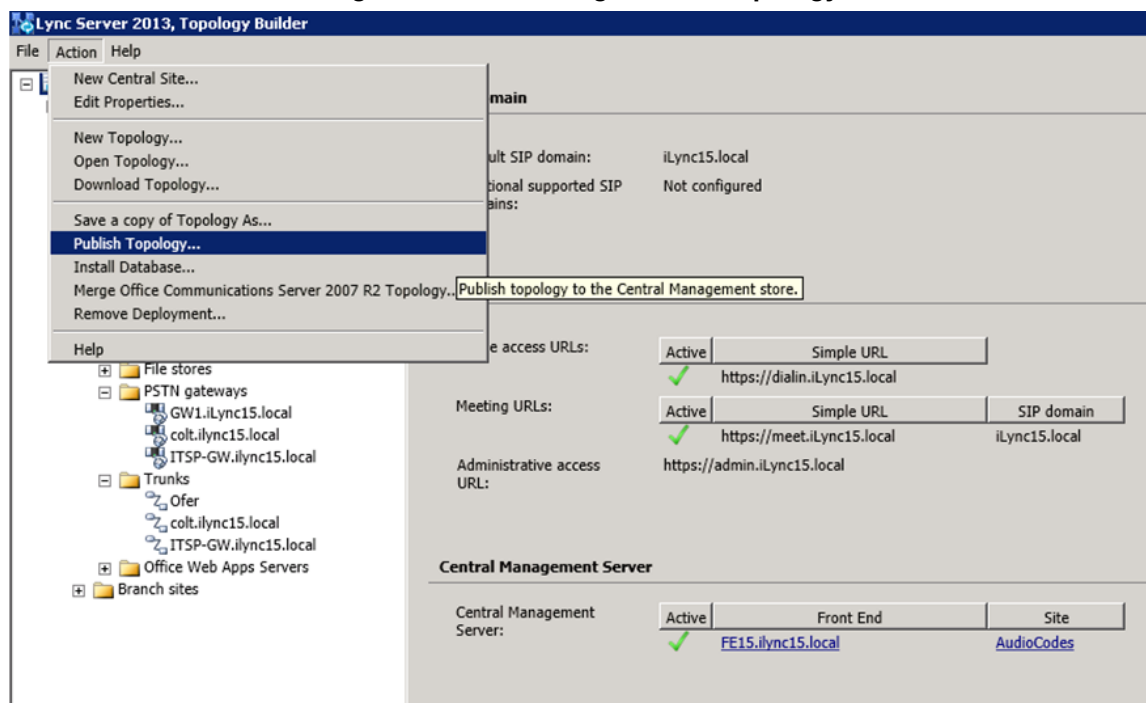
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



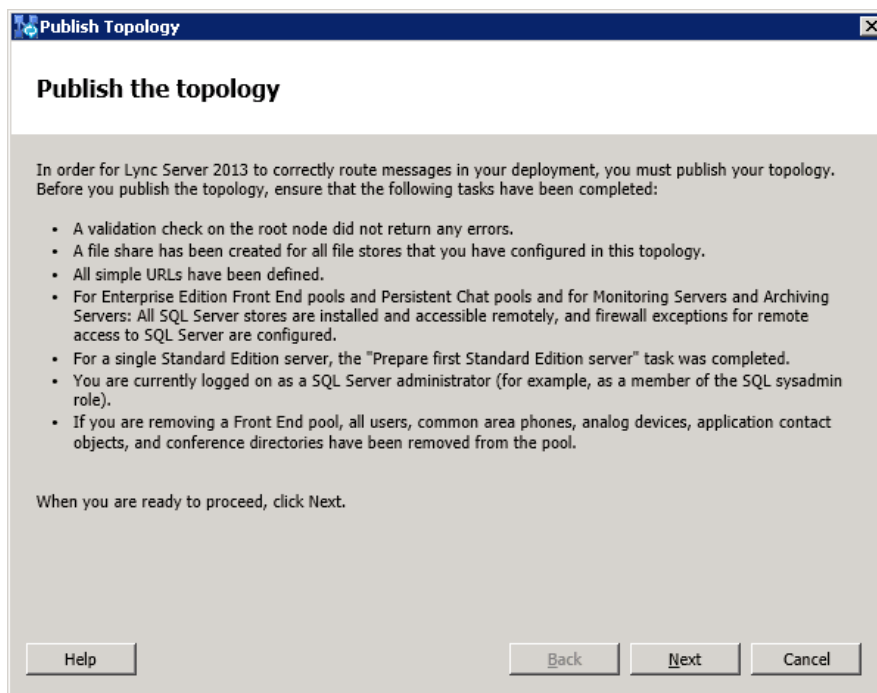
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



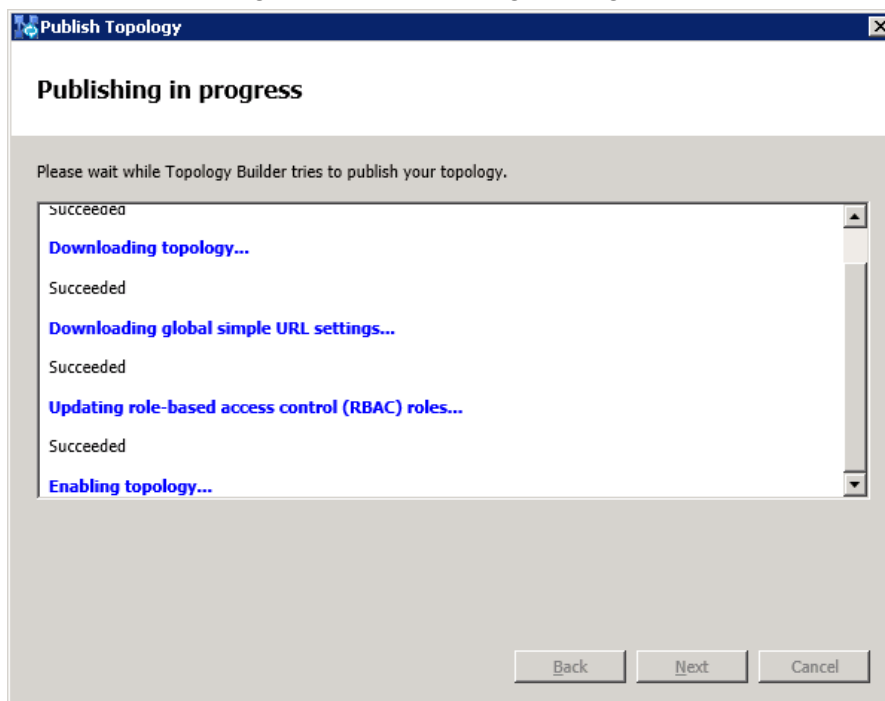
The following is displayed:

Figure 3-11: Publish the Topology



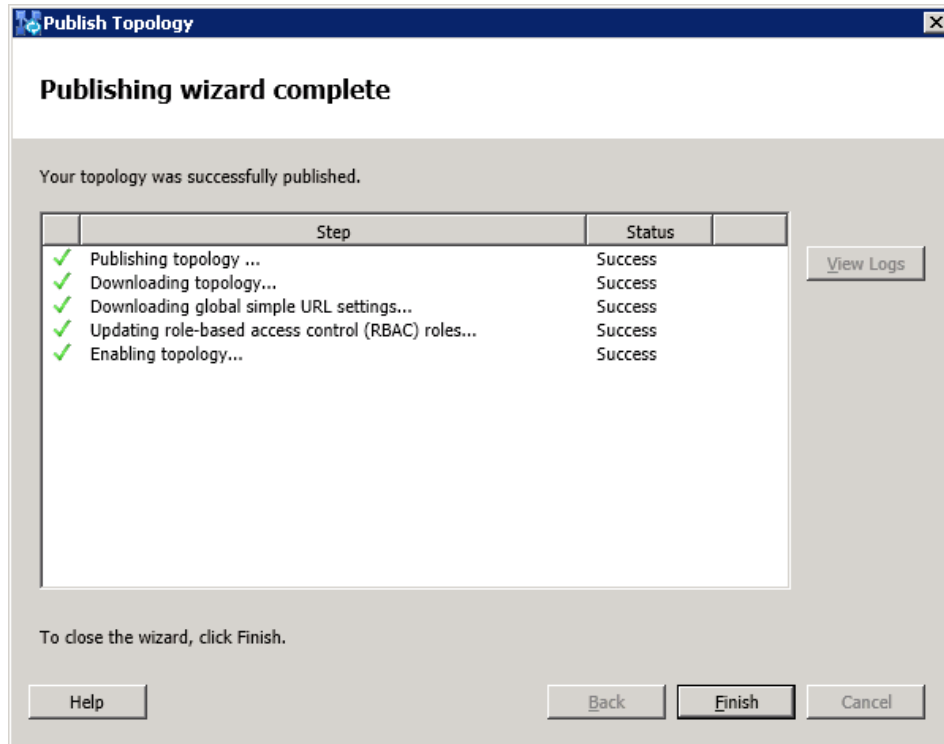
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

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:**

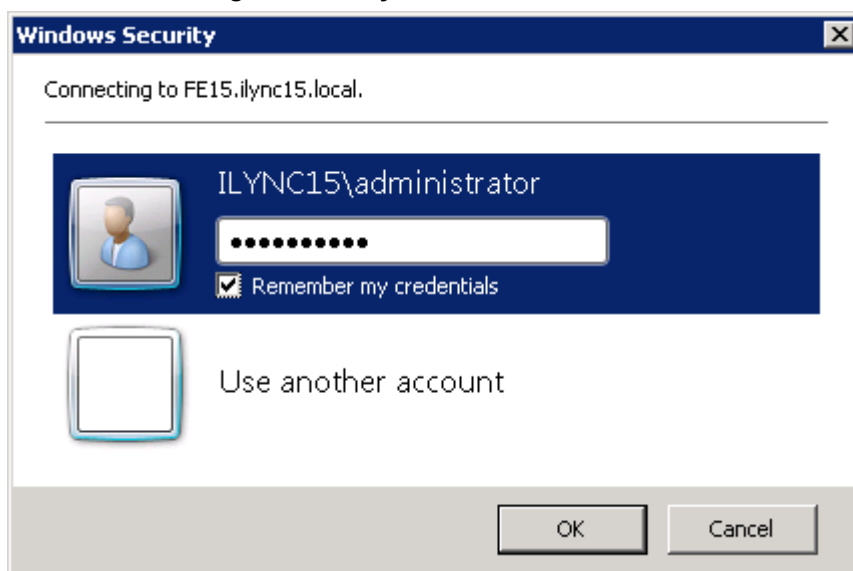
1. Start the Microsoft Lync Server 2013 Control Panel (**Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel



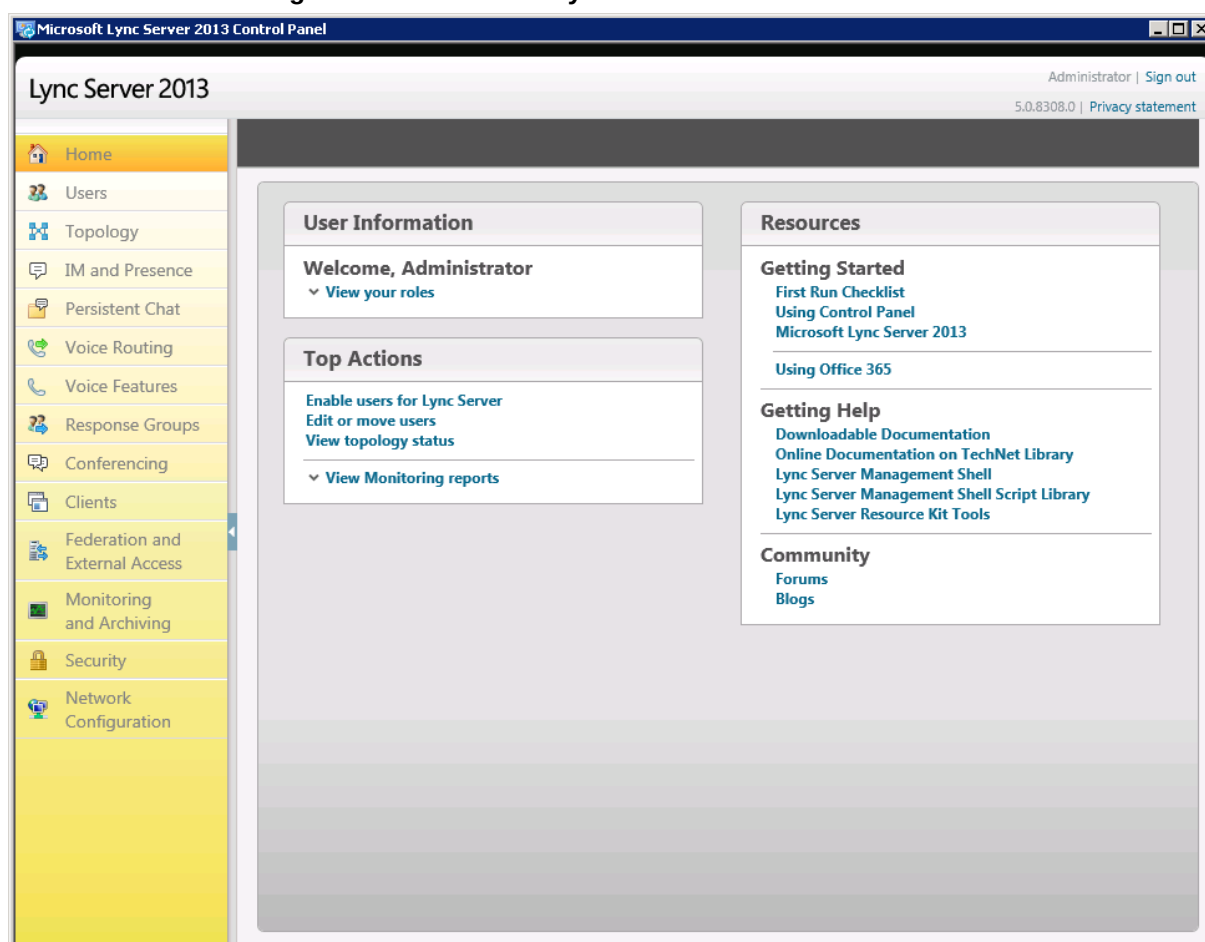
You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



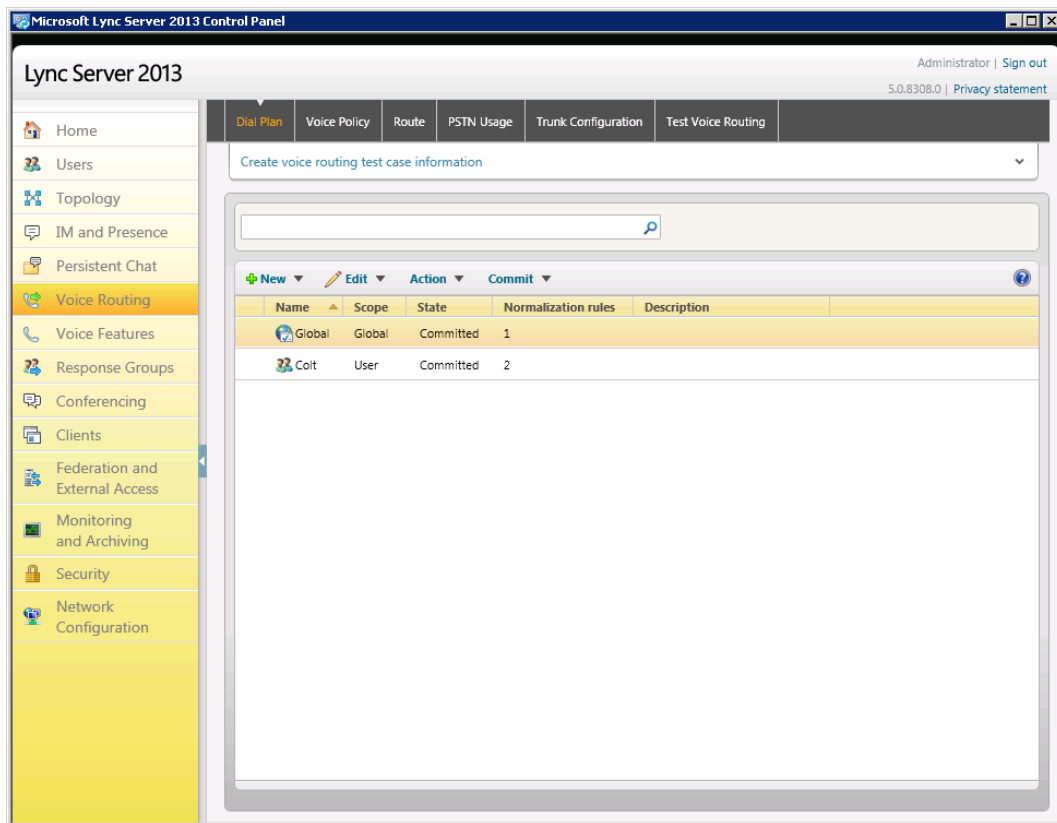
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



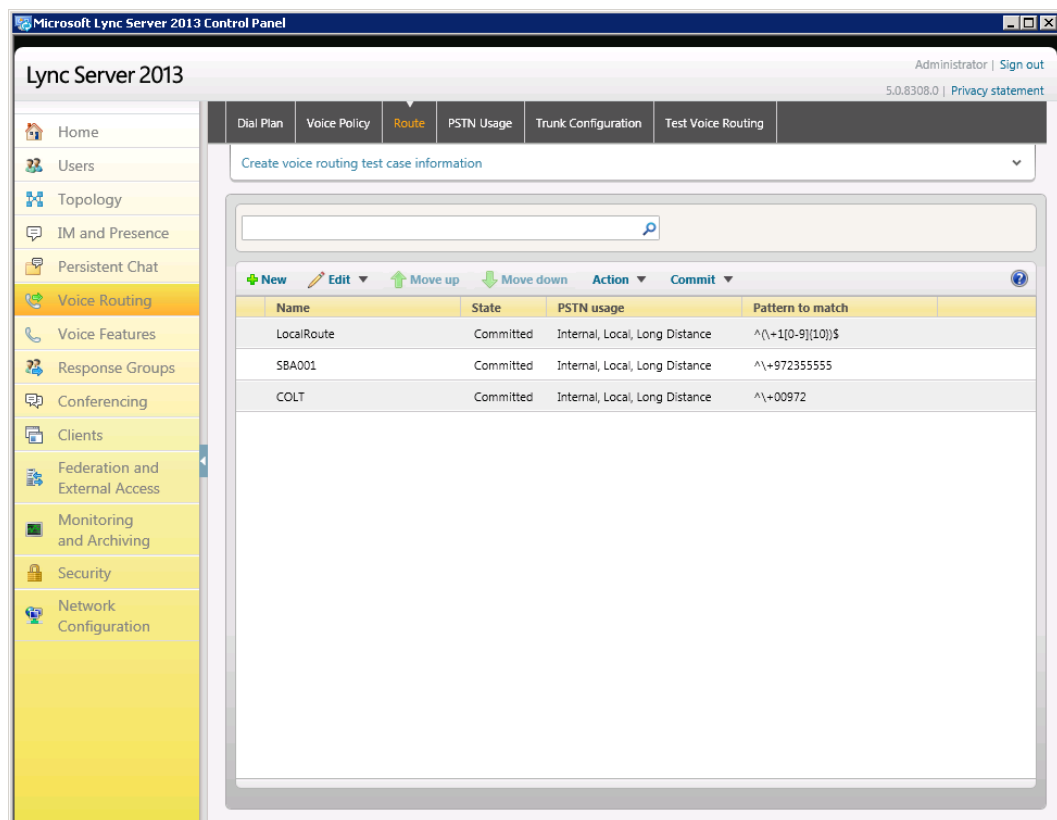
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



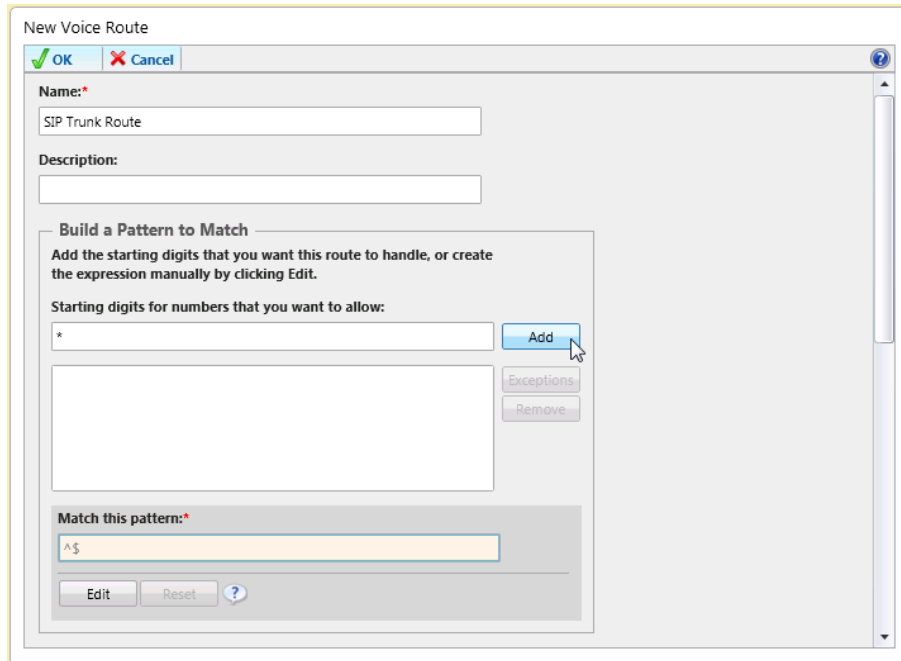
4. In the Voice Routing page, select the **Route** tab.

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

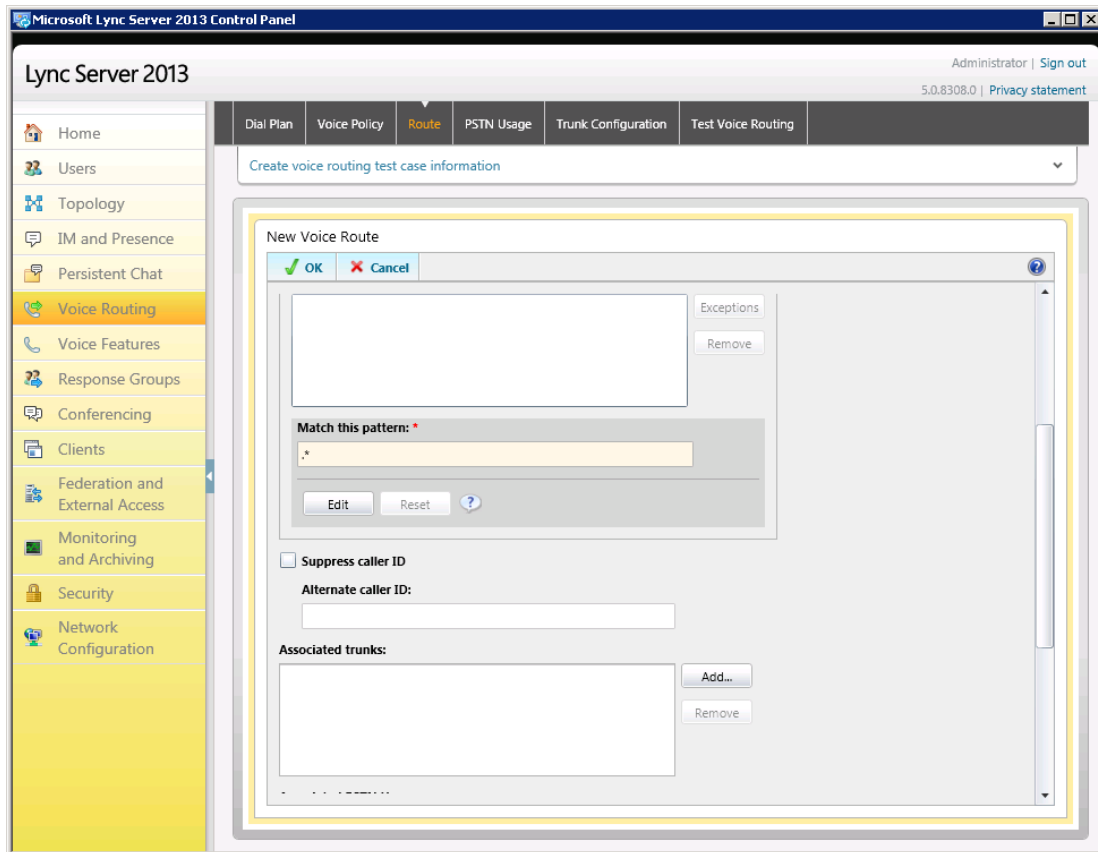
Match this pattern:*

^\$

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

Home Users Topology IM and Presence Persistent Chat Voice Routing Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration

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:

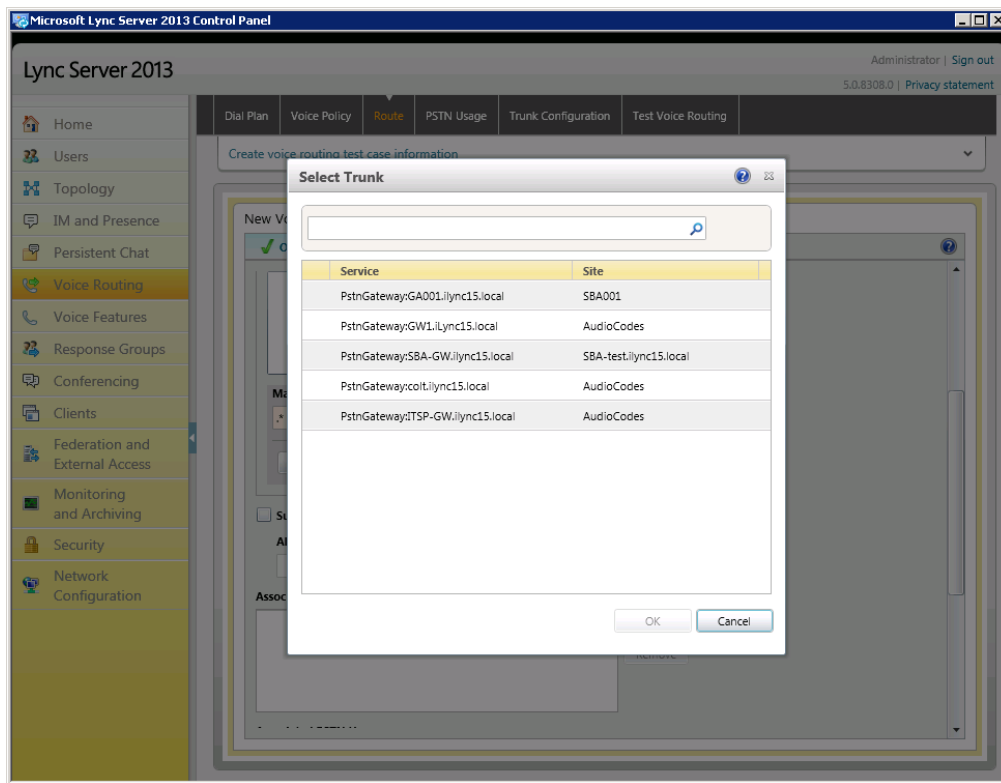
Associated trunks:

Add...

Remove

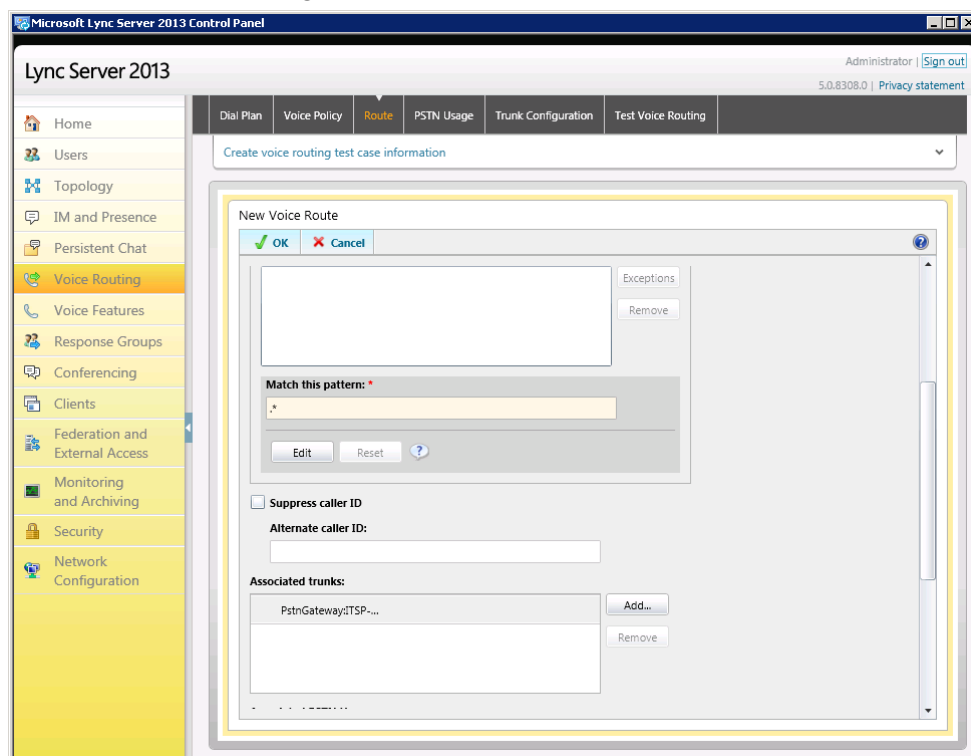
8. Associate the route with the E-SBC Trunk that you created:
 - a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



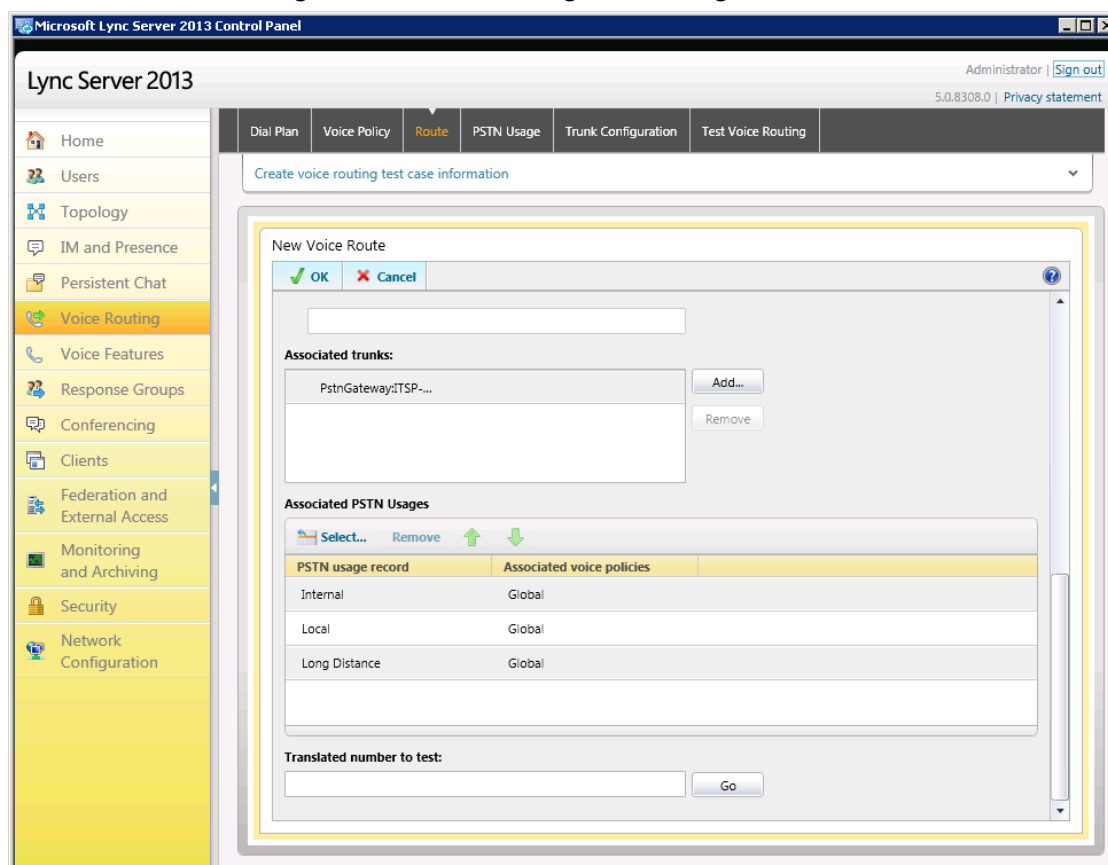
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



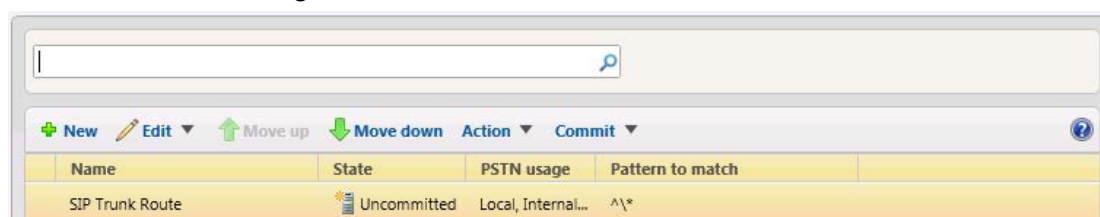
9. Associate a PSTN Usage to this route:
 - a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



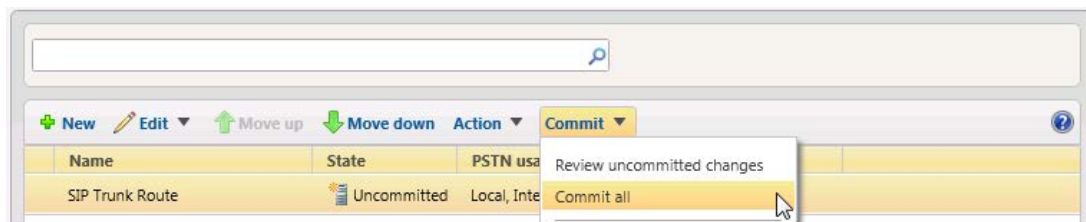
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



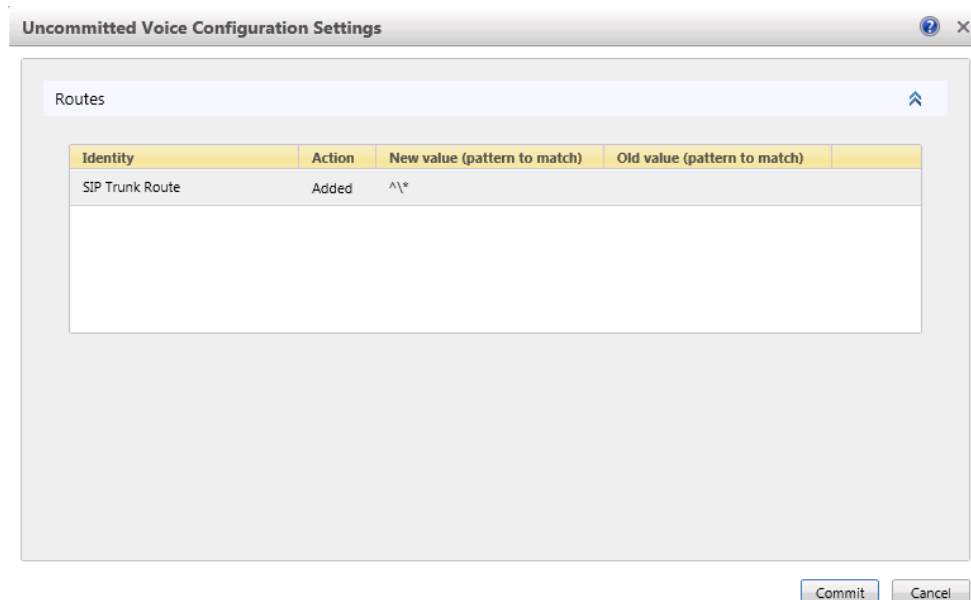
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



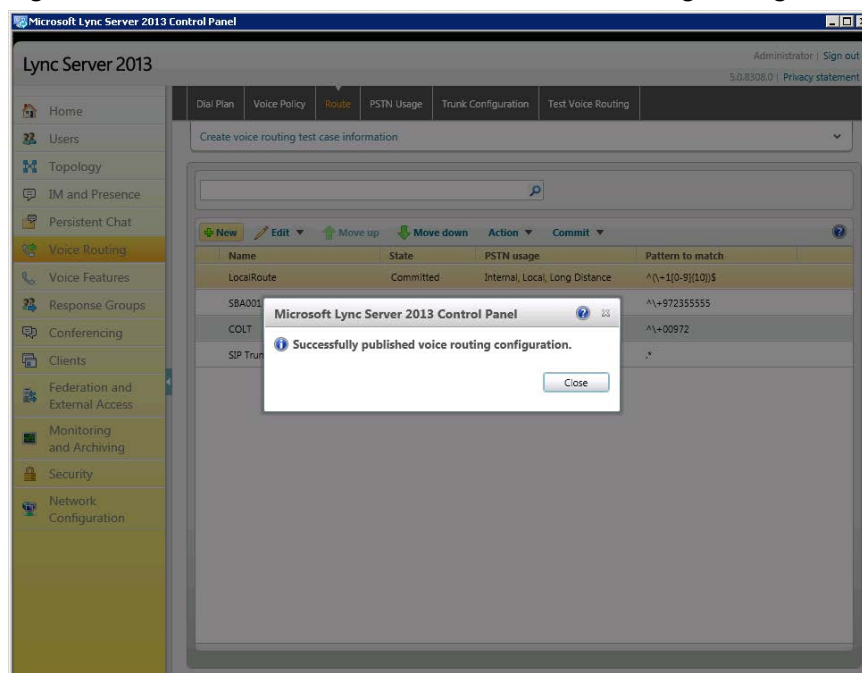
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



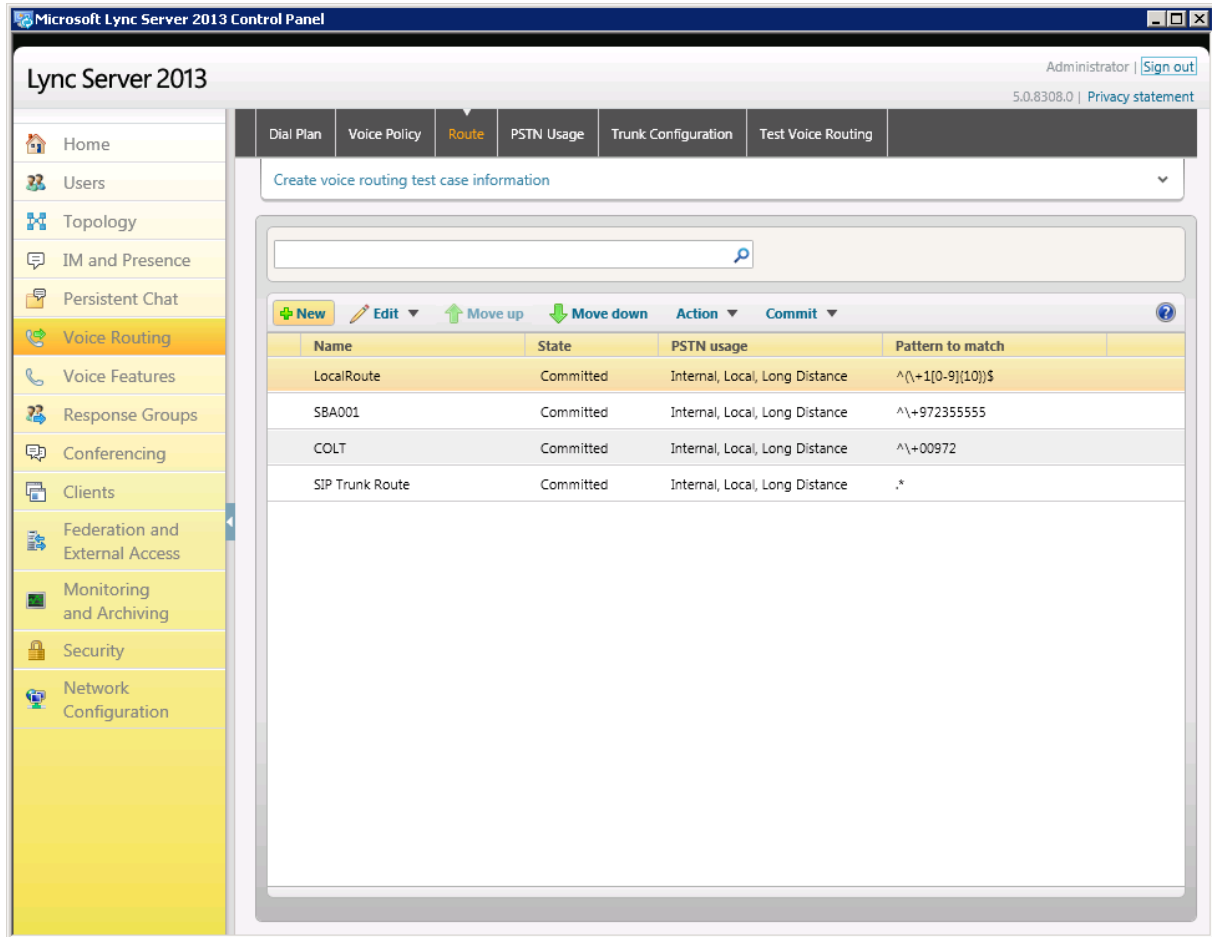
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

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



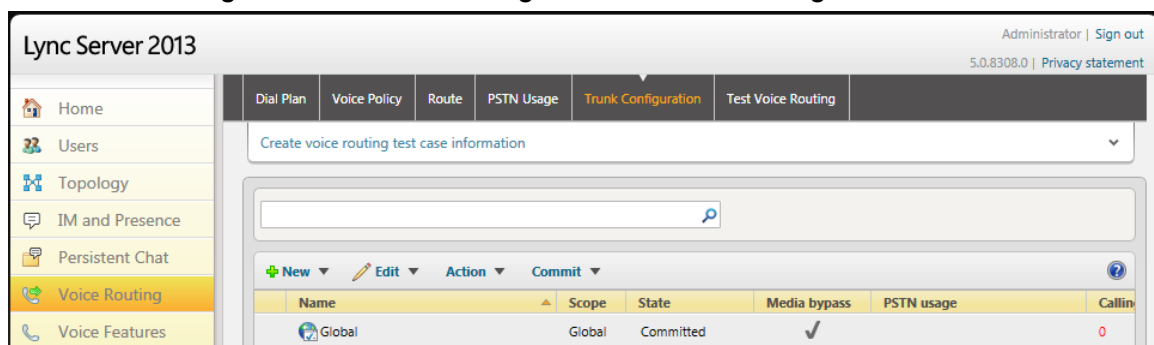
14. For ITSPs that implement a call identifier, continue with the following steps:



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 tIPicall SIP Trunk in the Diversion header. Using IP Profile (see Section 4.6 on page 48), the device adds this ID to the Diversion 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:

Edit Trunk Configuration - Global

OK Cancel

Scope: Global

Name: *

Global

Description:

Maximum early dialogs supported:

20

Encryption support level:

Required

Refer support:

Enable sending refer to the gateway

☒ Enable media bypass

☒ Centralized media processing

☐ Enable RTP latching

☒ Enable forward call history

☐ Enable forward P-Asserted-Identity data

☒ Enable outbound routing failover timer

^ Associated PSTN Usages

Select... Remove Up Down

- c. Select the **Enable forward call history** check box, and then click **OK**.
- d. Repeat Steps 11 through 13 to commit your settings.

Reader's Notes

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the tIPicall SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 12, and includes the following main areas:

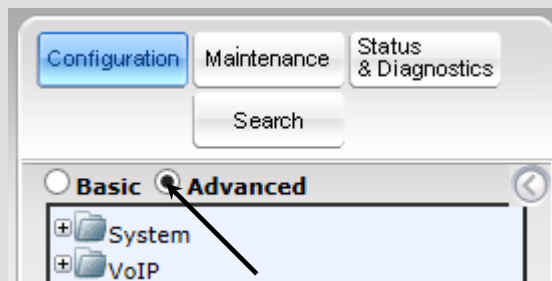
- E-SBC WAN interface - tIPicall SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

- For implementing Microsoft Lync and tIPicall 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:



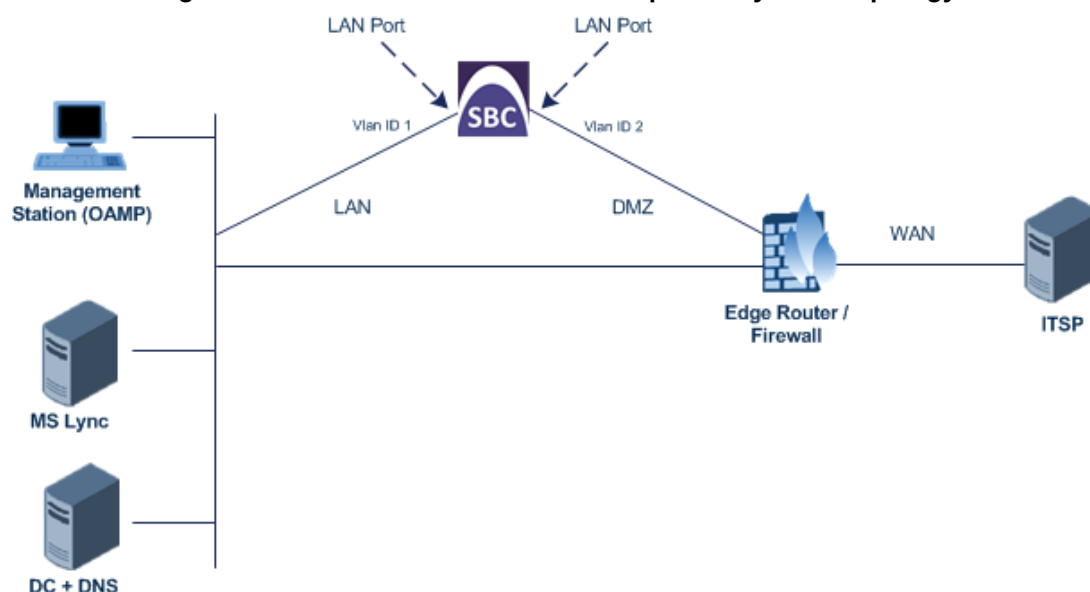
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

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
 - tIPicall 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 VLANs

This step describes how to define VLANs for each of the following interfaces:

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

➤ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	1
VLAN ID	2
Underlying Interface	GROUP_2 (Ethernet port group)
Name	vlan 2

Figure 4-2: Configured VLAN IDs in Ethernet Device Table

Ethernet Device Table			
Add +			
Index	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2

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

4.1.2 Step 1b: 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' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
 - b. Configure the interface as follows:

Parameter	Value
IP Address	10.15.17.77 (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 Device	vlan 1

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	195.189.192.153 (WAN IP address)
Prefix Length	25 (for 255.255.255.128)
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 Device	vlan 2

4. Click **Apply**, and then **Done**; the configured IP network interfaces are shown below:

Figure 4-3: Configured Network Interfaces in IP Interfaces Table

Interface Table									
Add +									
Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media	IPv4 Manual	10.15.17.77	16	10.15.0.1	Voice	10.15.25.1	0.0.0.0	vlan 1
1	Media + Control	IPv4 Manual	195.189.192.153	25	195.189.192.129	WANSP	80.179.52.100	80.179.55.100	vlan 2

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

4.1.3 Step 1c: 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 4-4: Configured Port Native VLAN

Physical Ports Settings							
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	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 4-5: 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 4.13 on page 78).

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 would be 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 > **VoIP Network** > **Media Realm Table**).
2. Modify the existing Media Realm for LAN traffic:

Parameter	Value
Index	0
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 4-6: Configuring Media Realm for LAN

The screenshot shows a web-based configuration interface for editing a Media Realm record. The dialog box is titled 'Edit Record #0'. It contains the following fields and values:

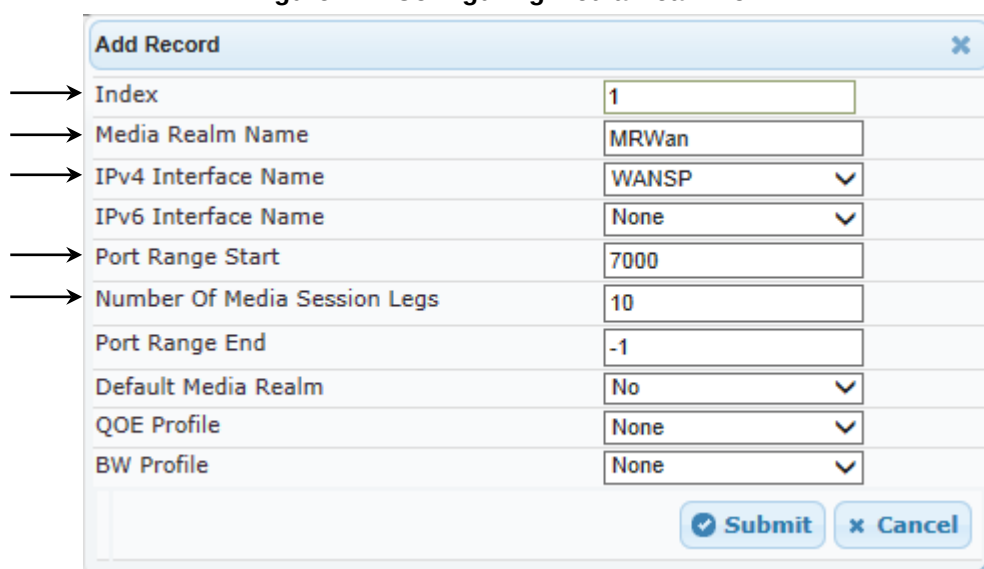
- Index:** 0
- Media Realm Name:** MRLan
- IPv4 Interface Name:** Voice
- IPv6 Interface Name:** None
- Port Range Start:** 6000
- Number Of Media Session Legs:** 10
- Port Range End:** 6090
- Default Media Realm:** Yes
- QOE Profile:** None
- BW Profile:** None

At the bottom right, there are 'Submit' and 'Cancel' buttons. Arrows on the left side of the image point to the Index, Media Realm Name, IPv4 Interface Name, IPv6 Interface Name, Port Range Start, and Number Of Media Session Legs fields.

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
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 4-7: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-8: Configured Media Realms in Media Realm Table

Media Realm Table			
Add +			
Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	MRLan	Voice	None
1	MRWan	WANSP	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 > **VoIP 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 Name	MRLan (associates SRD with Media Realm)

Figure 4-9: Configuring LAN SRD

The screenshot shows a web-based configuration interface for editing an SRD record. The dialog box is titled "Edit Record #1" and contains the following fields and values:

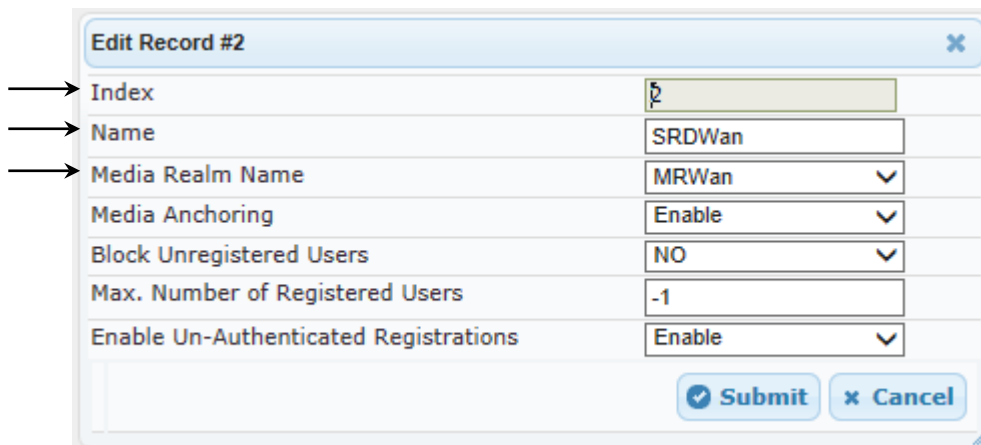
- Index:** 1
- Name:** SRDLan
- Media Realm Name:** MRLan (dropdown menu)
- Media Anchoring:** Enable (dropdown menu)
- Block Unregistered Users:** NO (dropdown menu)
- Max. Number of Registered Users:** -1
- Enable Un-Authenticated Registrations:** Enable (dropdown menu)

At the bottom right of the dialog are two buttons: "Submit" (with a checkmark icon) and "Cancel" (with an 'x' icon). Three arrows on the left side of the dialog point to the "Index", "Name", and "Media Realm Name" fields.

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

Parameter	Value
SRD Index	2
SRD Name	SRDWan
Media Realm	MRWan

Figure 4-10: Configuring WAN SRD



Edit Record #2 [X]

Index	2
Name	SRDWan
Media Realm Name	MRWan
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable

[Submit] [Cancel]

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 > **VoIP Network** > **SIP Interface Table**).
2. Configure a SIP interface for the LAN:

Parameter	Value
Index	1
Interface Name	Lync (arbitrary descriptive name)
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
Interface Name	Tipicall (arbitrary descriptive name)
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TCP and TLS	0
SRD	2

The configured SIP Interfaces are shown in the figure below:

Figure 4-11: Configured SIP Interfaces in SIP Interface Table

The screenshot shows the 'SIP Interface Table' configuration page. It includes an 'Add +' button and a table with the following data:

Index	Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	Lync	Voice	SBC	0	0	5067	1
2	Tipicall	WANSP	SBC	5060	0	0	2

At the bottom, there is a pagination bar showing 'Page 1 of 1', 'Show 10 records per page', and '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
- tIPicall SIP Trunk

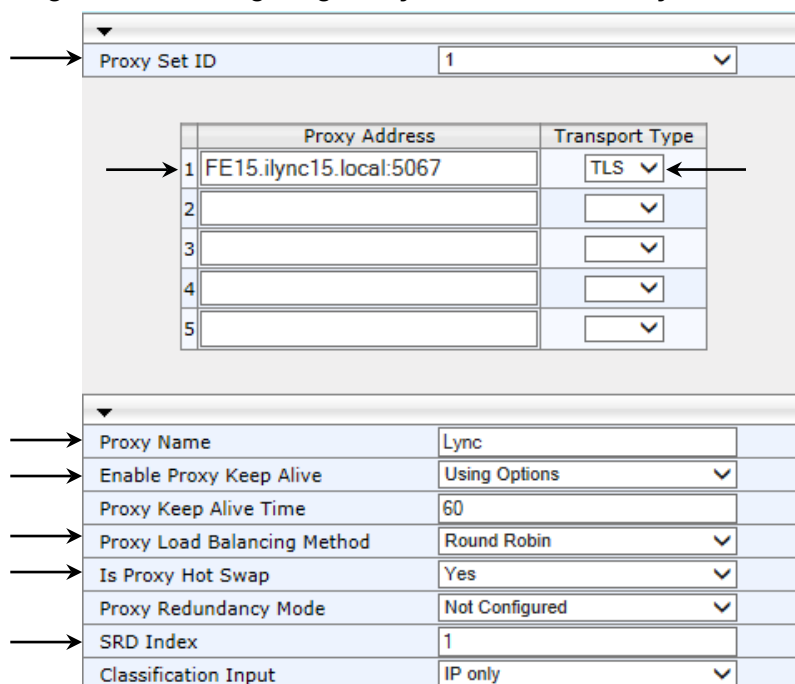
These Proxy Sets will later be associated with IP Groups.

➤ To configure Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP 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
Proxy Name	Lync (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	Yes
SRD Index	1

Figure 4-12: 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		

Proxy Name: Lync

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 tIPicall SIP Trunk:

Parameter	Value
Proxy Set ID	2
Proxy Address	tartarus.tipicall.net (tIPicall IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	Tipicall (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
Is Proxy Hot Swap	Yes
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to tIPicall SIP Trunk)

Figure 4-13: Configuring Proxy Set for tIPicall SIP Trunk

The screenshot shows the configuration interface for a Proxy Set. The fields and their values are as follows:

- Proxy Set ID:** 2
- Proxy Address Table:**

	Proxy Address	Transport Type
1	tartarus.tipicall.net	UDP
2		
3		
4		
5		
- Proxy Name:** Tipicall
- Enable Proxy Keep Alive:** Using Options
- Proxy Keep Alive Time:** 60
- Proxy Load Balancing Method:** Disable
- Is Proxy Hot Swap:** Yes
- 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 4.13 on page 78).

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
- tIPicall SIP Trunk located on WAN

➤ To configure IP Groups:

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

Parameter	Value
Index	1
Type	Server
Description	Lync (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	tartarus.tipicall.net (according to ITSP requirement)
SRD	1
Media Realm Name	MRLan
IP Profile ID	1

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

Parameter	Value
Index	2
Type	Server
Description	Tipicall (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	tartarus.tipicall.net (according to ITSP requirement)
SRD	2
Media Realm Name	MRWan
IP Profile ID	2

The configured IP Groups are shown in the figure below:

Figure 4-14: Configured IP Groups in IP Group Table

▼ IP Group Table								
Add +								
Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	Lync	1	tartarus.tipicall.net		Not Configured	No	1
2	Server	Tipicall	2	tartarus.tipicall.net		Not Configured	No	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
- tIPicall SIP trunk - to operate in non-secure mode using RTP and UDP

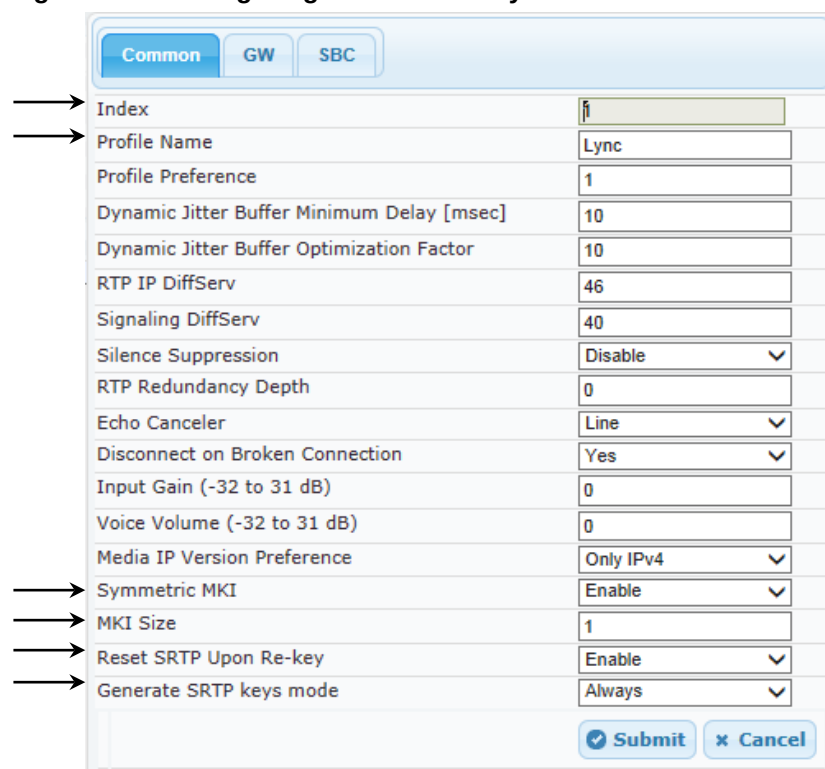
Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 46).

➤ To configure IP Profiles:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Profile Name	Lync (arbitrary descriptive name)
Symmetric MKI	Enable
MKI Size	1
Reset SRTP State Upon Re-key	Enable
Generate SRTP keys mode:	Always

Figure 4-15: Configuring IP Profile for Lync Server 2013 – Common Tab



Parameter	Value
Index	1
Profile Name	Lync
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceler	Line
Disconnect on Broken Connection	Yes
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Enable
MKI Size	1
Reset SRTP Upon Re-key	Enable
Generate SRTP keys mode	Always

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

Parameter	Value
SBC Media Security Behavior	SRTP
PRACK Mode	Optional (required, as tIPicall does not support PRACK)
Session Expires Mode	Supported (required, as tIPicall does not support Session Timer)
Remote Update Support	Supported Only After Connect
Remote Re-INVITE	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally (required, as Lync Server 2013 does not support receipt of SIP REFER)
Remote 3xx Behavior	Handle Locally (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
Enforce MKI Size	Enforce
Remote Early Media RTP Behavior	Delayed (required, as Lync Server 2013 does not send RTP immediately to remote side when it sends a SIP 18x response)

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

Common GW SBC	
Index	1
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	None
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
→ SBC Media Security Behavior	SRTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
→ PRACK Mode	Optional
→ Session Expires Mode	Supported
→ Remote Update Support	Supported Only After
→ Remote re-INVITE	Supported only with S
→ Remote Delayed Offer Support	Not Supported
→ Remote REFER Behavior	Handle Locally
→ Remote 3xx Behavior	Handle Locally
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
→ Enforce MKI Size	Enforce
→ Remote Early Media RTP Behavior	Delayed
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Transparent
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care
Submit Cancel	

5. Configure an IP Profile for the tIPicall SIP Trunk:
6. Click **Add**.
7. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Profile Name	Tipicall (arbitrary descriptive name)

Figure 4-17: Configuring IP Profile for tIPicall SIP Trunk – Common Tab

The screenshot shows the 'Common' tab configuration for the tIPicall SIP Trunk. The form contains the following parameters and values:

Parameter	Value
Index	2
Profile Name	Tipicall
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceler	Line
Disconnect on Broken Connection	Yes
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	300

At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

Parameter	Value
Profile ID	2
SBC Media Security Behavior	RTP
P-Asserted-Identity	Add (required for anonymous calls)
Diversion Mode	Add (required for forwarded calls)
History-Info Mode	Remove (required, as Lync Server 2013 send History-Info for forwarded calls)
Remote Update Support	Not Supported (required, as tIPicall SIP trunk not support Update, that send during session refreshment process)
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Remote Hold Format	Send Only (required, as tIPicall SIP Trunk close call if it not receive RTP within 80 seconds)

Figure 4-18: Configuring IP Profile for tIPicall SIP Trunk – SBC Tab

Common GW SBC	
→ Index	5
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	None
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
→ SBC Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
→ P-Asserted-Identity	Add
→ Diversion Mode	Add
→ History-Info Mode	Remove
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
→ Remote Update Support	Not Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Not Supported
→ Remote REFER Behavior	Handle Locally
Remote 3xx Behavior	Transparent
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
Enforce MKI Size	Don't enforce
Remote Early Media RTP Behavior	Immediate
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
→ Remote Hold Format	Send Only
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care
Submit Cancel	

4.7 Step 7: 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.

4.7.1 Step 7a: 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 4-19: Configuring NTP Server Address

NTP Settings		
NTP Server Address (IP or FQDN)	10.15.25.1	
NTP UTC Offset	Hours: 3	Minutes: 0
NTP Updated Interval	Hours: 24	Minutes: 0
NTP Secondary Server Address (IP or FQDN)		
NTP Authentication Key Identifier	0	
NTP Authentication Secret Key		

3. Click **Submit**.

4.7.2 Step 7b: 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)

Create CSR

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-----
MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNFQlUdXLMlseW5jMTUubG9jYWwWZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCKxytgT2W1vz0NGUstpa7w2DKKkxr8xA9sGLXwy0ZCyB49U1pDF
DJV8IldUfT8qL9d9V64f3z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAAgADANBgkqhkiG9w0BAQQFAAOBqQBLqe880JGrmEzPu5Q1
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**).

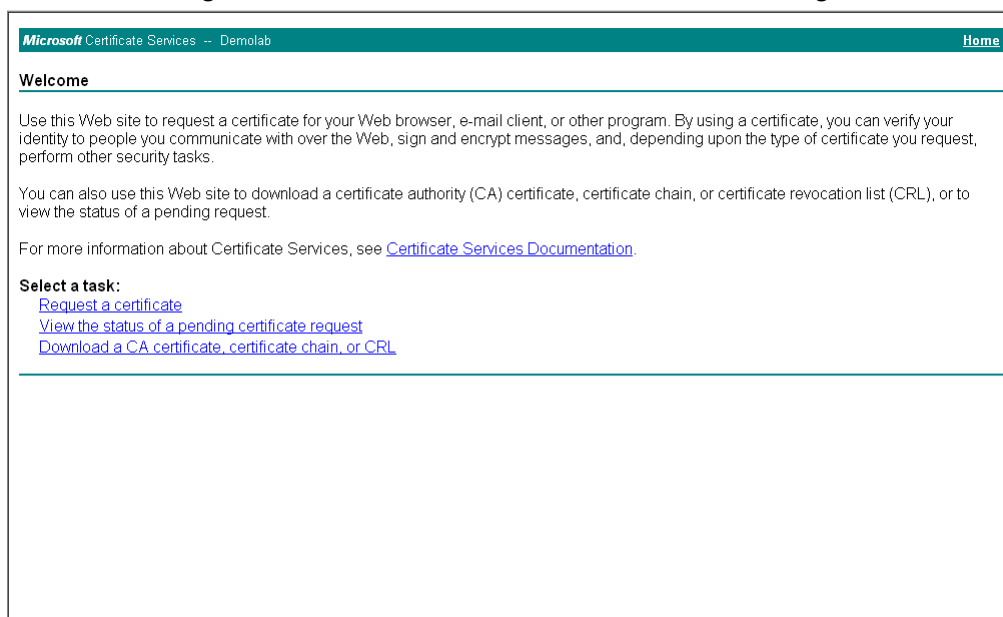


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 15).

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*.

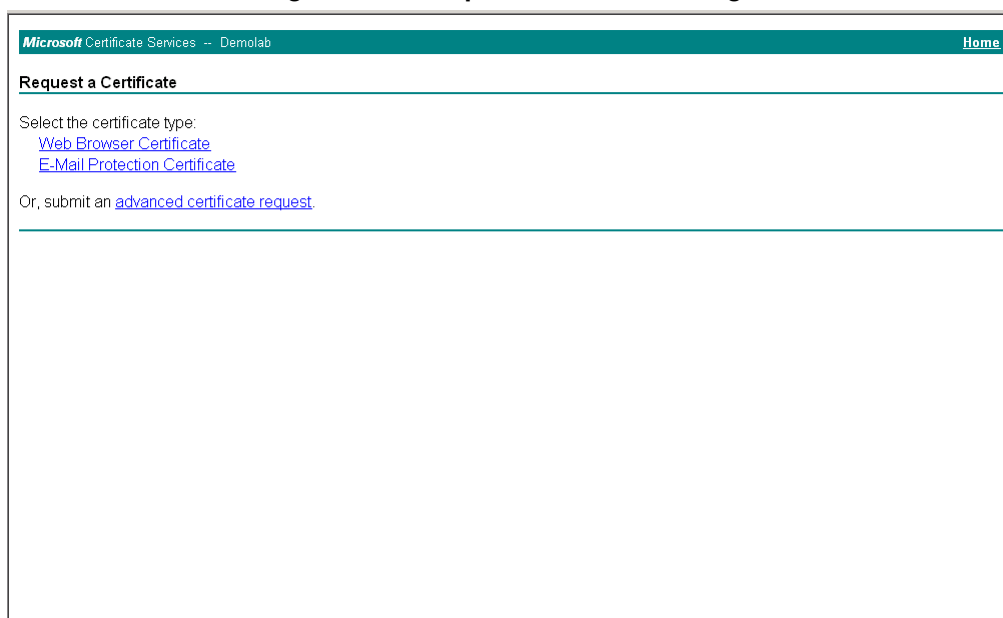
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

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
rr4ootrnsPOCAuEAAaAAMAOCSqGSIb3DQEBAUA
HnkHAKx8xHq9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj8ib+R5+YI+Oot57xT9DZXNg5Yp4G+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

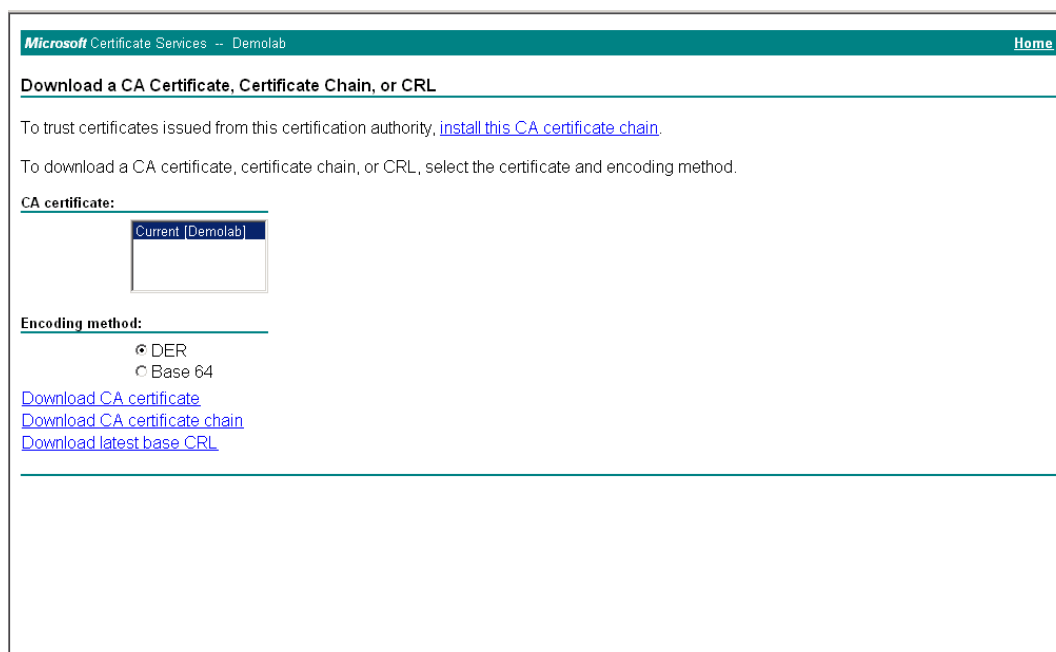
The certificate you requested was issued to you.

☐ 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



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)



20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.13 on page 78).

4.8 Step 8: 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 48).

➤ **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

Figure 4-28: Configuring SRTP

▼ General Media Security Settings		
⚡ Media Security	Enable	▼
⚡ Aria Protocol Support	Disable	▼
Media Security Behavior	Mandatory	▼
Authentication On Transmitted RTP Packets	Active	▼
Encryption On Transmitted RTP Packets	Active	▼
Encryption On Transmitted RTCP Packets	Active	▼
⚡ SRTP Tunneling Authentication for RTP	Disable	▼
⚡ SRTP Tunneling Authentication for RTCP	Disable	▼

3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.13 on page 78).

4.9 Step 9: 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 46, IP Group 1 represents Lync Server 2013, and IP Group 2 represents tIPicall 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 tIPicall SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to tIPicall SIP Trunk
- Calls from tIPicall 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:
3. Click **Add**.
4. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Route Name	OPTIONS termination (arbitrary descriptive name)
Source IP Group ID	1
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

Figure 4-29: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab

Rule	
Index	0
Route Name	OPTIONS termination
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

Submit Cancel

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-30: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

Action	
Index	0
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
Group Policy	None
Cost Group	None
Rules Set Id	-1

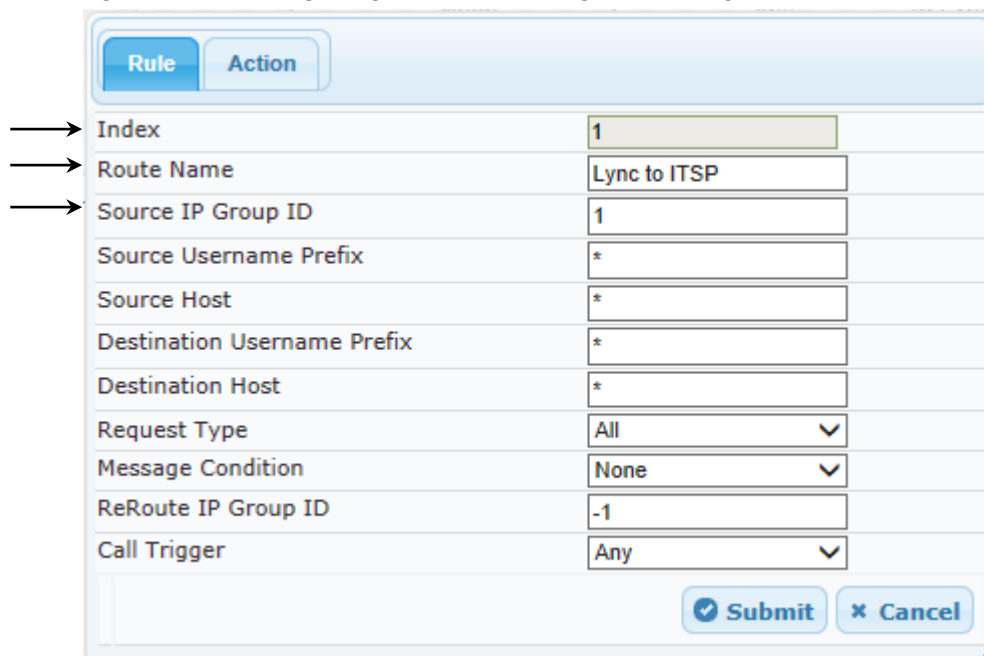
Submit Cancel

6. Configure a rule to route calls from Lync Server 2013 to tIPicall SIP Trunk:
 7. Click **Add**.

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

Parameter	Value
Index	1
Route Name	Lync to ITSP (arbitrary descriptive name)
Source IP Group ID	1

Figure 4-31: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab



Parameter	Value
Index	1
Route Name	Lync to ITSP
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	-1
Call Trigger	Any

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2

Figure 4-32: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab

Rule Action	
Index	1
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1

Submit Cancel

10. Configure a rule to route calls from tIPical SIP Trunk to Lync Server 2013:
11. Click **Add**.
12. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	ITSP to Lync (arbitrary descriptive name)
Source IP Group ID	2

Figure 4-33: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab

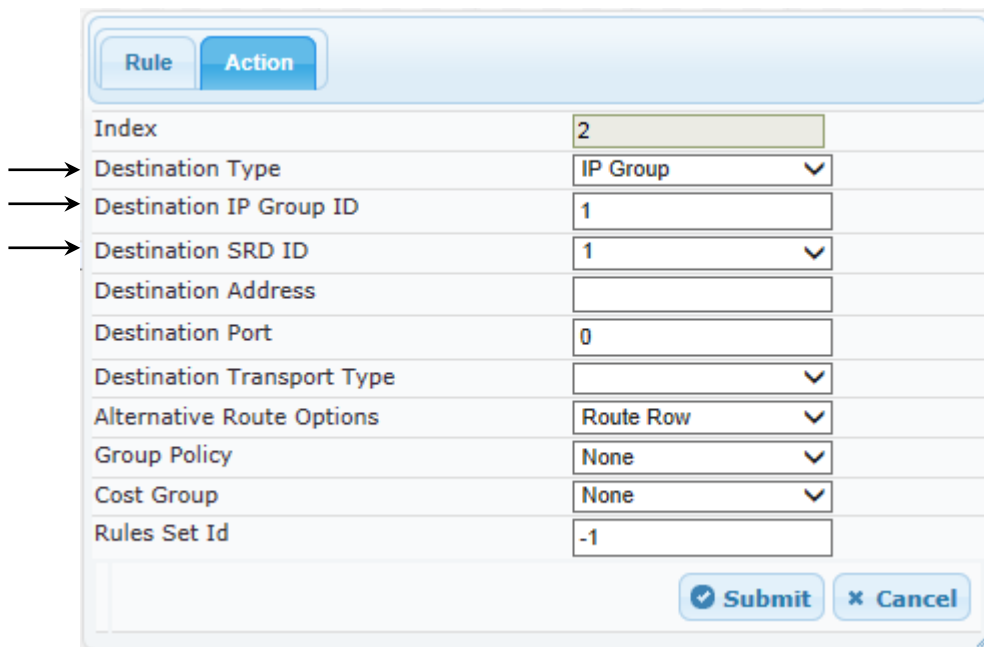
Rule	
Index	2
Route Name	ITSP to Lync
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any

Submit Cancel

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	1
Destination SRD ID	1

Figure 4-34: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab



Rule Action

Index: 2

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

Group Policy: None

Cost Group: None

Rules Set Id: -1

Submit Cancel

The configured routing rules are shown in the figure below:

Figure 4-35: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table

Add + Insert +

Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Destination Type	Destination IP Group ID	Destination Address
0	OPTIONS terminatio	*	*	*	None	-1	Any	Dest Address	-1	internal
1	Lync to ITSP	*	*	*	None	-1	Any	IP Group	2	
2	ITSP to Lync	*	*	*	None	-1	Any	IP Group	1	

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.

4.10 Step 10: 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 46, IP Group 1 represents Lync Server 2013, and IP Group 2 represents tIPicall 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 (tIPicall 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	1
Source IP Group	2
Destination IP Group	1
Destination Username Prefix	* (asterisk sign)

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

The screenshot shows the 'Rule' tab of the configuration form. The fields and their values are as follows:

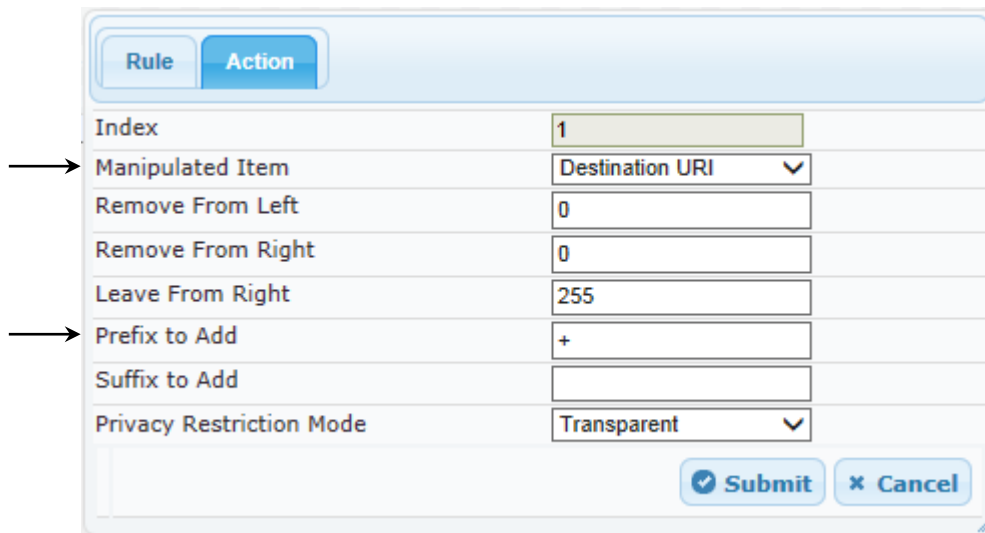
- Index: 1
- Manipulation Name: (empty)
- Additional Manipulation: No
- Source IP Group ID: 2
- Destination IP Group ID: 1
- Source Username Prefix: *
- Source Host: *
- Destination Username Prefix: *
- Destination Host: *
- Calling Name Prefix: *
- Message Condition: None
- Request Type: All
- ReRoute IP Group ID: -1
- Call Trigger: Any

At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

Parameter	Value
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 4-37: 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., tIPicall SIP Trunk):

Figure 4-38: Example of Configured IP-to-IP Outbound Manipulation Rules

IP to IP Outbound Manipulation												
Add + Insert +												
Index	Manipulation Name	Additional Manipulation	Source IP Group ID	Destination IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulated Item	Prefix to Add	Suffix to Add
1		No	2	1	*	*	*	*	All	Destination	+	
2		No	1	2	*	*	+	*	All	Destination		
3		No	1	2	+	*	*	*	All	Source URI		

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

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

4.11 Step 11: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules, including 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).

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

➤ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 1) for Lync Server 2013. This rule applies to messages received from the Lync Server 2013 (IP Group 1), for simultaneous ringing initiated by the Lync Server 2013 (IP Group 1). This adds an Action Value containing the Reason for the History-Info header, causing the E-SBC to add a Diversion Header towards the SIP Trunk.

Parameter	Value
Index	0
Manipulation Set ID	1
Message Type	invite
Condition	header.history-info.0==regex(<.*)(user=phone)(>)(.*)
Action Subject	header.history-info.0
Action Type	Modify
Action Value	\$1+\$2+'?Reason=SIP%3Bcause%3D404'+\$3+\$4

Figure 4-39: Configuring SIP Message Manipulation Rule 0 (for Lync Server 2013)

The screenshot shows the 'Edit Record' dialog box with the following fields and values:

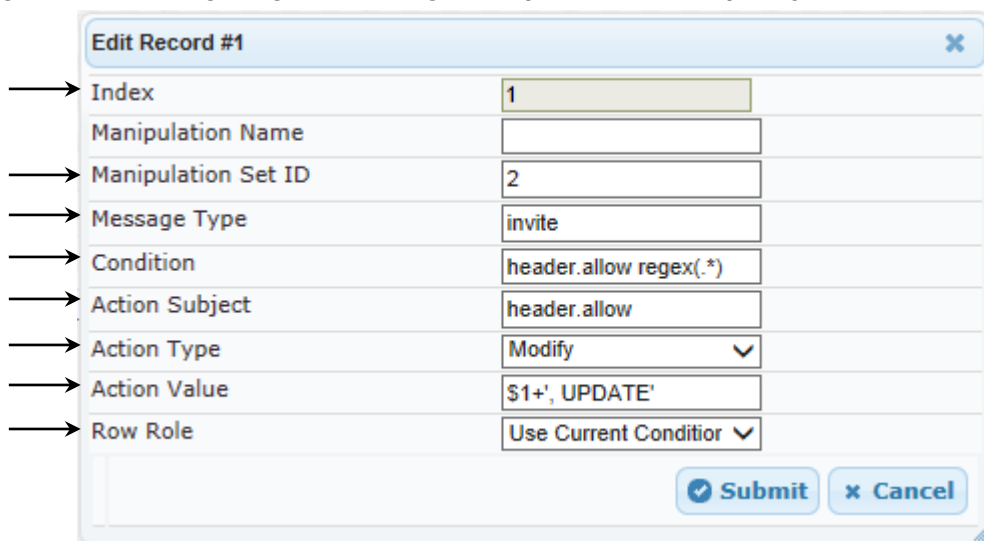
- Index: 0
- Manipulation Set ID: 1
- Message Type: invite
- Condition: header.history-info.0==regex.(
- Action Subject: header.history-info.0
- Action Type: Modify
- Action Value: \$1+\$2+'?Reason=SIP%3Bcause%3D404'+\$3+\$4
- Row Role: Use Current Condition

Buttons at the bottom: Submit, Cancel.

3. The tIPicall SIP Trunk does not support the UPDATE method and therefore does not send it in the INVITE message. In order to “push” Microsoft Lync to send an UPDATE message during the session timer refresh procedure, configure the following manipulation rule (Manipulation Set 2) for Lync Server 2013:

Parameter	Value
Index	1
Manipulation Set ID	2
Message Type	invite
Condition	header.allow regex(.*)
Action Subject	header.allow
Action Type	Modify
Action Value	\$1+', UPDATE'
Row Role	Use Current Condition

Figure 4-40: Configuring SIP Message Manipulation Rule 1 (for Lync Server 2013)



The screenshot shows the 'Edit Record #1' dialog box with the following fields and values:

- Index: 1
- Manipulation Name: (empty)
- Manipulation Set ID: 2
- Message Type: invite
- Condition: header.allow regex(.*)
- Action Subject: header.allow
- Action Type: Modify (dropdown arrow)
- Action Value: \$1+', UPDATE'
- Row Role: Use Current Condition (dropdown arrow)

At the bottom right, there are 'Submit' and 'Cancel' buttons.

4. For this interoperability test topology, manipulation for call forwarding initiated by Lync Server 2013 (i.e., IP Group 1) is required to replace the user part of the SIP From header with the user part of Diversion header. To perform this, configure the following manipulation rule (Manipulation Set 4) for tIPicall SIP Trunk:

Parameter	Value
Index	2
Manipulation Set ID	4
Message Type	any.request
Condition	header.diversion exists
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.diversion.url.user
Row Role	Use Current Condition

Figure 4-41: Configuring SIP Message Manipulation Rule 2 (for tIPicall SIP Trunk)

The screenshot shows a web-based configuration interface for SIP Message Manipulation Rules. The 'Edit Record #2' dialog is open, displaying the following configuration details:

- Index:** 2
- Manipulation Name:** (empty field)
- Manipulation Set ID:** 4
- Message Type:** any.request
- Condition:** header.diversion exists
- Action Subject:** header.from.url.user
- Action Type:** Modify
- Action Value:** header.diversion.url.user
- Row Role:** Use Current Condition

Navigation arrows are visible on the left side of the form, and 'Submit' and 'Cancel' buttons are located at the bottom right.

5. For this interoperability test topology, manipulation for call transfers initiated by Lync Server 2013 (i.e., IP Group 1) is required to replace the user part of the SIP From header with the user part of Referred-By header. To perform this, configure the following manipulation rule (Manipulation Set 4) for tIPicall SIP Trunk:

Parameter	Value
Index	3
Manipulation Set ID	4
Message Type	any.request
Condition	header.referred-by exists
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.referred-by.url.user
Row Role	Use Current Condition

Figure 4-42: Configuring SIP Message Manipulation Rule 3 (for tIPicall SIP Trunk)

Edit Record #3

Index	3
Manipulation Name	
Manipulation Set ID	4
Message Type	any.request
Condition	header.referred-by exists
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.referred-by.url.user
Row Role	Use Current Condition

Submit
Cancel

6. The following rule removes the '+' prefix from the User part in the From Header.

Parameter	Value
Index	4
Manipulation Set ID	4
Message Type	
Condition	
Action Subject	header.from.url.user
Action Type	Remove Prefix
Action Value	'+'
Row Role	Use Current Condition

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

The screenshot shows a web-based configuration interface for editing a SIP message manipulation rule. The window is titled 'Edit Record #4'. It contains several input fields and dropdown menus. The 'Index' field is set to 4. The 'Manipulation Set ID' is also set to 4. The 'Action Subject' is 'header.from.url.user', the 'Action Type' is 'Remove Prefix', and the 'Action Value' is '+'. The 'Row Role' is 'Use Current Condition'. At the bottom right, there are 'Submit' and 'Cancel' buttons.

7. Configure another manipulation rule (Manipulation Set 4) for tIPicall SIP Trunk which accepts calls only from its own users. For dealing with anonymous calls, we added the P-Asserted-Identity Header in SIP Trunk IP Profile. In case of call forwarding, the P-Asserted-Identity Header will contain the call originator number. If so, the following rule is applied to INVITE messages sent to the tIPicall SIP Trunk (IP Group 2) for Forwarded Calls initiated by the Lync Server 2013 (IP Group 1). This will replace the User part of the P-Asserted-Identity Header with the User part of the From Header.

Parameter	Value
Index	5
Manipulation Set ID	4
Message Type	invite.request
Condition	header.from.url !contains 'anonymous'
Action Subject	header.p-asserted-identity.url
Action Type	Modify

Action Value	header.from.url
Row Role	Use Current Condition

Figure 4-44: Configuring SIP Message Manipulation Rule 5 (for tIPicall SIP Trunk)

Edit Record #5

Index	5
Manipulation Name	
Manipulation Set ID	4
Message Type	invite.request
Condition	header.from.url !contains
Action Subject	header.p-asserted-identity
Action Type	Modify
Action Value	header.from.url
Row Role	Use Current Condition

Submit
Cancel

8. Configure another manipulation rule (Manipulation Set 4) for tIPicall SIP Trunk. This rule is applied to response messages sent to the tIPicall SIP Trunk (IP Group 2) for '404 Not Found' or '488 Not Acceptable Here' responses initiated by Lync Server 2013 (IP Group 1). This will replace the method type '404' or '488' with the value '486', because tIPicall SIP Trunk does not recognize '404' and '488' method types.

Parameter	Value
Index	6
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='404' '488'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'486'
Row Role	Use Current Condition

Figure 4-45: Configuring SIP Message Manipulation Rule 6 (for tIPicall SIP Trunk)

Figure 4-46: Configured SIP Message Manipulation Rules

Message Manipulations							
Add + Insert +							
Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0		1	invite	header.history-info.0==regex(<.*)(use	header.history-info.0	Modify	\$1+\$2+'?Reasc
1		2	invite	header.allow regex(<.*)(use	header.allow	Modify	\$1+', UPDATE'
2		4	any.request	header.diversion exists	header.from.url.user	Modify	header.diversion
3		4	any.request	header.referred-by exists	header.from.url.user	Modify	header.referred
4		4			header.from.url.user	Remove Prefix	'+'
5		4	invite.request	header.from.url !contains 'anonymous'	header.p-asserted-id	Modify	header.from.url
6		4	any.response	header.request-uri.methodtype=='404' '488'	header.request-uri.m	Modify	'486'

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

The table displayed below includes SIP message manipulation rules which are bound together by commonality via Manipulation Set IDs 1 and 4, which are executed for messages sent to and from the tIPicall 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 tIPicall 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

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Lync Server 2013 (IP Group 1), for simultaneous ringing initiated by the Lync Server 2013 (IP Group 1). This adds an Action Value containing the Reason for the History-Info header, causing the E-SBC to add a Diversion Header towards the SIP Trunk.	
1	To “push” Microsoft Lync to send an UPDATE message during the Session Timer Refresh procedure , configure Manipulation Set 2 for Lync Server 2013.	tIPicall SIP Trunks do not support the UPDATE method and therefore does not send it in the INVITE message.
2	For this interoperability test topology, manipulation for call forwarding initiated by Lync Server 2013 (i.e., IP Group 1) is required to replace the User part of the From Header with the User part of Diversion Header.	tIPicall SIP Trunks accept calls only from their own users.
3	For this interoperability test topology, manipulation for call transfers initiated by Lync Server 2013 (i.e., IP Group 1) is required to replace User part of the From Header with the User part of Referred-By Header.	
4	This rule removes the ‘+’ prefix from the User part in the From Header.	
5	For dealing with anonymous calls we add the P-Asserted-Identity Header in the tIPicall SIP Trunk IP Profile. In case of call forwarding, the P-Asserted-Identity Header will contain the call originator number. If so, the manipulation rule is applied to INVITE messages sent to the tIPicall SIP Trunk (IP Group 2) for Forwarded Calls initiated by the Lync Server 2013 (IP Group 1). This will replace the User part of the P-Asserted-Identity Header with the User part of the From Header.	
6	This rule is applied to RESPONSE messages sent to the tIPicall SIP Trunk (IP Group 2) for ‘404 Not Found’ or ‘488 Not Acceptable Here’ responses initiated by Lync Server 2013 (IP Group 1). This replaces the ‘404’ or ‘488’ method types with the ‘486’ value.	tIPicall SIP Trunk not recognizes ‘404’ or ‘488’ method type.

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 4-47: Assigning Manipulation Sets 1 and 2 to IP Group 1

The screenshot shows the 'SBC' configuration tab for IP Group 1. The 'Index' field is set to 1. The 'Classify By Proxy Set' dropdown is set to 'Enable'. The 'Max. Number of Registered Users' field is set to -1. The 'Inbound Message Manipulation Set' field is set to 1, and the 'Outbound Message Manipulation Set' field is set to 2. The 'Registration Mode' dropdown is set to 'User Initiates Registration', and the 'Authentication Mode' dropdown is set to 'User Authenticates'. The 'Authentication Method List' field is empty. The 'SBC Client Forking Mode' dropdown is set to 'Sequential'. The 'Source URI Input' and 'Destination URI Input' dropdowns are both set to 'Not Configured'. The 'Username' and 'Password' fields are empty. At the bottom right, there are 'Submit' and 'Cancel' buttons. Two arrows point to the 'Inbound Message Manipulation Set' and 'Outbound Message Manipulation Set' fields.

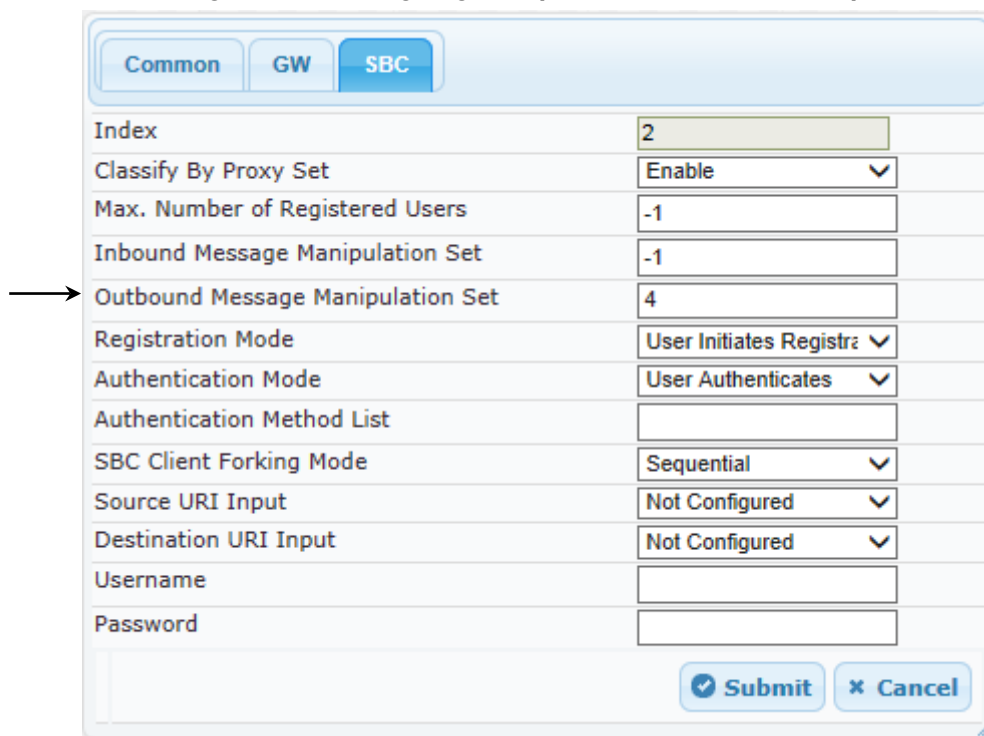
Common GW SBC	
Index	1
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Inbound Message Manipulation Set	1
Outbound Message Manipulation Set	2
Registration Mode	User Initiates Registration
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential
Source URI Input	Not Configured
Destination URI Input	Not Configured
Username	
Password	

Submit Cancel

- 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 4-48: Assigning Manipulation Set 4 to IP Group 2



The screenshot shows the configuration page for IP Group 2, SBC tab. The 'Outbound Message Manipulation Set' field is highlighted with an arrow and set to 4. The 'Index' field is set to 2. The 'Classify By Proxy Set' dropdown is set to 'Enable'. The 'Max. Number of Registered Users' field is set to -1. The 'Inbound Message Manipulation Set' field is set to -1. The 'Registration Mode' dropdown is set to 'User Initiates Registr'. The 'Authentication Mode' dropdown is set to 'User Authenticates'. The 'Authentication Method List' field is empty. The 'SBC Client Forking Mode' dropdown is set to 'Sequential'. The 'Source URI Input' dropdown is set to 'Not Configured'. The 'Destination URI Input' dropdown is set to 'Not Configured'. The 'Username' and 'Password' fields are empty. The 'Submit' and 'Cancel' buttons are at the bottom right.

Field	Value
Index	2
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	4
Registration Mode	User Initiates Registr
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential
Source URI Input	Not Configured
Destination URI Input	Not Configured
Username	
Password	

- e. Click **Submit**.

4.12 Step 12: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

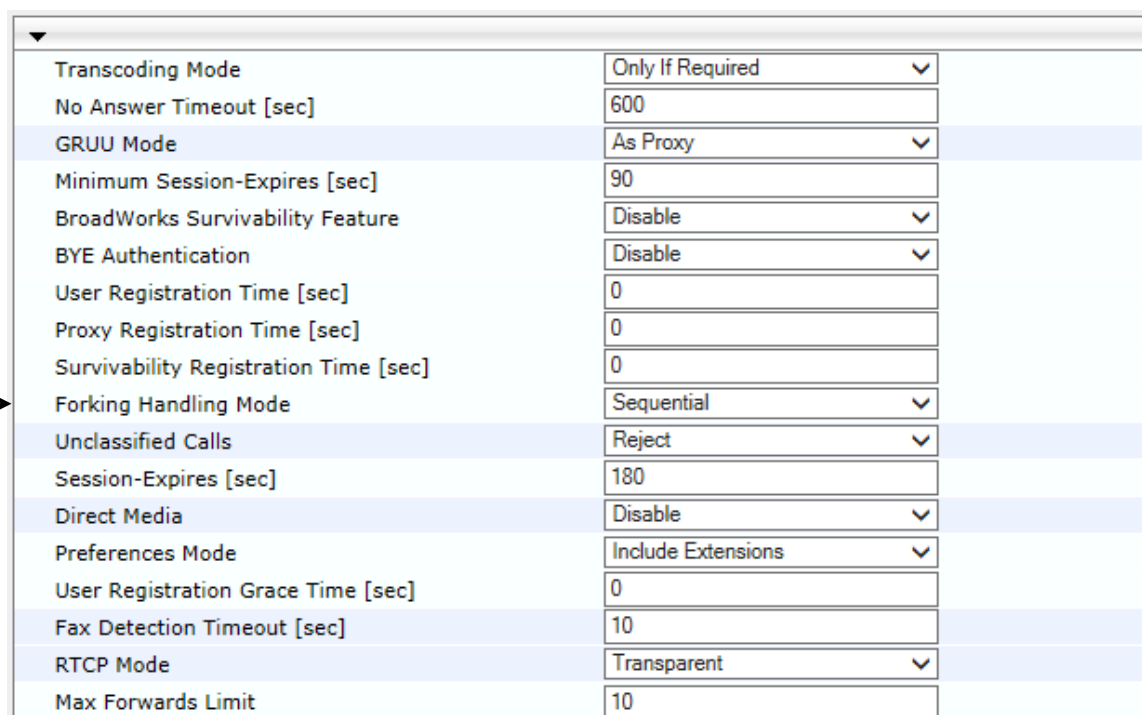
4.12.1 Step 12a: Configure Call Forking Mode

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 the 18x response 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 4-49: Configuring Forking Mode



The screenshot shows the 'General Settings' page for the E-SBC. The 'Forking Handling Mode' is set to 'Sequential'. An arrow points to this setting from the left. The table below represents the data visible in the screenshot.

Transcoding Mode	Only If Required
No Answer Timeout [sec]	600
GRUU Mode	As Proxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
BYE Authentication	Disable
User Registration Time [sec]	0
Proxy Registration Time [sec]	0
Survivability Registration Time [sec]	0
Forking Handling Mode	Sequential
Unclassified Calls	Reject
Session-Expires [sec]	180
Direct Media	Disable
Preferences Mode	Include Extensions
User Registration Grace Time [sec]	0
Fax Detection Timeout [sec]	10
RTCP Mode	Transparent
Max Forwards Limit	10

3. Click **Submit**.

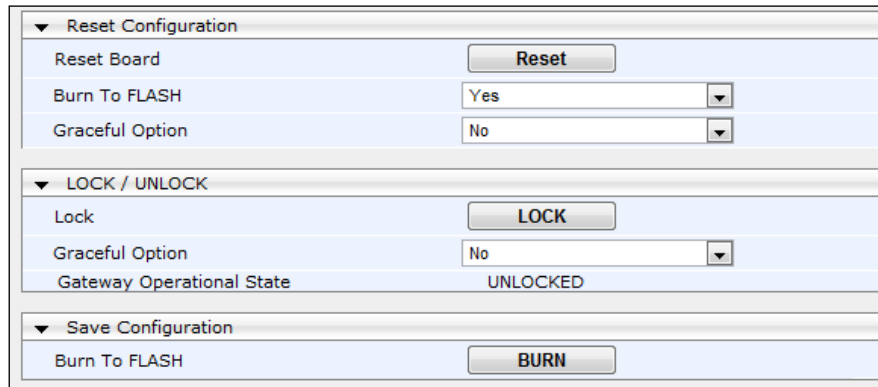
4.13 Step 13: Reset the E-SBC

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 4-50: Resetting the E-SBC



The screenshot shows a web-based configuration interface for an E-SBC. It is divided into three main sections:

- Reset Configuration:** Contains a "Reset Board" button, a "Burn To FLASH" dropdown menu set to "Yes", and a "Graceful Option" dropdown menu set to "No".
- LOCK / UNLOCK:** Contains a "Lock" button, a "Graceful Option" dropdown menu set to "No", and a "Gateway Operational State" label showing "UNLOCKED".
- Save Configuration:** Contains a "Burn To FLASH" button labeled "BURN".

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

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 33, 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 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 2265355
;Slot Number: 1
;Software Version: SIP_F6.80A.009.005
;DSP Software Version: 5014AE3_R => 680.17
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M  Flash size: 64M  Core speed: 300Mhz
;Num of DSP Cores: 3  Num DSP Channels: 62
;Num of physical LAN ports: 12
;Profile: NONE
;Key features;;Board Type: 72 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;System features: POE-
AF ;DSP Voice features: IpmDetector RTCP-XR AMRPolicyManagement ;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
;QOE features: VoiceQualityMonitoring MediaEnhancement ;Channel Type: RTP
DspCh=62 IPMediaDspCh=62 ;PSTN FALLBACK Supported ;E1Trunks=2 ;T1Trunks=2
;FXSPorts=4 ;FXOPorts=4 ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;Control Protocols: MGCP MEGACO H323 SIP TPNCP
SASurvivability SBC=60 MSFT CLI TRANSCODING=60 FEU=60 TestCall=60
SIPRec=60 CODER-TRANSCODING=60 EMS SBC-SIGNALING=60 SBC-MEDIA=60 ;Default
features;;Coders: G711 G726;

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

[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value

```

```
NTPServerIP = '10.15.25.1'

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

FarEndDisconnectType = 7

[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
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'Tipicall'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value

[SIP Params]

GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
```



```

SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[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 4 = "FE_5_1", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 1, 4, "User Port #11", "GROUP_6",
"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 2 = "GROUP_3", 2, "FE_5_1", "FE_5_2";
EtherGroupTable 3 = "GROUP_4", 2, "FE_5_3", "FE_5_4";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";

```

```

EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName;
DeviceTable 0 = 1, "GROUP_1", "vlan 1";
DeviceTable 1 = 2, "GROUP_2", "vlan 2";

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.153, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 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_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 10, 6090, 1, "", "";
CpMediaRealm 1 = "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 = "tartarus.tipicall.net", -1, 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_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,  
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,  
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,  
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,  
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,  
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,  
IpProfile_SBCDiversionsMode, 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_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,  
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,  
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,  
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,  
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,  
IpProfile_SBCJitterCompensation,
```

```

IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;
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, -1, 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 3, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 2, 0, 0, 0,
0, 300;
IpProfile 2 = "Tipicall", 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, -1, 0,
2, 0, 0, 1, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 0, 0, 2, 0, 3, 0, 1,
0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 300;

[ \IpProfile ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode,
ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, -1, -1, "";
ProxySet 1 = "Lync", 1, 60, 1, 1, 1, 0, -1, -1, "";
ProxySet 2 = "Tipicall", 1, 60, 0, 1, 2, 0, -1, -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_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "Lync", 1, "tartarus.tipicall.net", "", 0, -1, -1, 0, -1,
1, "MRlan", 1, 1, -1, 1, 2, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "";
IPGroup 2 = 0, "Tipicall", 2, "tartarus.tipicall.net", "", 0, -1, -1, 0,
-1, 2, "MRwan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==",
0, "", "", "", 0, "", "";

[ \IPGroup ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,

```

```

IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS termination", 1, "*", "*", "*", "*", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "Lync to ITSP", 1, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 2, "", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to Lync", 2, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 1, "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPSPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 1 = "Lync", "Voice", 2, 0, 0, 5067, 1, "", -1, 0, 500;
SIPInterface 2 = "Tipicall", "WANSP", 2, 5060, 0, 0, 2, "", -1, 0, 500;

[ \SIPInterface ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
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, "*", "*", "+", "*", "*", "", 0, -
1, 0, 1, 3, 0, 255, "00", "", 0;
IPOutboundManipulation 3 = "", 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, 1;

[ \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 ]

[ AllowedCodersGroup1 ]

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

[ \AllowedCodersGroup1 ]

[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";

[ \AllowedCodersGroup2 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "", 1, "invite", "header.history-
info.0==regex.(<.*)(user=phone)(>)(.*)", "header.history-info.0", 2,
"$1+$2+'?Reason=SIP%3Bcause%3D404'+$3+$4", 0;
MessageManipulations 1 = "", 2, "invite", "header.allow regex(.*)",
"header.allow", 2, "$1+', UPDATE'", 0;
MessageManipulations 2 = "", 4, "any.request", "header.diversion exists",
"header.from.url.user", 2, "header.diversion.url.user", 0;
MessageManipulations 3 = "", 4, "any.request", "header.referred-by
exists", "header.from.url.user", 2, "header.referred-by.url.user", 0;
```

```
MessageManipulations 4 = "", 4, "", "", "header.from.url.user", 6, "'+'",
0;
MessageManipulations 5 = "", 4, "invite.request", "header.from.url
!contains 'anonymous'", "header.p-asserted-identity.url", 2,
"header.from.url", 0;
MessageManipulations 6 = "", 4, "any.response", "header.request-
uri.methodtype=='404'/'488'", "header.request-uri.methodtype", 2,
"'486'", 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

B Configuring Transcoding from G.729 to G.711

The following describes how to configure transcoding from G.729 to G.711.

B.1 Step 1: 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 necessary **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 4-51: 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 4.13 on page 78).

B.2 Step 2: 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 tIPicall 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 tIPicall SIP Trunk.



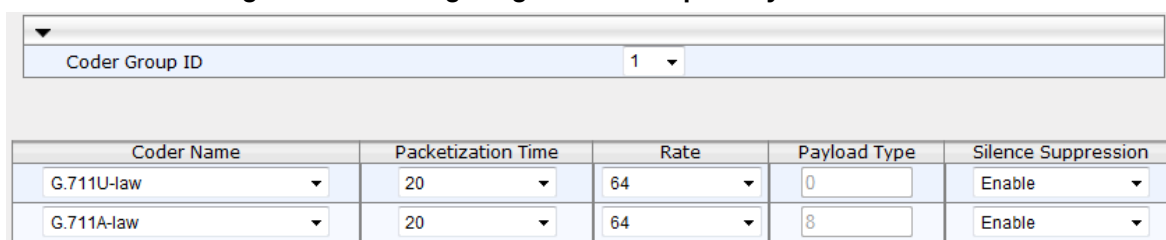
Note: The Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➤ **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 4-52: Configuring Coder Group for Lync Server 2013

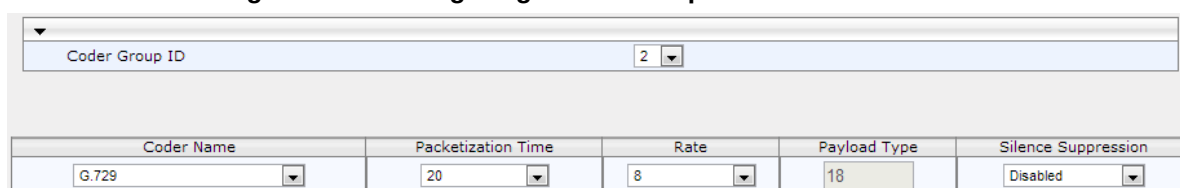


Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-law	20	64	0	Enable
G.711A-law	20	64	8	Enable

3. Configure a Coder Group for tIPicall SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	G.729

Figure 4-53: Configuring Coder Group for tIPicall 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 tIPicall SIP Trunk uses the G.729 coder whenever possible.



Note: This Allowed Coders Group ID will be assigned to the IP Profile belonging to the tIPicall SIP Trunk in the next step.

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

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

Parameter	Value
Allowed Coders Group ID	1
Coder Name	G.711 A-law
Coder Name	G.711 U-law

Figure 4-54: Configuring Allowed Coders Group for tIPicall SIP Trunk

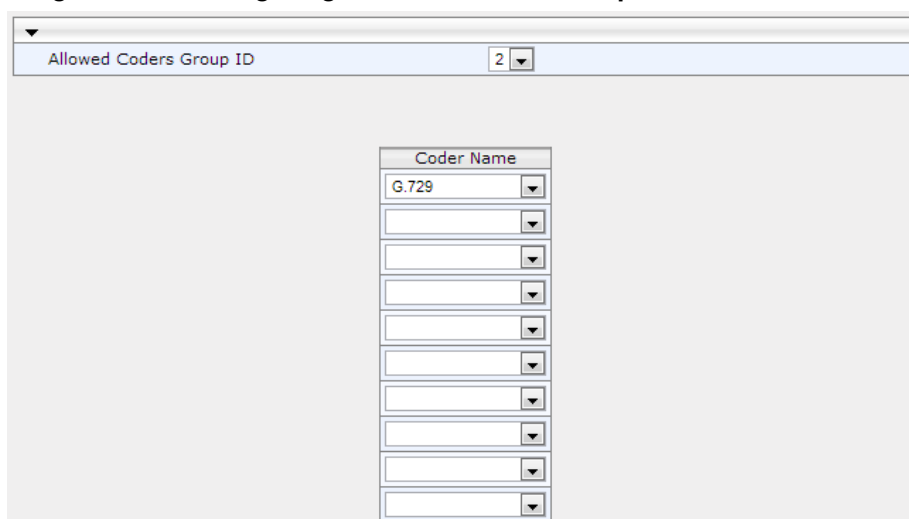
3. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).

➤ **To set a preferred coder for the tIPicall SIP Trunk:**

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

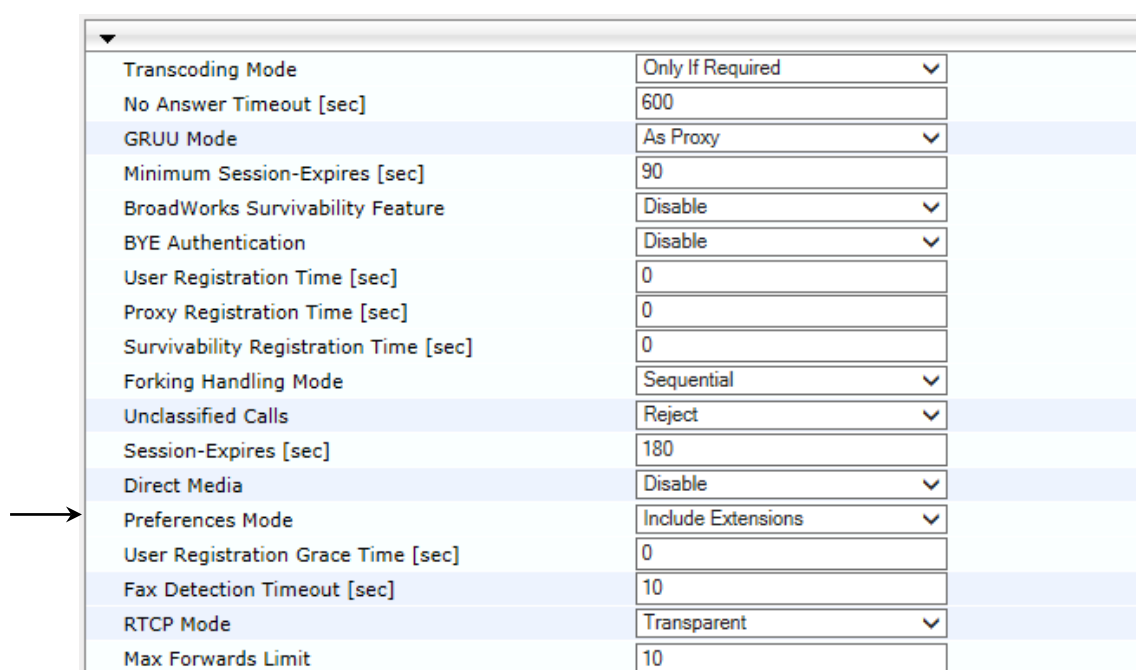
Parameter	Value
Allowed Coders Group ID	2
Coder Name	G.729

Figure 4-55: Configuring Allowed Coders Group for tIPicall SIP Trunk



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

Figure 4-56: SBC Preferences Mode



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

B.3 Step 3: Configure Coders in the IP Profiles

This step describes how to configure defined in the previous step coders in the IP Profiles.

➤ **To configure Coders in the IP Profiles:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Edit** on Lync Profile.
3. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Extension Coders Group ID	Coders Group 1
Allowed Coders Group ID	Coders Group 1
Allowed Coders Mode	Restriction (lists Allowed Coders first and then original coders in received SDP offer)

Figure 4-57: Configuring Coders in IP Profile for Lync Server 2013 – SBC Tab

Common GW SBC	
Index	1
Extension Coders Group ID	Coders Group 1
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	Coders Group 1
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction

4. Configure an IP Profile for the tIPicall SIP Trunk:
5. Click **Edit** on tIPicall Profile.
6. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Restriction (lists Allowed Coders first and then original coders in received SDP offer)

Figure 4-58: Configuring IP Profile for tIPicall SIP Trunk – Common Tab

Common GW SBC	
Index	2
Extension Coders Group ID	Coders Group 2
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	Coders Group 2
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction



Configuration Note