

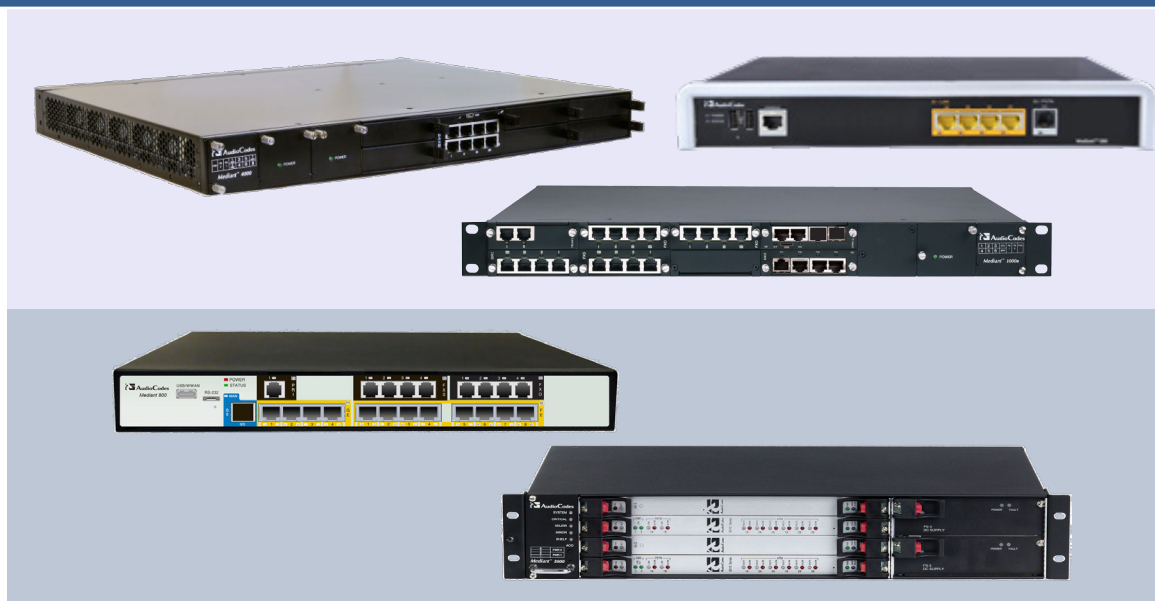
Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

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



Microsoft Partner
Gold Communications



Version 6.8

December 2014

Document # LTRT-12360

Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	NextGenTel SIP Trunking Version.....	9
2.3	Microsoft Lync Server 2013 Version	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitation	11
3	Configuring Lync Server 2013	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway	13
3.2	Configuring the "Route" on Lync Server 2013.....	21
4	Configuring AudioCodes E-SBC.....	31
4.1	Step 1: IP Network Interfaces Configuration	32
4.1.1	Step 1a: Configure VLANs.....	33
4.1.2	Step 1b: Configure Network Interfaces.....	33
4.1.3	Step 1c: Configure the Native VLAN ID.....	35
4.2	Step 2: Enable the SBC Application	35
4.3	Step 3: Signaling Routing Domains Configuration	36
4.3.1	Step 3a: Configure Media Realms.....	36
4.3.2	Step 3b: Configure SRDs	38
4.3.3	Step 3c: Configure SIP Signaling Interfaces	40
4.4	Step 4: Configure Proxy Sets	41
4.5	Step 5: Configure IP Groups.....	44
4.6	Step 6: Configure IP Profiles	46
4.7	Step 7: Configure Coders	53
4.8	Step 8: SIP TLS Connection Configuration.....	54
4.8.1	Step 8a: Configure the NTP Server Address.....	54
4.8.2	Step 8b: Configure a Certificate	55
4.9	Step 9: Configure SRTP	60
4.10	Step 10: Configure Maximum Media Channels.....	61
4.11	Step 11: Configure IP-to-IP Call Routing Rules	62
4.12	Step 12: Configure IP-to-IP Manipulation Rules.....	68
4.13	Step 13: Configure Message Manipulation Rules	70
4.14	Step 14: Miscellaneous Configuration.....	82
4.14.1	Step 14a: Configure Call Forking Mode	82
4.14.2	Step 14b: Configure SBC Session Refreshing Policy	83
4.15	Step 15: Reset the E-SBC	84
A	AudioCodes INI File	85

This page is intentionally left blank.

Notice

This document describes how to connect the Microsoft Lync Server 2013 and NextGenTel SIP Trunk using AudioCodes Mediant E-SBC product series, which includes the Mediant 500 E-SBC, 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 2014 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: December-11-2014

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

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

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and NextGenTel Partners who are responsible for installing and configuring NextGenTel'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.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none">▪ Mediant 500 E-SBC▪ Mediant 800 Gateway & E-SBC▪ Mediant 1000B Gateway & E-SBC▪ Mediant 3000 Gateway & E-SBC▪ Mediant 2600 E-SBC▪ Mediant 4000 E-SBC
Software Version	SIP_6.80A.250.001
Protocol	<ul style="list-style-type: none">▪ SIP/UDP or SIP/TCP (to the NextGenTel SIP Trunk)▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 NextGenTel SIP Trunking Version

Table 2-2: NextGenTel Version

Vendor/Service Provider	NextGenTel
SSW Model/Service	Asterisk PBX
Software Version	1.8.7.0
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

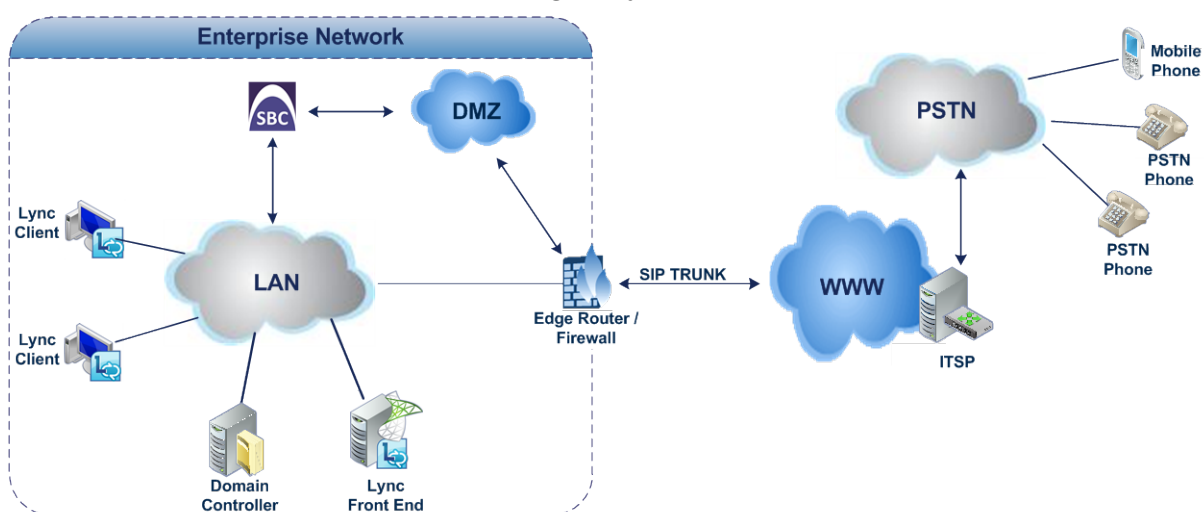
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and NextGenTel 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 NextGenTel'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 NextGenTel'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 NextGenTel SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN▪ NextGenTel SIP Trunk is located on the WAN
Signaling Transcoding	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type▪ NextGenTel SIP Trunk operates with SIP-over-UDP or SIP-over-TCP transport type
Codecs Transcoding	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders▪ NextGenTel SIP Trunk supports G.711A-law coder only
Media Transcoding	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 operates with SRTP media type▪ NextGenTel SIP Trunk operates with RTP media type

2.4.2 Known Limitation

The following limitation was observed in the interoperability tests performed for AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and NextGenTel SIP Trunk:

- Fax support is optional and is not a guaranteed service by the NextGenTel SIP Trunk.

This page is intentionally left blank.

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.

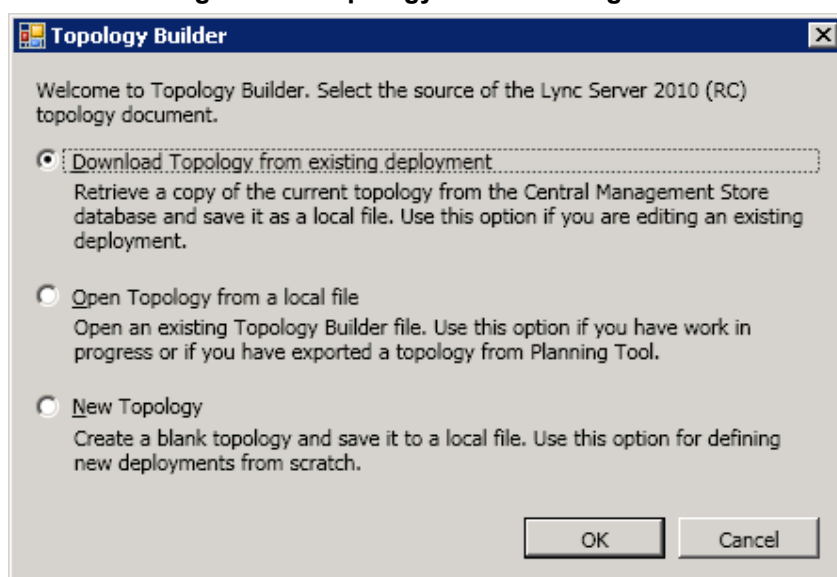
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



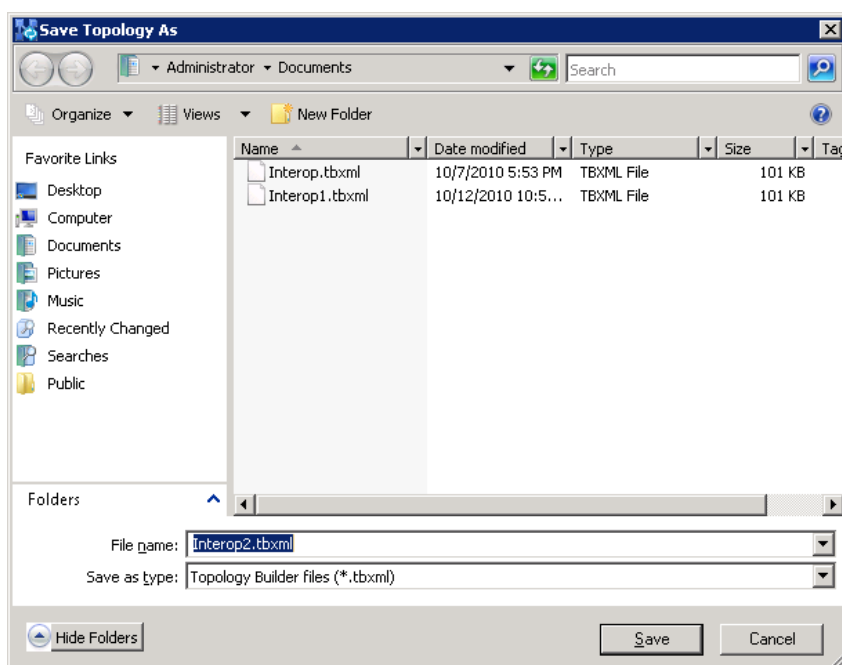
The following is displayed:

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:

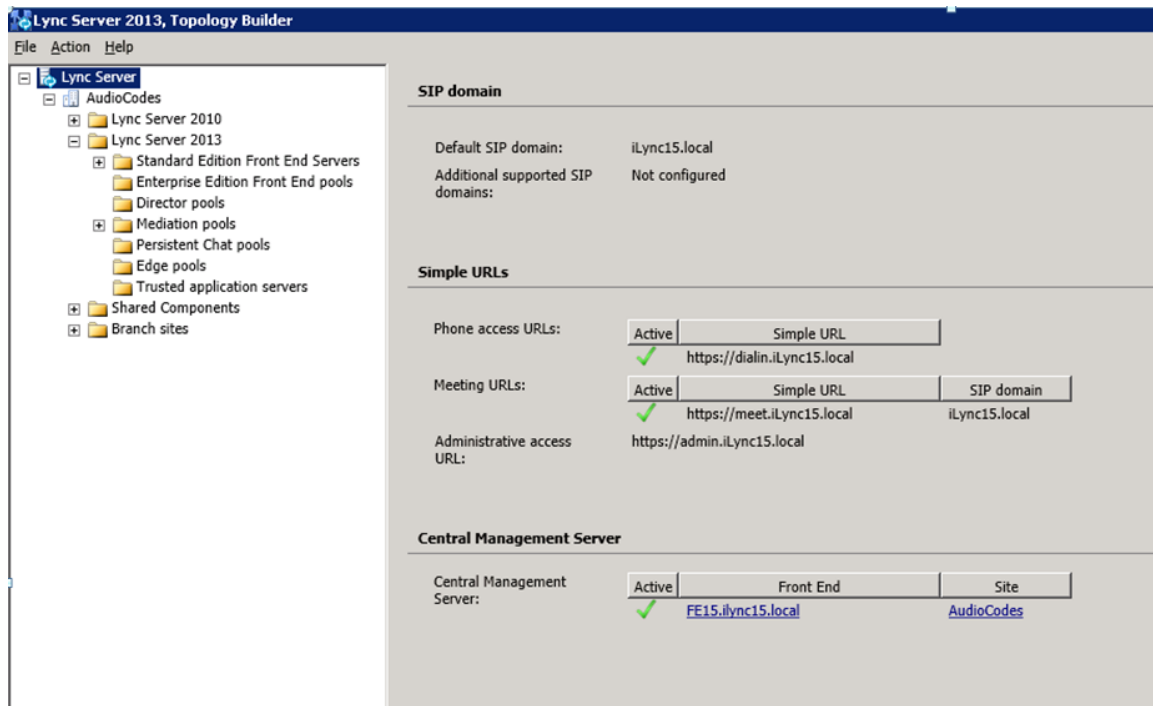
Figure 3-3: Save Topology Dialog Box



- 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.

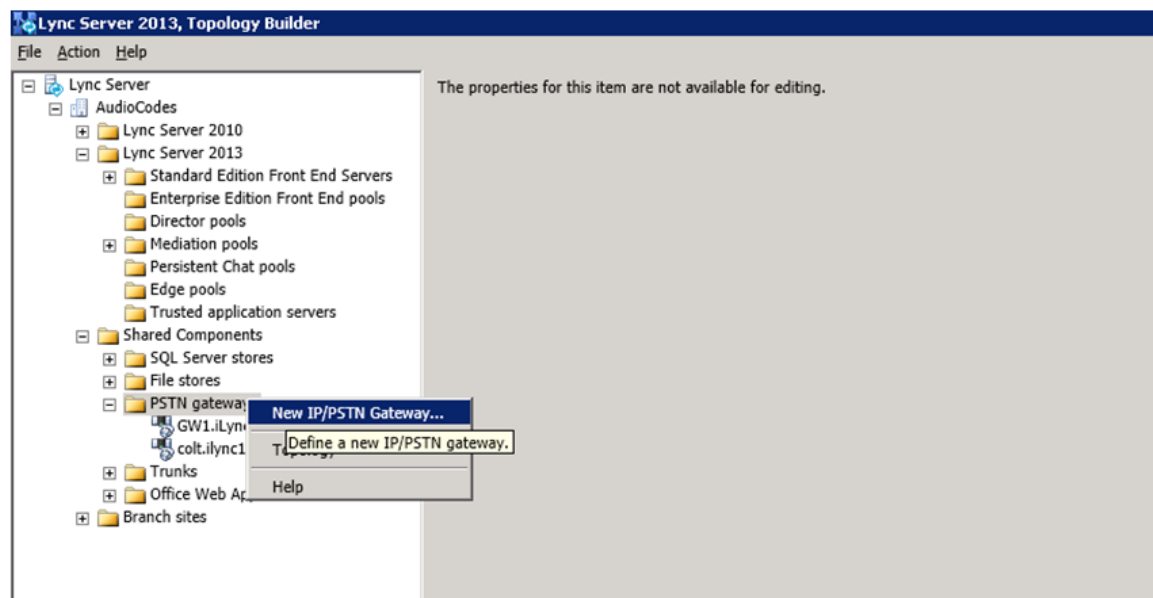
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



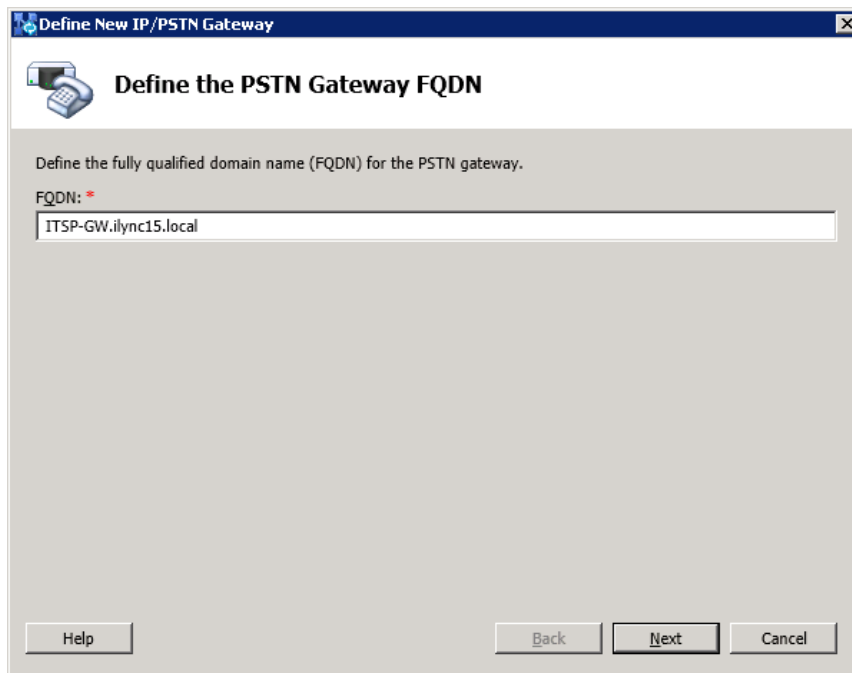
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

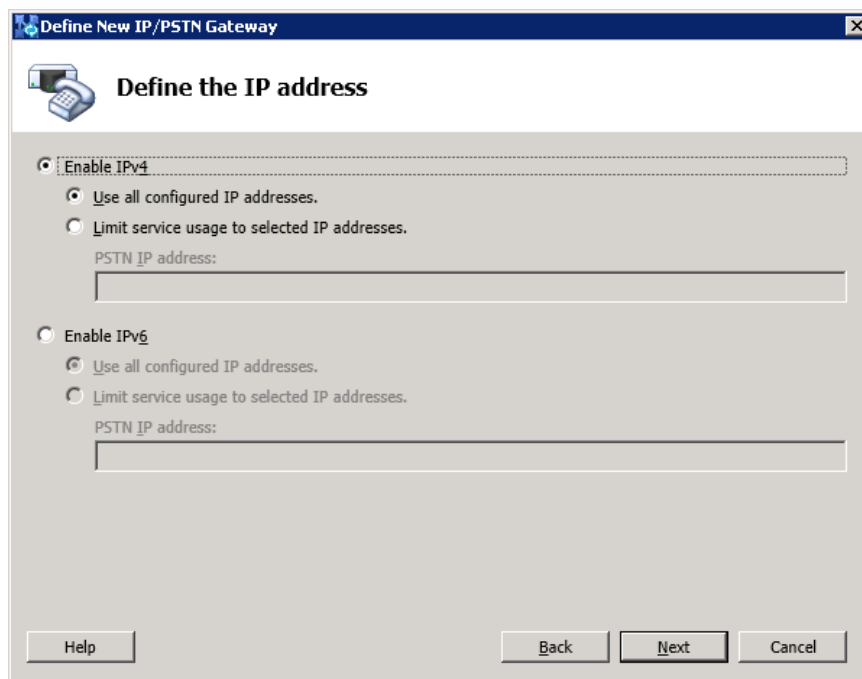
Figure 3-6: Define the PSTN Gateway FQDN



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" and "Enable IPv6". Under "Enable IPv4", there are two sub-options: "Use all configured IP addresses." (selected) and "Limit service usage to selected IP addresses." (unselected). Below these is a text box labeled "PSTN IP address:". The "Enable IPv6" section is also present but not selected. 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 New IP/PSTN Gateway

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

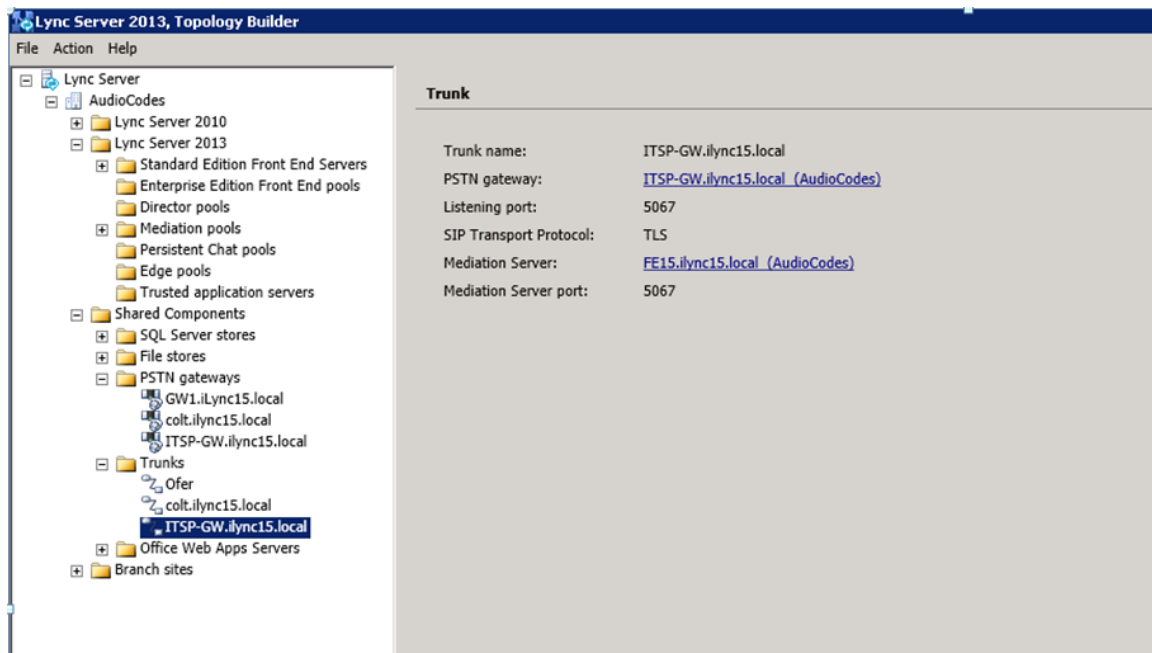
Associated Mediation Server port: *
5067

Help Back Finish Cancel

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

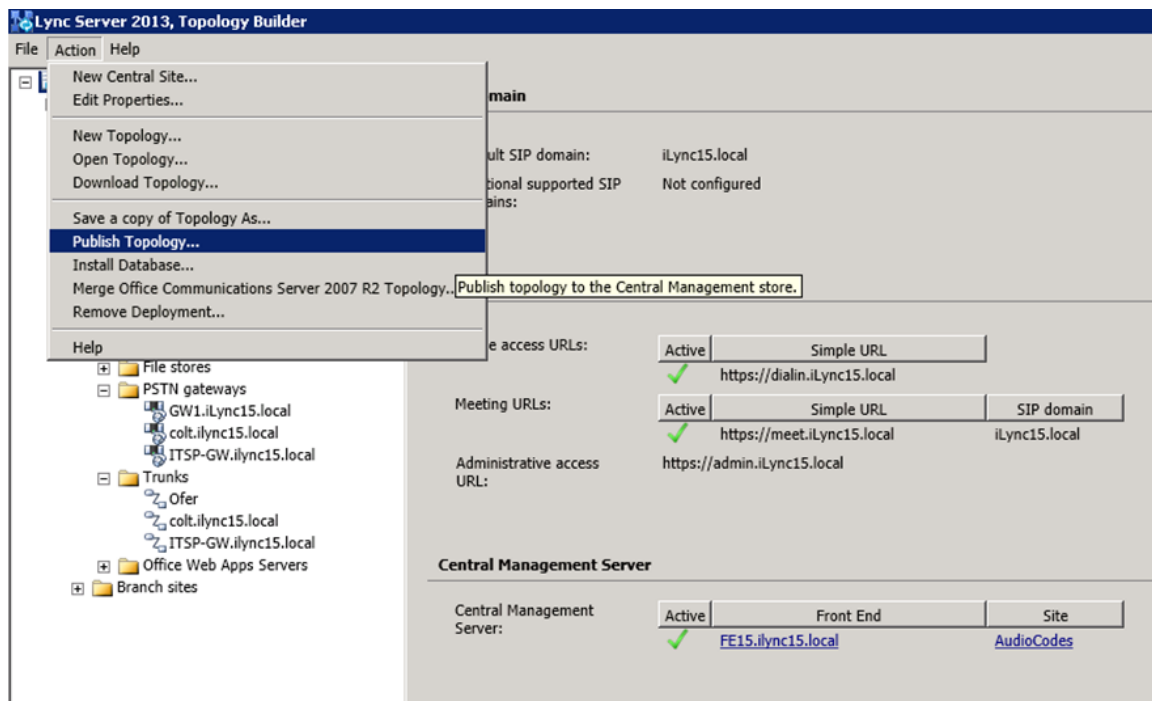
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



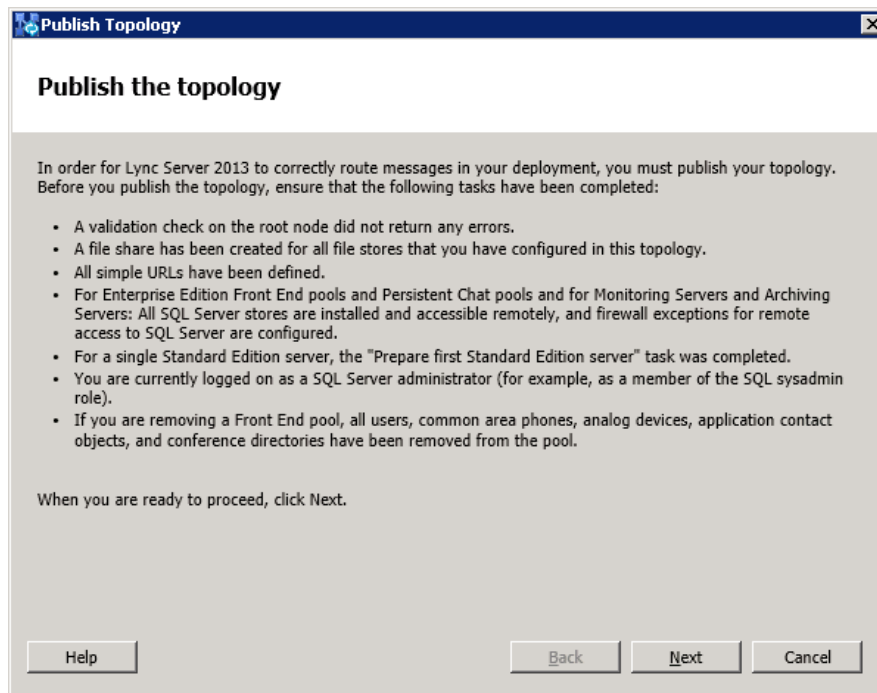
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



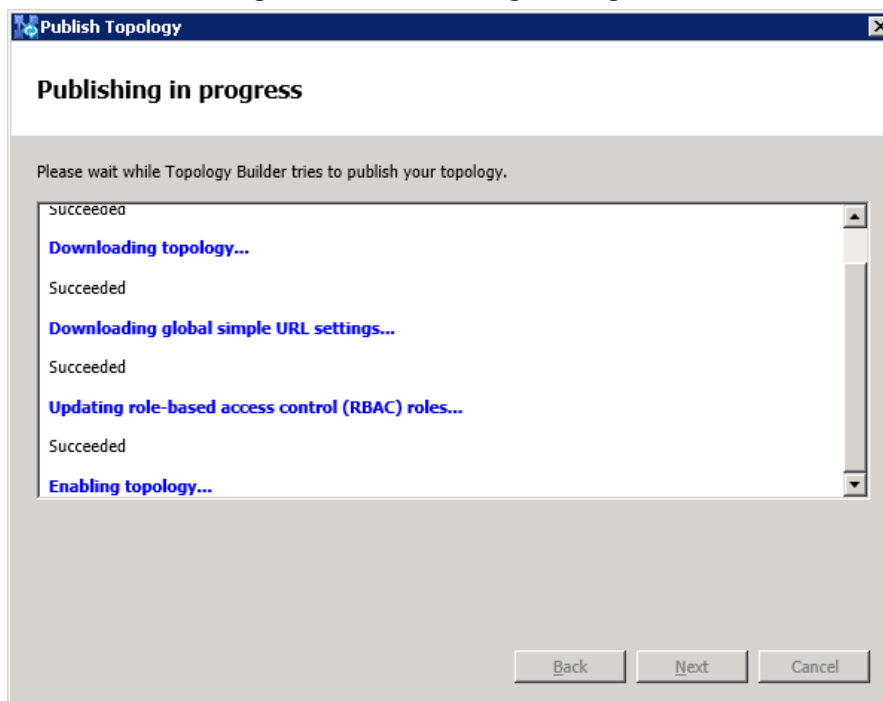
The following is displayed:

Figure 3-11: Publish the Topology



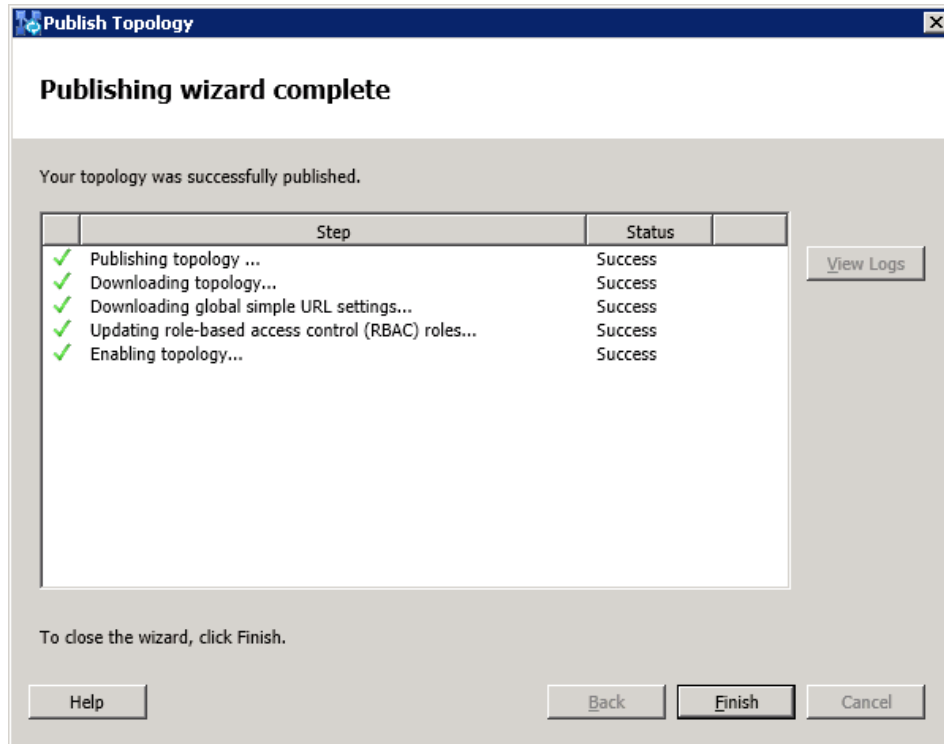
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

The procedure below describes how to configure a "Route" on the Lync Server 2013 and to associate it with the E-SBC PSTN gateway.

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

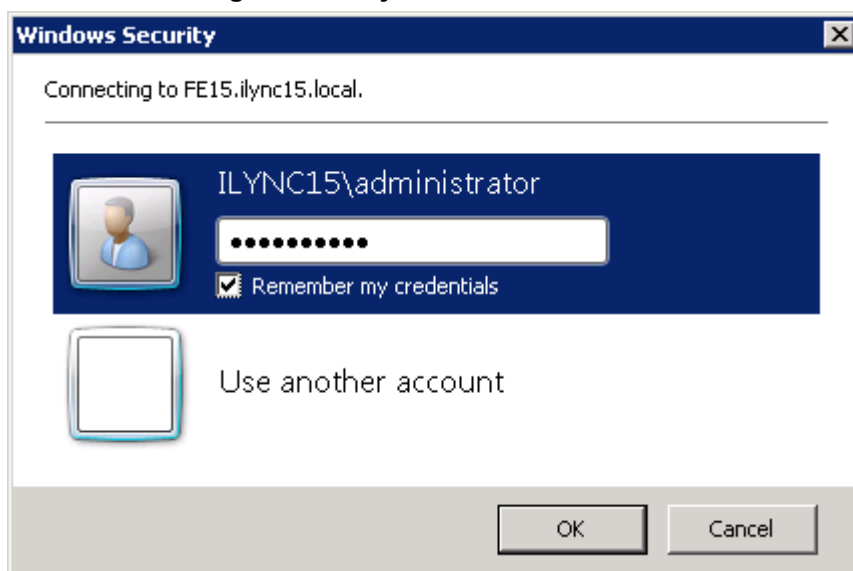
1. Start the Microsoft Lync Server 2013 Control Panel (**Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel



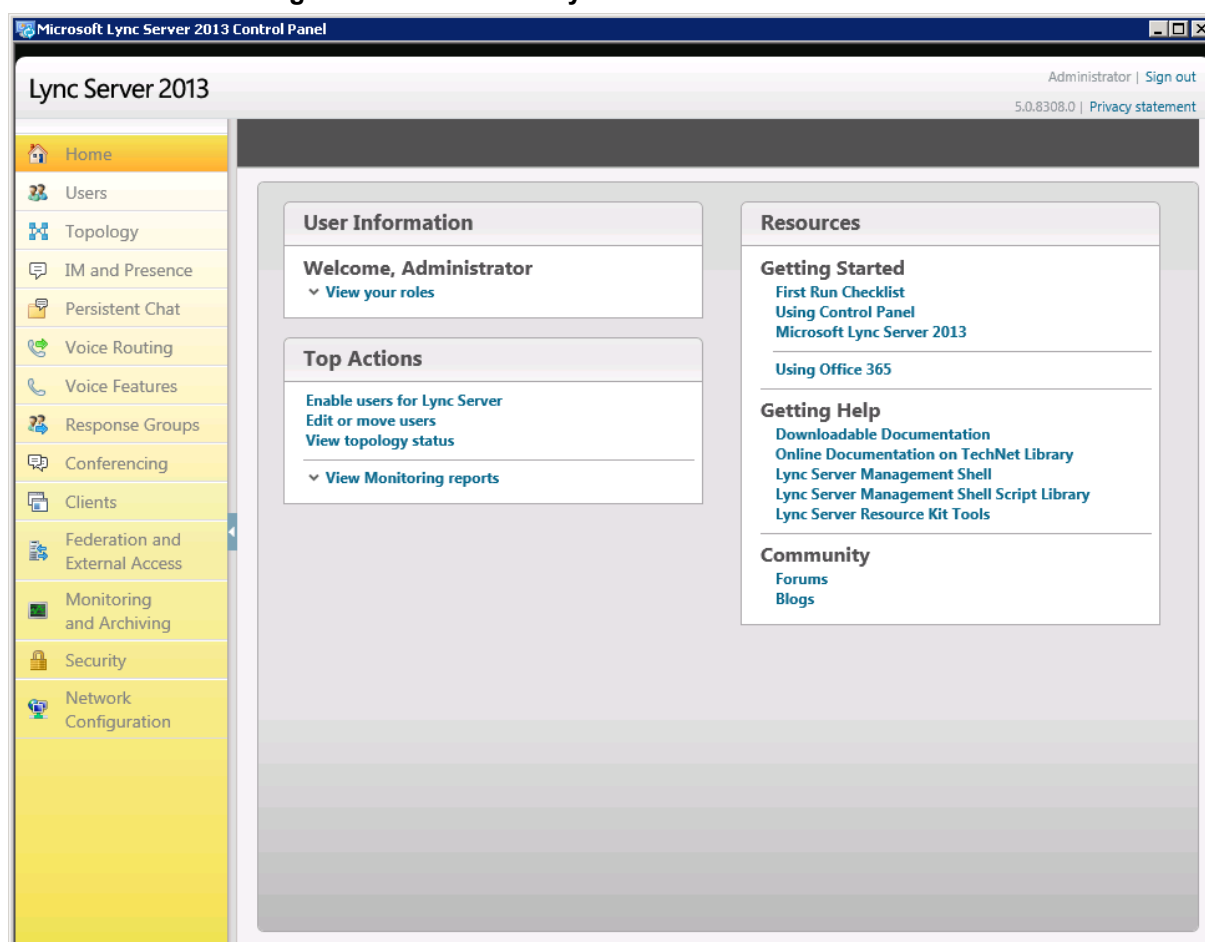
You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



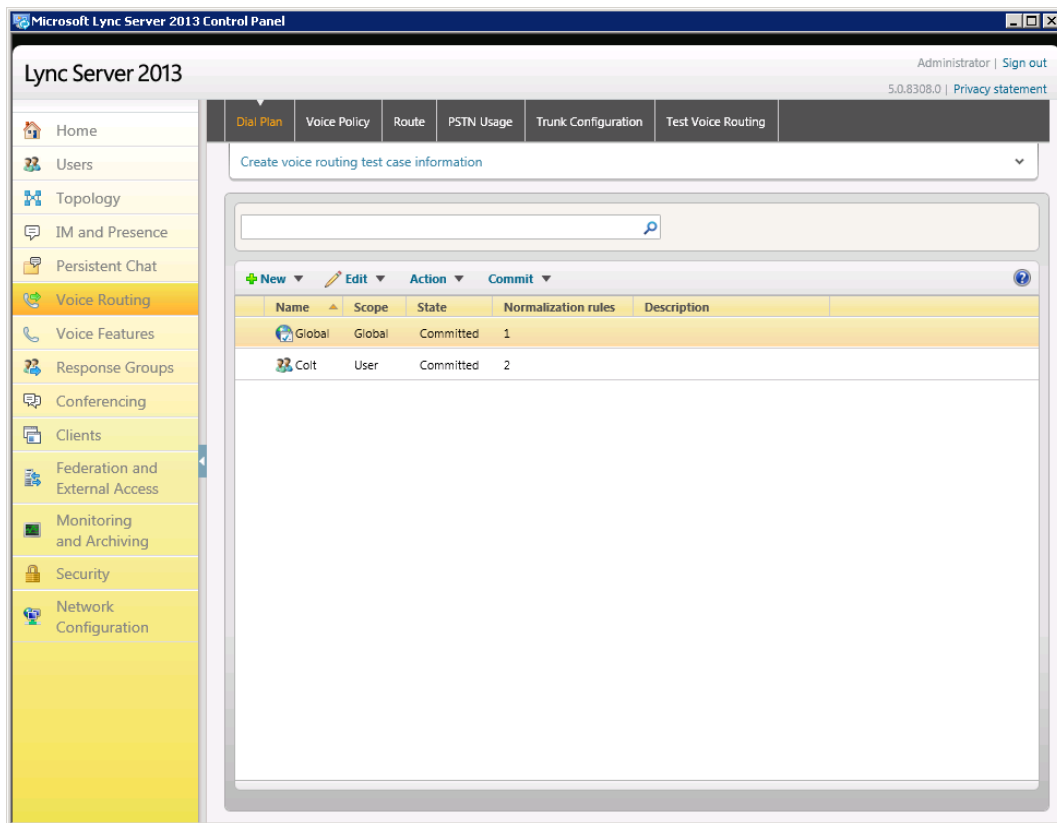
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



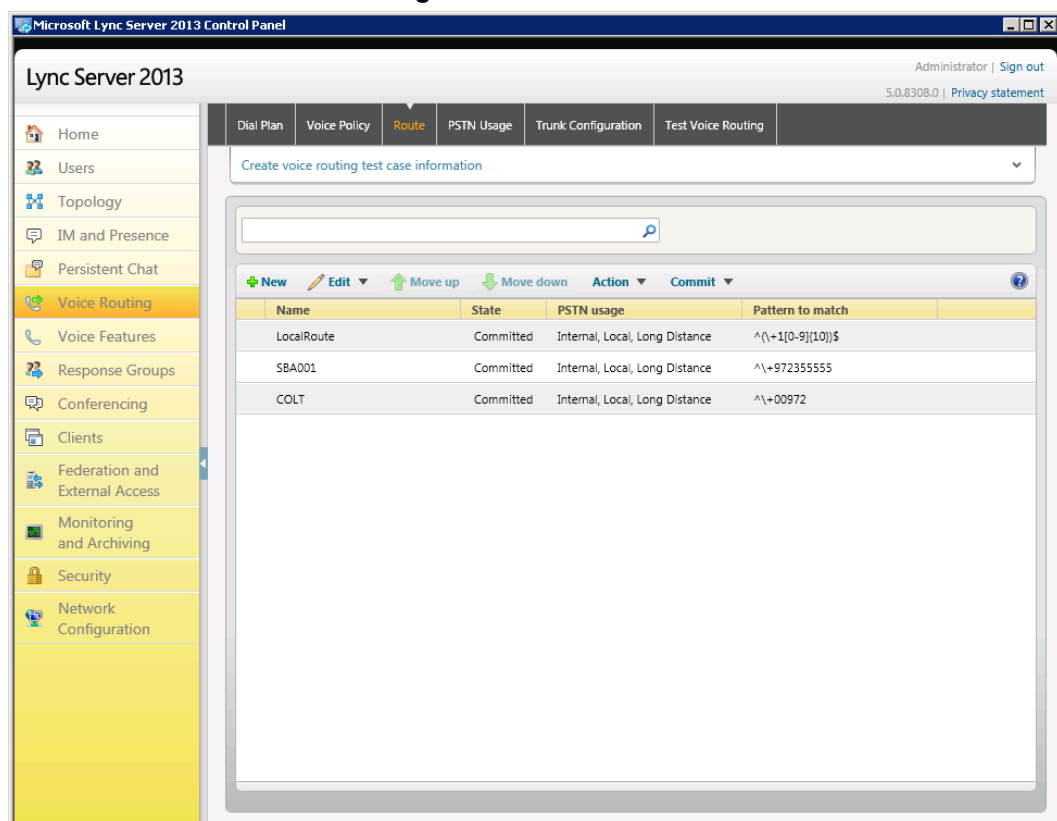
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



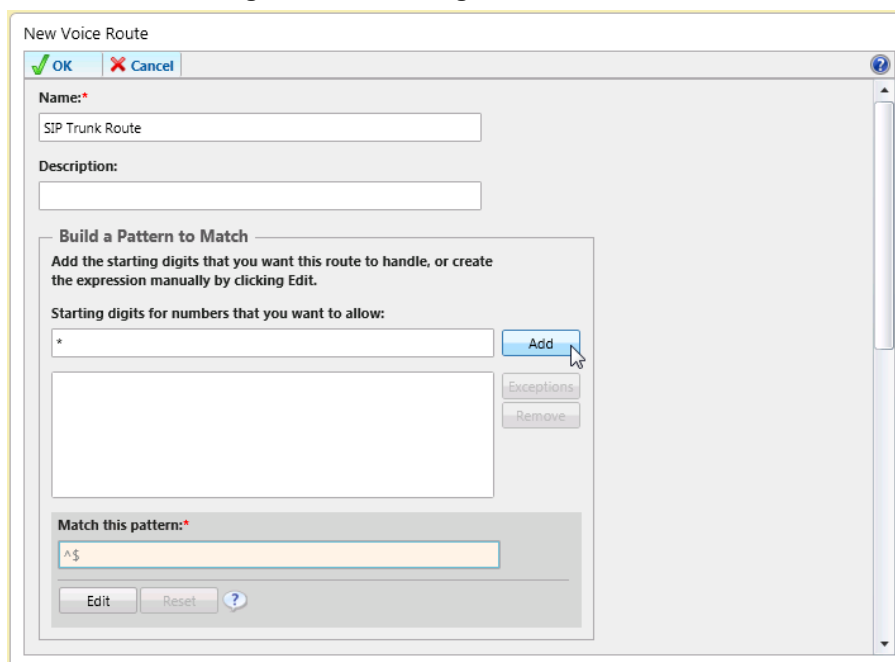
4. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



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

Figure 3-19: Adding New Voice Route



New Voice Route

OK Cancel

Name:*

SIP Trunk Route

Description:

Build a Pattern to Match

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

Starting digits for numbers that you want to allow:

* Add

Exceptions

Remove

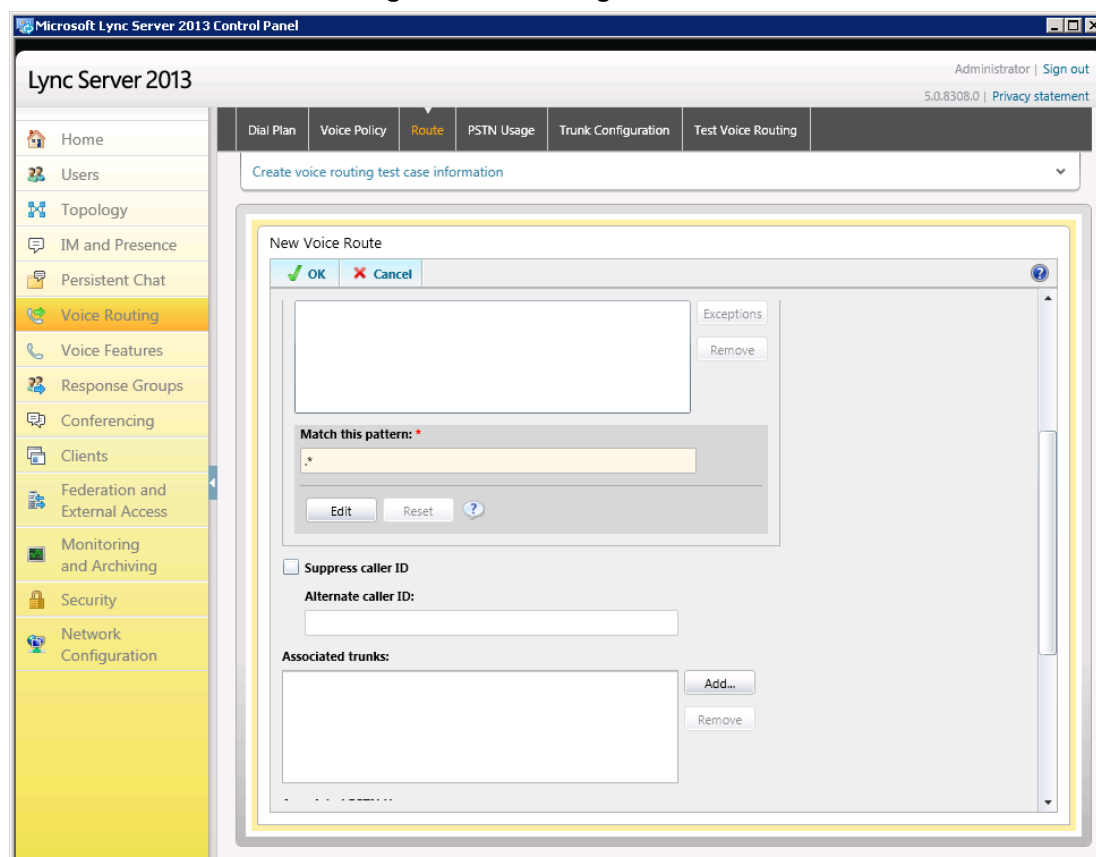
Match this pattern:*

^\$

Edit Reset ?

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

Figure 3-20: Adding New Trunk



Microsoft Lync Server 2013 Control Panel

Lync Server 2013

Administrator | Sign out

5.0.8308.0 | Privacy statement

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

Create voice routing test case information

New Voice Route

OK Cancel

Exceptions

Remove

Match this pattern:*

*

Edit Reset ?

☐ Suppress caller ID

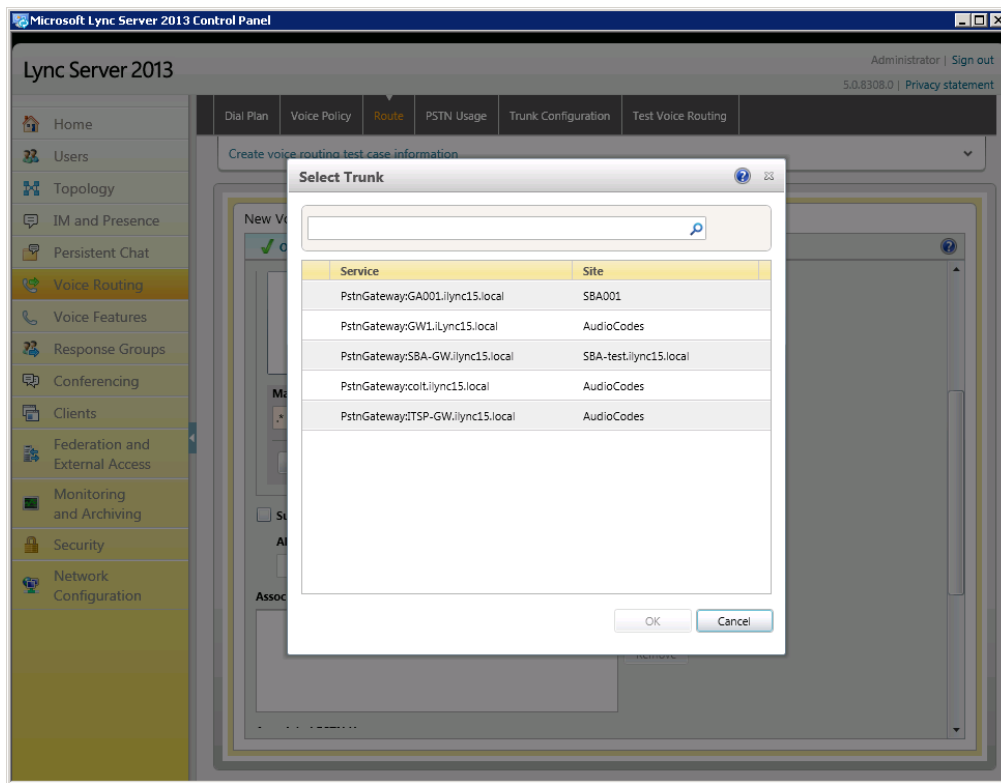
Alternate caller ID:

Associated trunks:

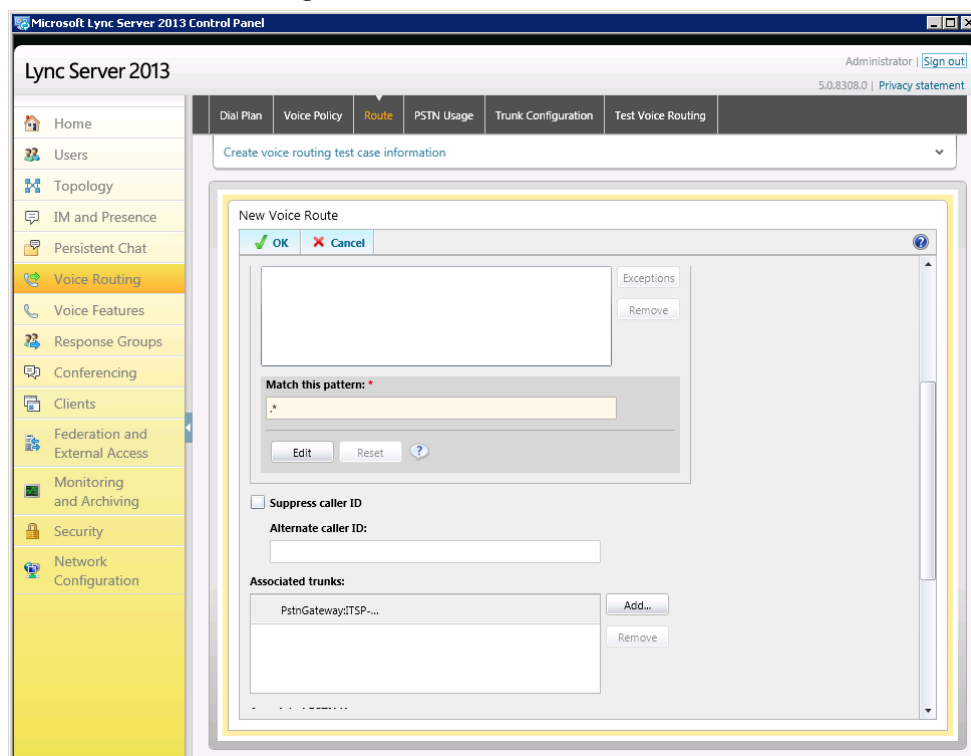
Add...

Remove

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

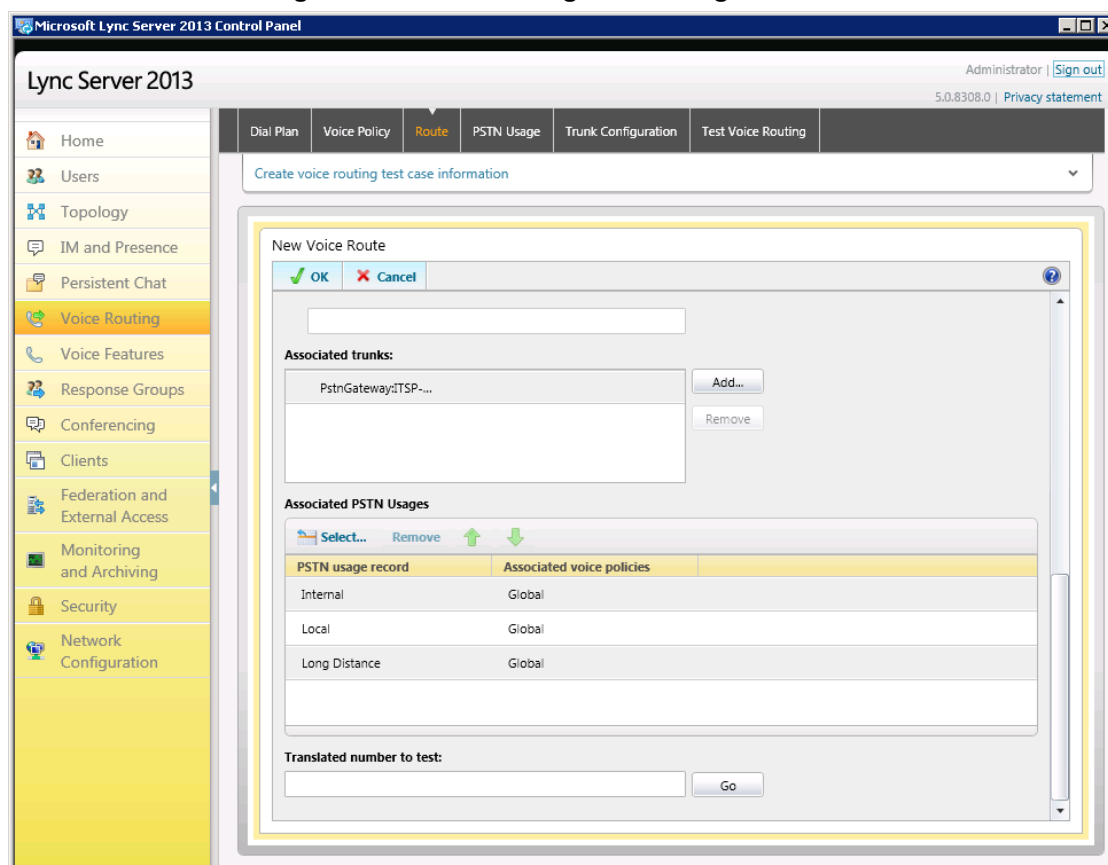
Figure 3-21: List of Deployed Trunks

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

Figure 3-22: Selected E-SBC Trunk

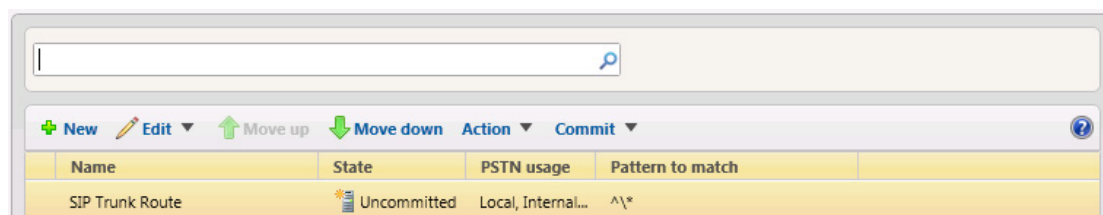
9. Associate a PSTN Usage to this route:
 - a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



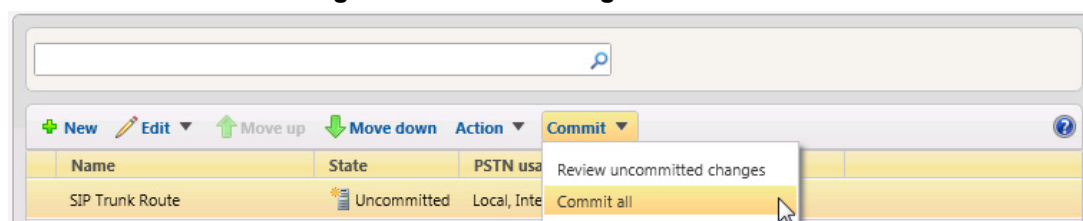
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



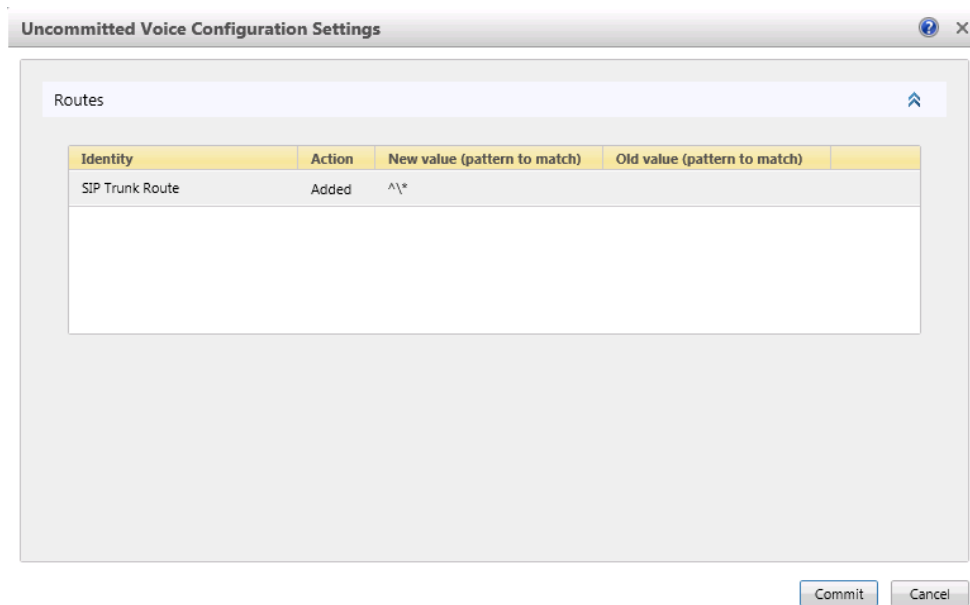
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



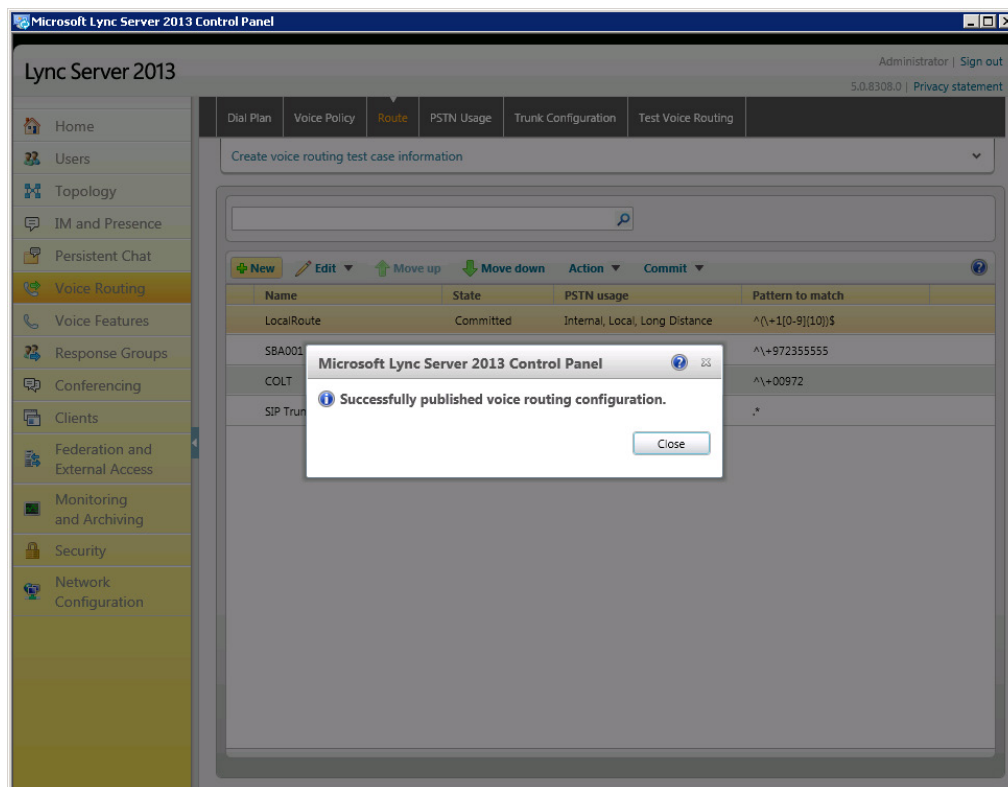
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



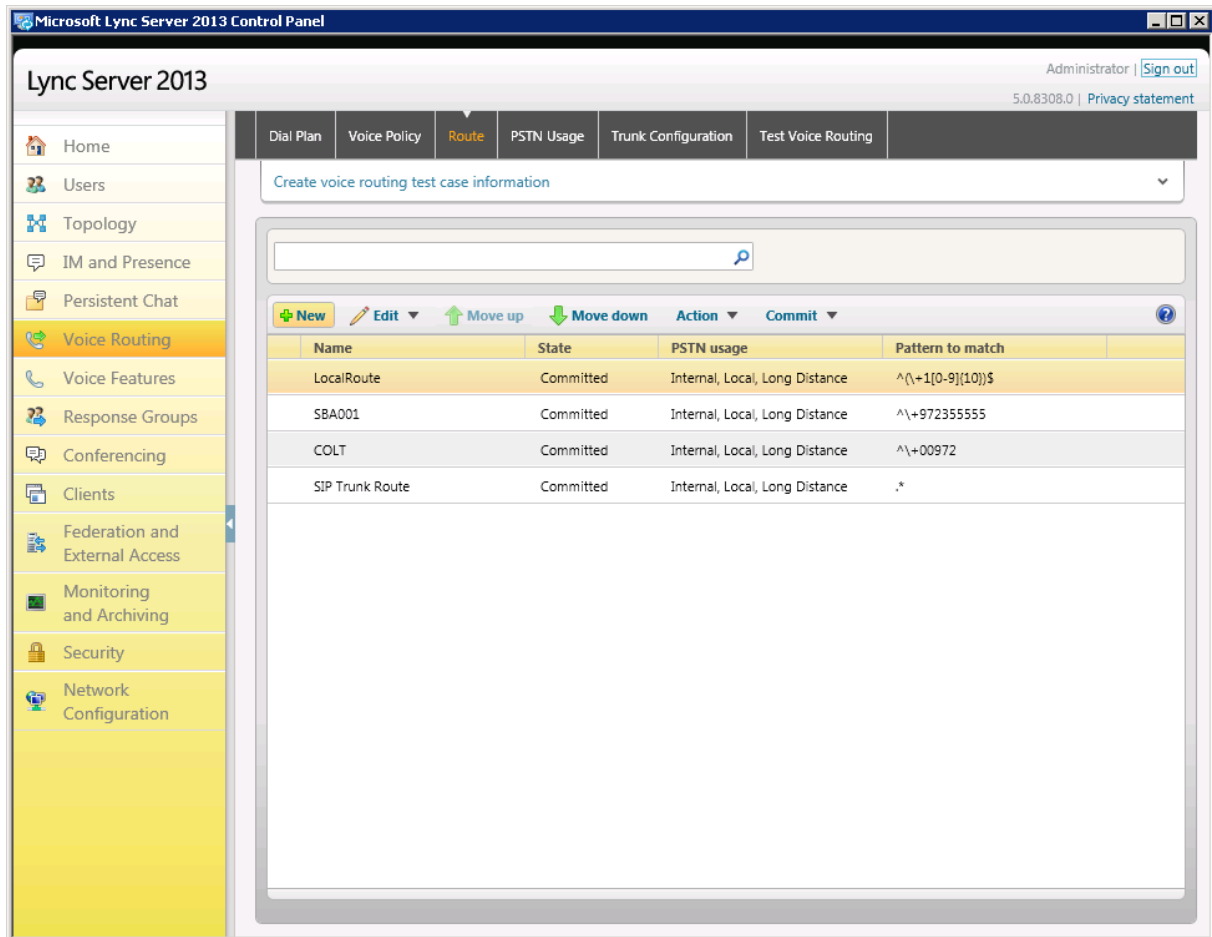
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

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



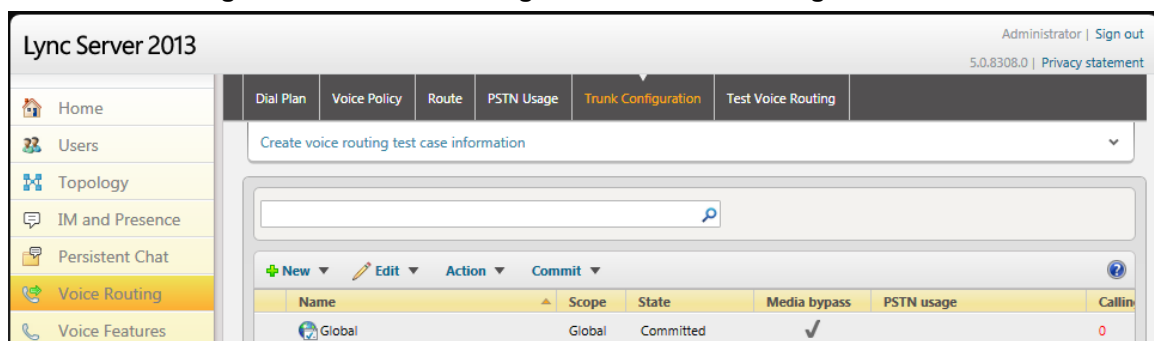
14. For ITSPs that implement a call identifier, continue with the following steps:



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 NextGenTel SIP Trunk in the P-Asserted-Identity header. Using a Message Manipulation rule (see Section 4.13 on page 70), the device adds this ID to the P-Asserted-Identity header in the sent INVITE message.

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

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



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

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.

This page is intentionally left blank.

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 NextGenTel SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- E-SBC WAN interface - NextGenTel 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*).

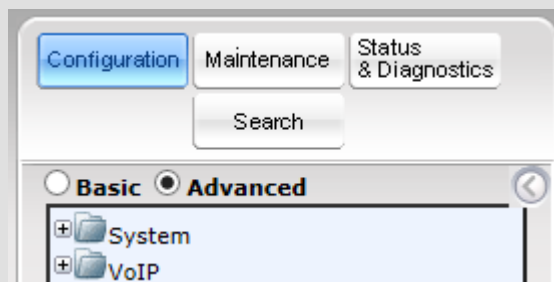
Notes:

- For implementing Microsoft Lync and NextGenTel 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 interoperability test and document does not cover all security aspects for connecting the SIP Trunk to the Microsoft Lync environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, 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:



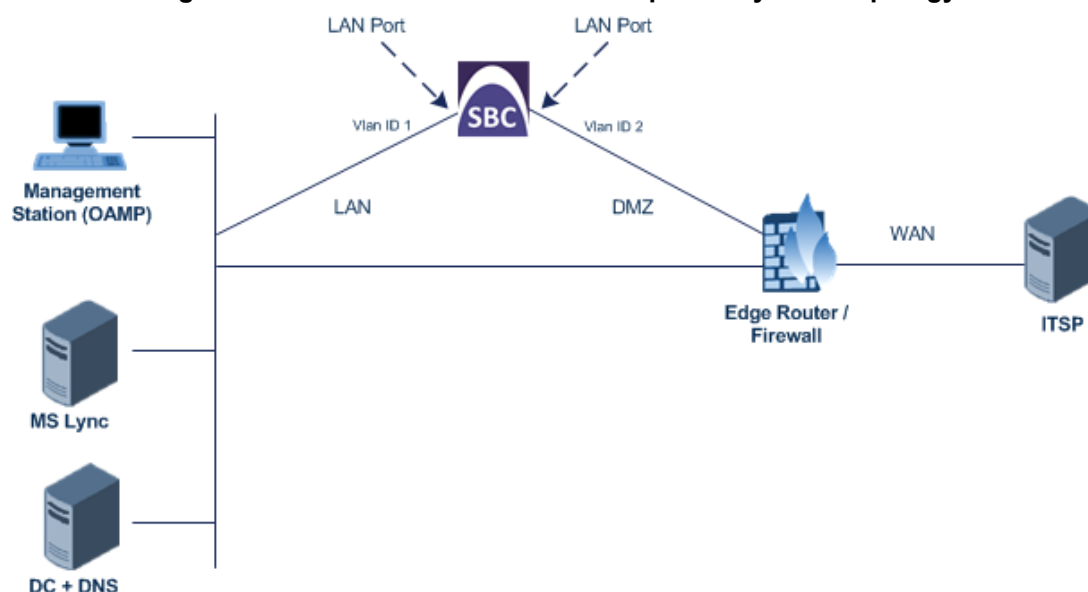
- When the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

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
 - NextGenTel 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	10.15.17.55 (IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Gateway	10.15.0.1
VLAN ID	1
Interface Name	Voice (arbitrary descriptive name)
Primary DNS Server IP Address	10.15.25.1
Underlying 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	195.189.192.159 (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	QAMP + Media +	IPv4 Manual	10.15.17.15	16	10.15.0.1	Voice	10.15.25.1	0.0.0.0	vlan 1
1	Media + Control	IPv4 Manual	195.189.192.156	25	195.189.192.129	WANSP	80.179.52.100	80.179.55.100	vlan 2
<div> Page 1 of 1 Show 10 records per page View 1 - 2 of 2 </div>									

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 4.15 on page 84).

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

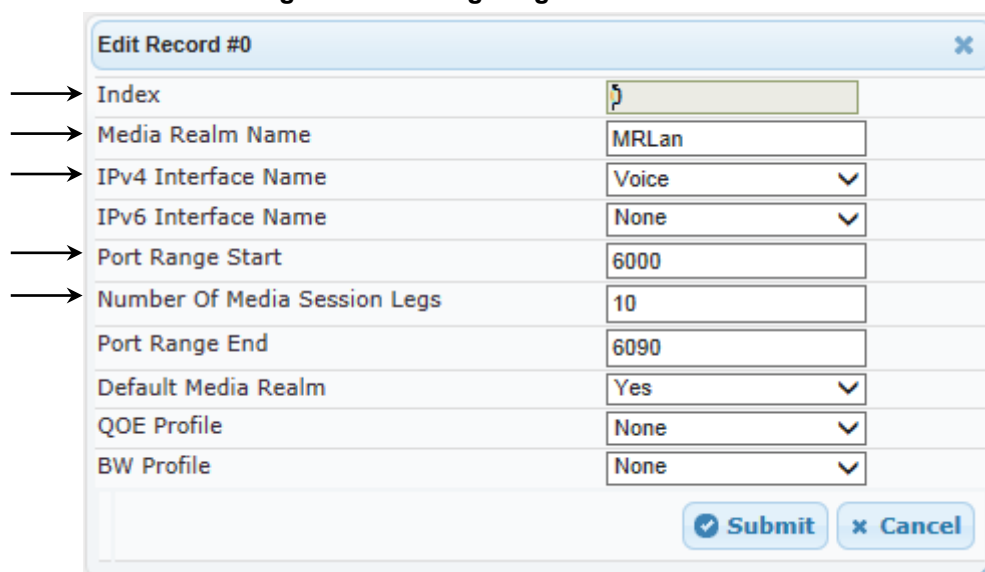
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ 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



Edit Record #0	
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

Submit Cancel

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 screenshot shows a web-based configuration interface for adding a new Media Realm record. The 'Add Record' dialog box contains the following fields and values:

- Index:** 1
- Media Realm Name:** MRWan
- IPv4 Interface Name:** WANSP
- IPv6 Interface Name:** None
- Port Range Start:** 7000
- Number Of Media Session Legs:** 10
- Port Range End:** -1
- Default Media Realm:** No
- QOE Profile:** None
- BW Profile:** None

Arrows on the left side of the dialog point to the Index, Media Realm Name, IPv4 Interface Name, IPv6 Interface Name, and Port Range Start fields.

The configured Media Realms are shown in the figure below:

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

The screenshot shows the 'Media Realm Table' with the following data:

Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	MRLan	Voice	None
1	MRWan	WANSP	None

The table is displayed on page 1 of 1, showing 10 records per page. The bottom of the table shows 'View 1 - 2 of 2'.

4.3.2 Step 3b: Configure SRDs

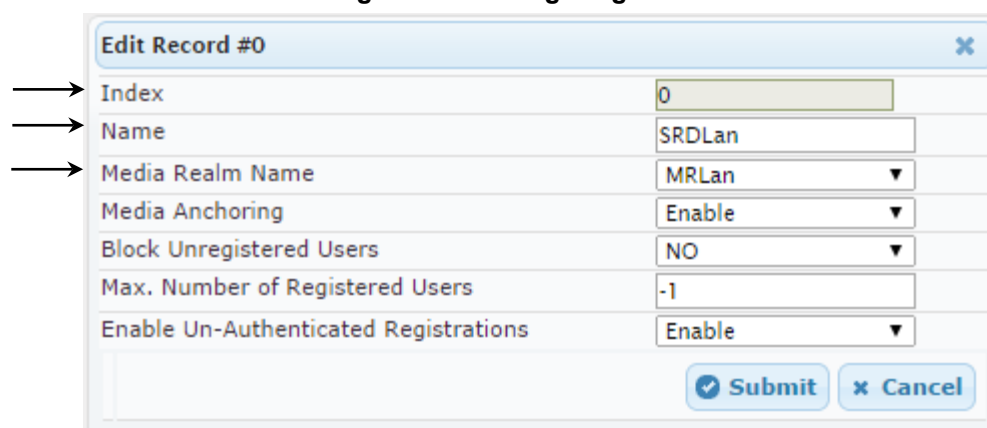
This step describes how to configure the SRDs.

➤ **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
Index	0
Name	SRDLan (descriptive name for SRD)
Media Realm	MRLan (associates SRD with Media Realm)

Figure 4-9: Configuring LAN SRD



The screenshot shows a web-based configuration interface for editing a record. The title bar says "Edit Record #0". The form contains the following fields and values:

- Index:** 0
- Name:** SRDLan
- Media Realm Name:** MRLan
- Media Anchoring:** Enable
- Block Unregistered Users:** NO
- Max. Number of Registered Users:** -1
- Enable Un-Authenticated Registrations:** Enable

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

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

Parameter	Value
Index	1
Name	SRDWan
Media Realm	MRWan

Figure 4-10: Configuring WAN SRD

→ Index: 1

→ 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

The configured SRDs are shown in the figure below:

Figure 4-11: Configured SRDs in SRD Table

SRD Table			
Add +			
Index	Name	Media Realm Name	Media Anchoring
0	SRDLan	MRLan	Enable
1	SRDWan	MRWan	Enable

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

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:

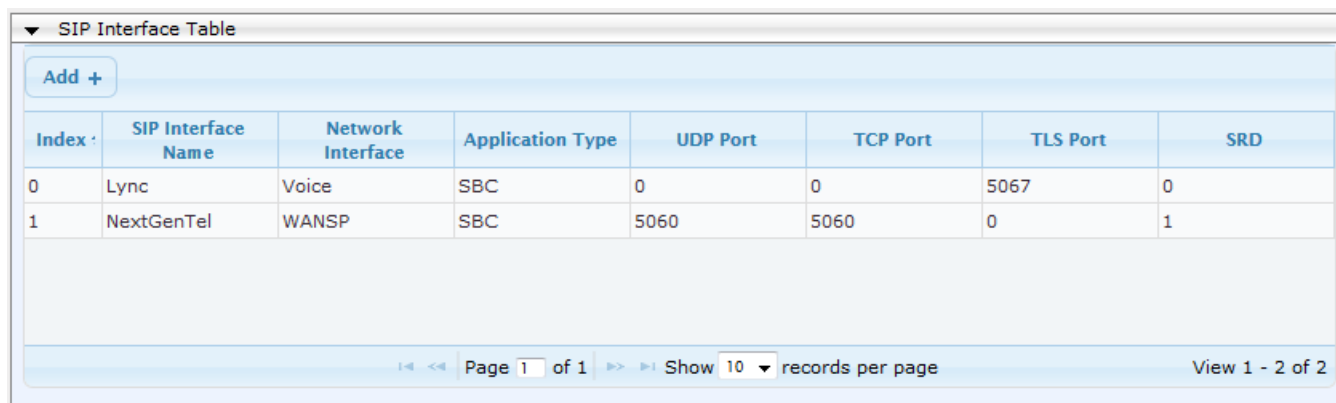
Parameter	Value
Index	0
Interface Name	Lync (arbitrary descriptive name)
Network Interface	Voice
Application Type	SBC
TLS Port	5067
TCP and UDP	0
SRD	0

3. Configure a SIP interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

Figure 4-12: Configured SIP Interfaces in SIP Interface Table



SIP Interface Table							
Add +							
Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
0	Lync	Voice	SBC	0	0	5067	0
1	NextGenTel	WANSP	SBC	5060	5060	0	1

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

4.4 Step 4: Configure Proxy Sets

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

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

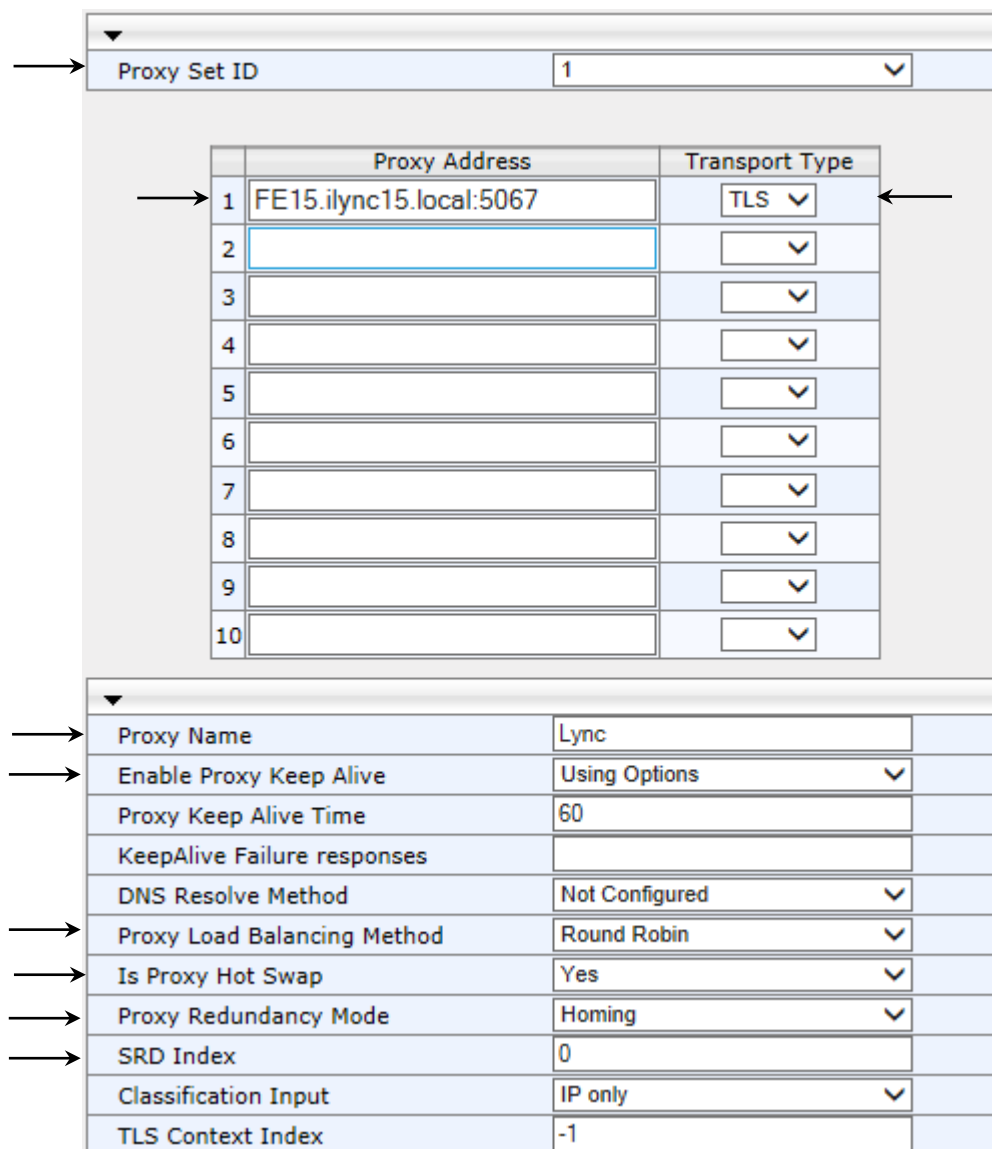
- Microsoft Lync Server 2013
- NextGenTel SIP Trunk

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
Proxy Redundancy Mode	Homing
SRD Index	0

Figure 4-13: 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		
6		
7		
8		
9		
10		

Proxy Name: Lync

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

KeepAlive Failure responses:

DNS Resolve Method: Not Configured

Proxy Load Balancing Method: Round Robin

Is Proxy Hot Swap: Yes

Proxy Redundancy Mode: Homing

SRD Index: 0

Classification Input: IP only

TLS Context Index: -1

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

Parameter	Value
Proxy Set ID	2
Proxy Address	85.119.137.82:5060 (NextGenTel IP address and destination port)
Transport Type	UDP
Proxy Name	NextGenTel (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
KeepAlive Failure responses	503 (Enables handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case, the E-SBC attempts to locate an alternative route for the call.)
SRD Index	1 (enables classification by Proxy Set for SRD of IP Group belonging to NextGenTel SIP Trunk)

Figure 4-14: Configuring Proxy Set for NextGenTel SIP Trunk

Proxy Set ID: 2

	Proxy Address	Transport Type
1	85.119.137.82:5060	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name	NextGenTel
Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
KeepAlive Failure responses	503
DNS Resolve Method	Not Configured
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only
TLS Context Index	-1

4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.15 on page 84).

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
- NextGenTel 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	NextGenTel (according to ITSP requirement)
SRD	0
Media Realm Name	MRLan
IP Profile ID	1

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

Parameter	Value
Index	2
Type	Server
Description	NextGenTel (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	NextGenTel (according to ITSP requirement)
SRD	1
Media Realm Name	MRWan
IP Profile ID	2

The configured IP Groups are shown in the figure below:

Figure 4-15: 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	195.189.192.159			No	0
2	Server	NextGenTel	2	195.189.192.159			No	1
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
- NextGenTel 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 44).

➤ 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)
Disconnect on Broken Connection	No
Symmetric MKI	Enable
MKI Size	1
Reset SRTP State Upon Re-key	Enable
Generate SRTP keys mode:	Always

Figure 4-16: 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 Canceled	Line
Disconnect on Broken Connection	No
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
Jitter Buffer Max Delay [msec]	300

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

Parameter	Value
SBC Media Security Behavior	SRTP
PRACK Mode	Optional (required, as NextGenTel SIP Trunk does not generate PRACK)
Session Expires Mode	Supported (required, as NextGenTel SIP Trunk does not generate Session Expire Timer in incoming calls, so SBC will negotiate it with Lync Server)
Remote Update Support	Supported Only After Connect
Remote Re-	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)
RTCP Mode	Generate Always (required, as NextGenTel SIP Trunk does not send RTCP packets in hold call, and in this case, Microsoft Lync 2013 will terminate the call with network problems as the cause)

Figure 4-17: 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 Aft
Remote re-INVITE	Supported only with
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	Standard
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Generate Always
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Transparent
Remote Multiple Answers Mode	Disabled
Keep VIA Headers	Not Configured
Keep User-Agent Header	Not Configured
User Behind NAT UDP Registration Time	-1
User Behind NAT TCP Registration Time	-1

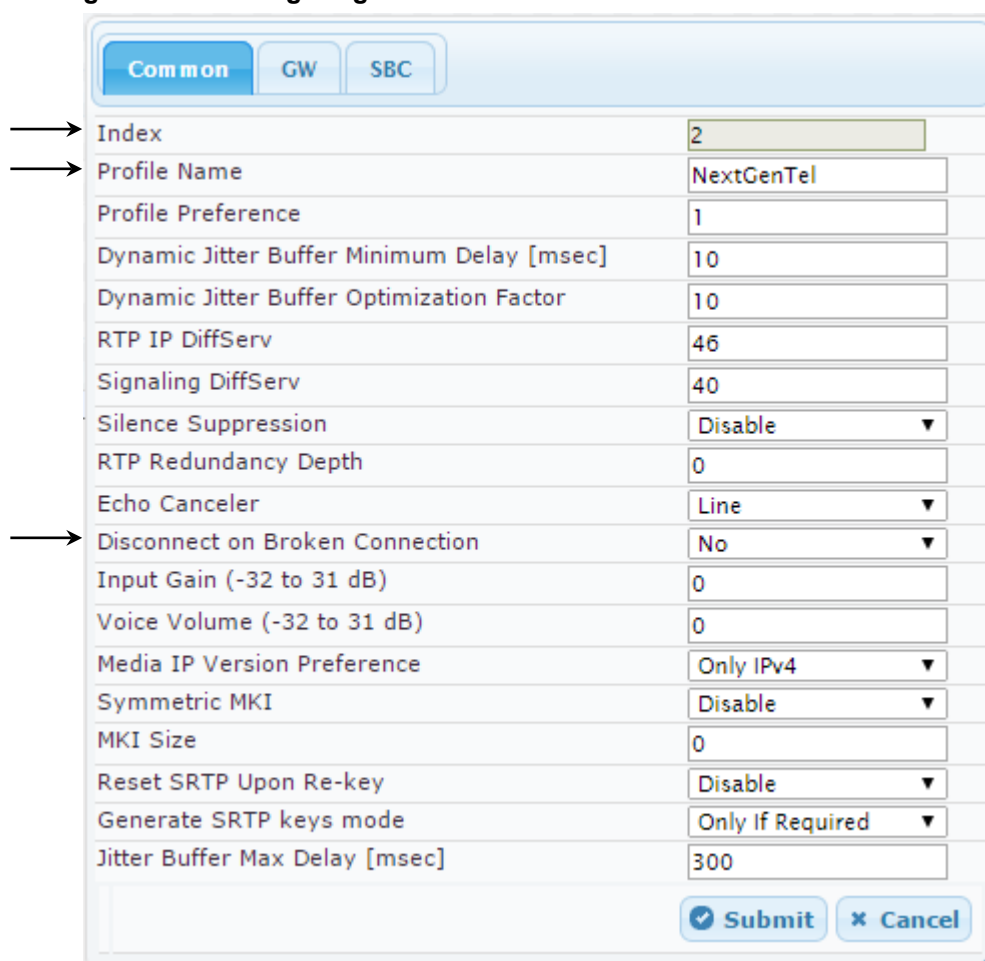
Submit Cancel

➤ **To configure an IP Profile for the NextGenTel SIP Trunk:**

1. Click **Add**.
2. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Profile Name	NextGenTel (arbitrary descriptive name)
Disconnect on Broken Connection	No

Figure 4-18: Configuring IP Profile for NextGenTel SIP Trunk – Common Tab



Parameter	Value
Index	2
Profile Name	NextGenTel
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	No
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

Submit Cancel

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

Parameter	Value
Index	2
Allowed Coders Group ID	Coders Group 0
Allowed Coders Mode	Restriction and Preference
SBC Media Security Behavior	RTP
P-Asserted-Identity	Add (required for anonymous calls)
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Play RBT To Transferee	Yes

Figure 4-19: Configuring IP Profile for NextGenTel SIP Trunk – SBC Tab

Common GW SBC	
→ Index	2
Extension Coders Group ID	None ▼
Transcoding Mode	Only If Required ▼
Allowed Media Types	
→ Allowed Coders Group ID	Coders Group 0 ▼
→ Allowed Video Coders Group ID	None ▼
→ Allowed Coders Mode	Restriction and Prel ▼
→ SBC Media Security Behavior	RTP ▼
RFC 2833 Behavior	As Is ▼
Alternative DTMF Method	As Is ▼
→ P-Asserted-Identity	Add ▼
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	Transparent ▼
Session Expires Mode	Transparent ▼
Remote Update Support	Supported ▼
Remote re-INVITE	Supported ▼
Remote Delayed Offer Support	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	Transparent ▼
Remote Replaces Behavior	Standard ▼
SDP Ptime Answer	Remote Answer ▼
Preferred PTime	0
Use Silence Suppression	Transparent ▼
RTP Redundancy Behavior	AS IS ▼
→ Play RBT To Transferee	Yes ▼
RTCP Mode	Transparent ▼
Jitter Compensation	Disable ▼
Remote Renegotiate on Fax Detection	Transparent ▼
Remote Multiple Answers Mode	Disabled ▼
Keep VIA Headers	Not Configured ▼
Keep User-Agent Header	Not Configured ▼
User Behind NAT UDP Registration Time	-1
User Behind NAT TCP Registration Time	-1

4.7 Step 7: Configure Coders

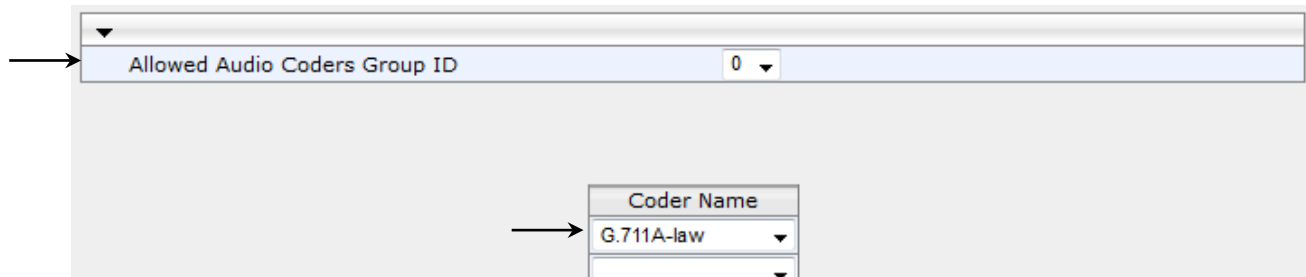
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the NextGenTel SIP Trunk uses the G.711A-law coder only. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the NextGenTel SIP Trunk in the previous step (see Section 4.6 on page 46).

➤ **To set a preferred coder for the NextGenTel 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	0
Coder Name	G.711 A-law

Figure 4-20: Configuring Allowed Coders Group for NextGenTel SIP Trunk



4.8 Step 8: SIP TLS Connection Configuration

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

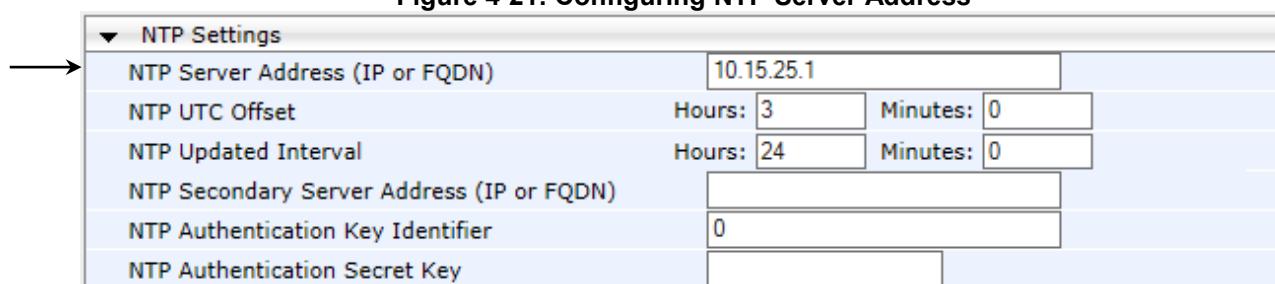
4.8.1 Step 8a: Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the E-SBC receives the accurate and current date and time. This is necessary for validating certificates of remote parties.

➤ To configure the NTP server address:

1. Open the Application Settings page (**Configuration** tab > **System** > **Application Settings**).
2. In the 'NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.25.1**).

Figure 4-21: 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**.

4.8.2 Step 8b: Configure a Certificate

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

The procedure involves the following main steps:

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

➤ **To configure a certificate:**


1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row, and then click the **Context Certificates**  button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP-GW.ilync15.local**).
 - b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-22: Certificate Signing Request – Creating CSR

Certificate Signing Request	
Subject Name [CN]	ITSP-GW.ilync15.local
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
<input type="button" value="Create CSR"/>	
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.	
<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLmlseW5jMTUubG9jYVwwZ8w DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioo0LVrwNsC1 3TMgncMVxdp9/BCXyygT2W1vz0NGUstypa7w2DKKkxr8xA9sGLXwy0ZCyB49U1pDF DJV8IldUfT8qL9d9V64f3Z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz 52203jtjXKmdAgMBAAGgADANBgkqhkiG9w0BAQQFAAQBQBLqe880JGrmEzPu5Q1 pRGiOuEQ4Pr6PL+JKghii6UpLmHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y 8z8hOCZXV/E4MrR2s8bYb6bqxeteAXs+VwxgKObb4pSFfGLc82+dZUcODAB0w2Fv nxSEcPACKnZittF/GgW+4AaMQ== -----END CERTIFICATE REQUEST----- </pre>	

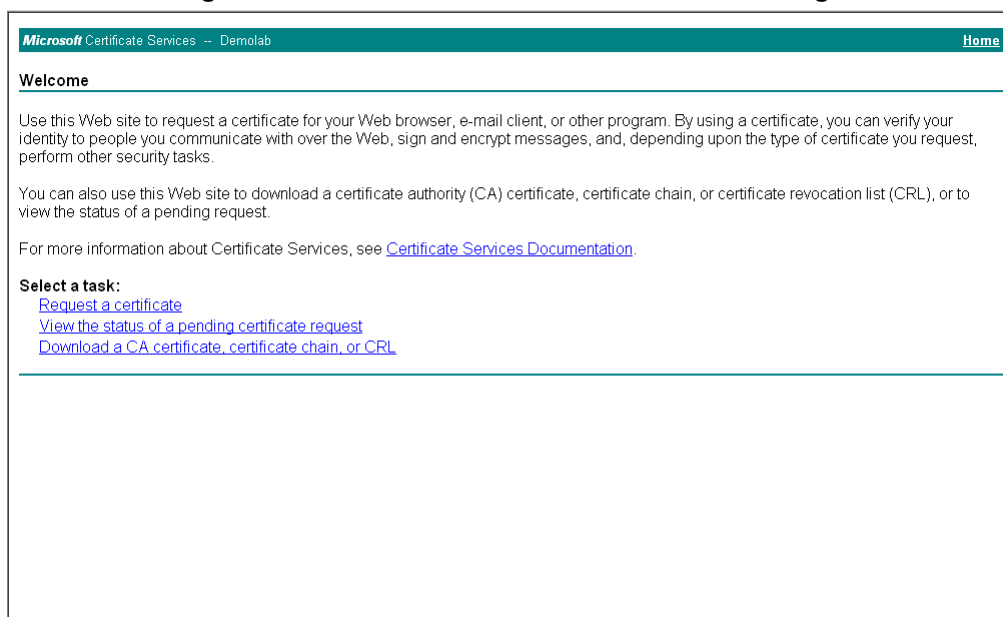


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).

5. Copy the CSR from the line "**-----BEGIN CERTIFICATE REQUEST-----**" 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*.

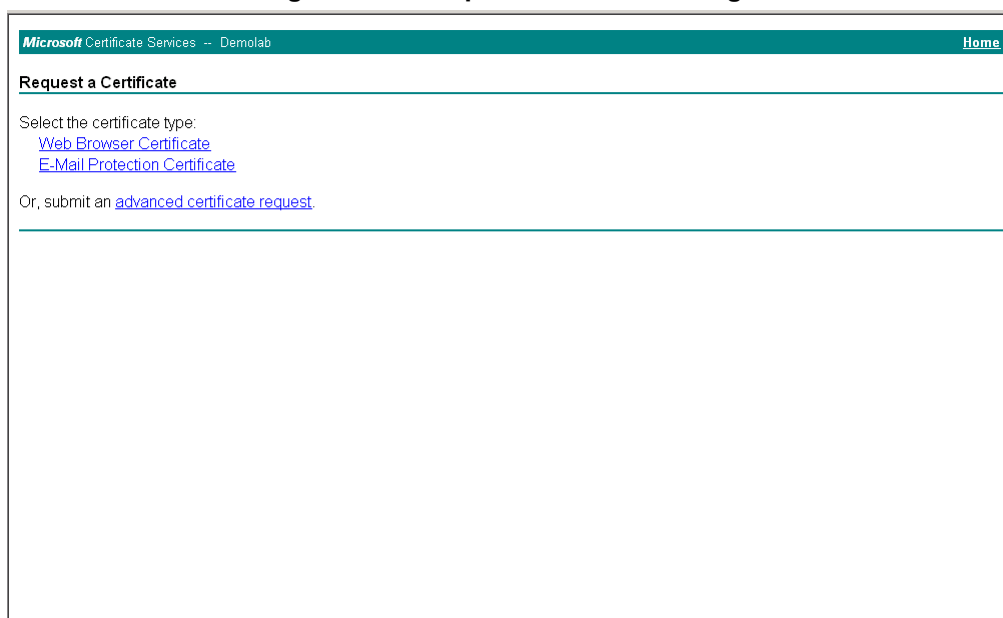
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-23: Microsoft Certificate Services Web Page



7. Click **Request a certificate**.

Figure 4-24: Request a Certificate Page



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

Figure 4-25: 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 4-26: 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
rr4ootrnsPOCAvEAAaAAMAOGCsqGS Ib3 DQEBBAUA
HnkHAKx8xHq9gaAgoLKmuch2Bo2m4gEcOGAFT8ok
9fSm8c4Bj8ib+R5+YI+Oot57xT9DZXNg5Yp4G+OB
vnQuXOUUX6BeVBT71aO83HcA
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

[Submit >](#)


- Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
- From the 'Certificate Template' drop-down list, select **Web Server**.
- Click **Submit**.

Figure 4-27: Certificate Issued Page

Certificate Issued

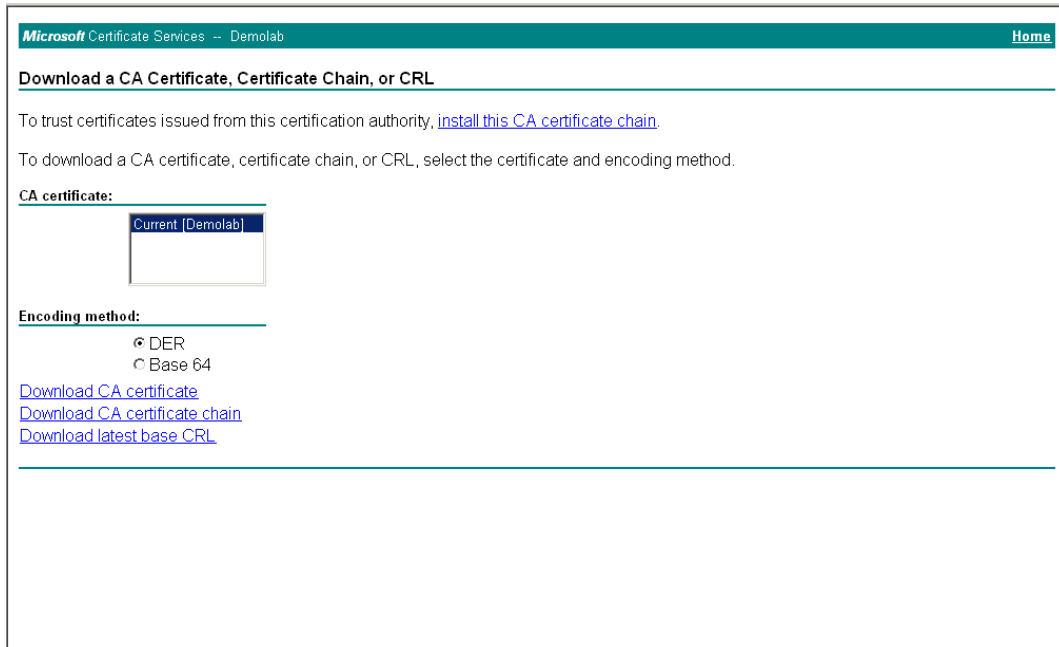
The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded

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

13. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
14. Save the file as *gateway.cer* to a folder on your computer.
15. Click the **Home** button or navigate to the certificate server at <http://<Certificate Server>/CertSrv>.
16. Click **Download a CA certificate, certificate chain, or CRL**.

Figure 4-28: Download a CA Certificate, Certificate Chain, or CRL Page



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

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Current [Demolab]

Encoding method:

☒ DER
☐ Base 64

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

17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.

20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
 - a. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-29: Upload Device Certificate Files from your Computer Group

▼ Upload certificate files from your computer

Private key pass-phrase (optional)

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

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

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

- b. In the E-SBC's Web interface, return to the **TLS Contexts** page.
- c. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates** button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
- d. Click the **Import** button, and then select the certificate file to load.

Figure 4-30: Importing Root Certificate into Trusted Certificates Store

Import New Certificate ✕

D:\backup\warehouse\c

21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 84).

4.9 Step 9: Configure SRTP

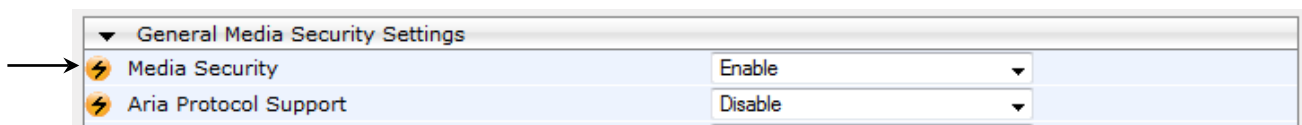
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 46).

➤ **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 4-31: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 84).

4.10 Step 10: Configure Maximum Media Channels

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



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

➤ **To configure the maximum number of media channels:**

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

Figure 4-32: Configuring Number of Media Channels

Number of Media Channels	30
--------------------------	----

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section [4.15](#) on page [84](#)).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 44, IP Group 1 represents Lync Server 2013, and IP Group 2 represents NextGenTel 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 NextGenTel SIP Trunk (WAN):

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

Figure 4-33: 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 4-34: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

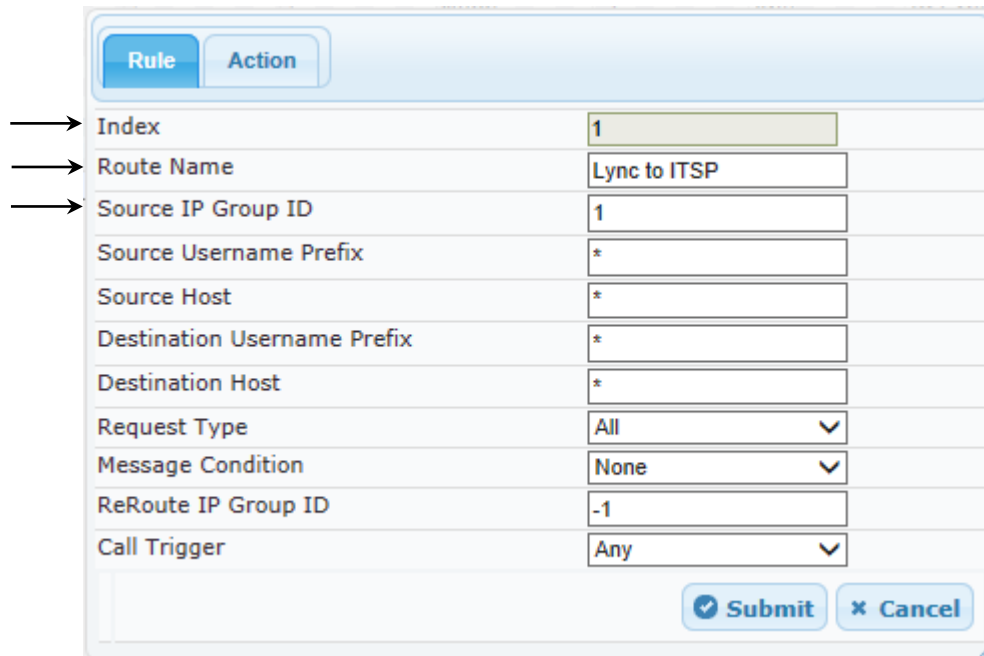
Action	
Index	0
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1

Submit Cancel

6. Configure a rule to route calls from Lync Server 2013 to NextGenTel 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 4-35: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab



Rule	
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

Submit Cancel

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	1

Figure 4-36: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab

The screenshot shows the 'Action' tab of a configuration window. The 'Rule' tab is also visible. The 'Action' tab contains the following fields:

- Index: 1
- Destination Type: IP Group (dropdown menu)
- Destination IP Group ID: 2
- Destination SRD ID: 1 (dropdown menu)
- Destination Address: (empty text field)
- Destination Port: 0
- Destination Transport Type: (empty dropdown menu)
- Alternative Route Options: Route Row (dropdown menu)
- Group Policy: None (dropdown menu)
- Cost Group: None (dropdown menu)

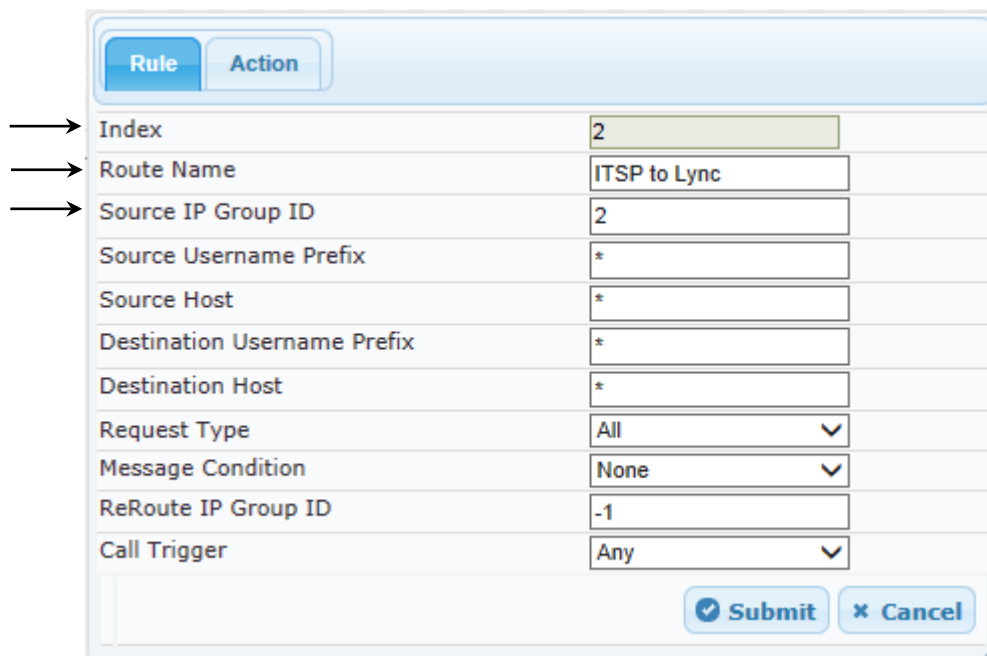
At the bottom right, there are 'Submit' and 'Cancel' buttons. Three arrows on the left point to the 'Destination Type', 'Destination IP Group ID', and 'Destination SRD ID' fields.

➤ To configure rule to route calls from NextGenTel SIP Trunk to Lync Server 2013:

1. Click **Add**.
2. 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 4-37: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab



Parameter	Value
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

3. 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	0

Figure 4-38: 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: 0

Destination Address:

Destination Port: 0

Destination Transport Type:

Alternative Route Options: Route Row

Group Policy: None

Cost Group: None

Submit Cancel

The configured routing rules are shown in the figure below:

Figure 4-39: 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	Call Setup Rules Set ID	Destination Type	Destination SRD ID	
0	OPTIONS ter	*	*	*	None	-1	Any	-1	Dest Address	None	
1	Lync to ITSP	*	*	*	None	-1	Any	-1	IP Group	1	
2	ITSP to Lync	*	*	*	None	-1	Any	-1	IP Group	0	

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



Note: The routing configuration may change according to your specific deployment topology.

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 44, IP Group 1 represents Lync Server 2013, and IP Group 2 represents NextGenTel SIP Trunk.



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

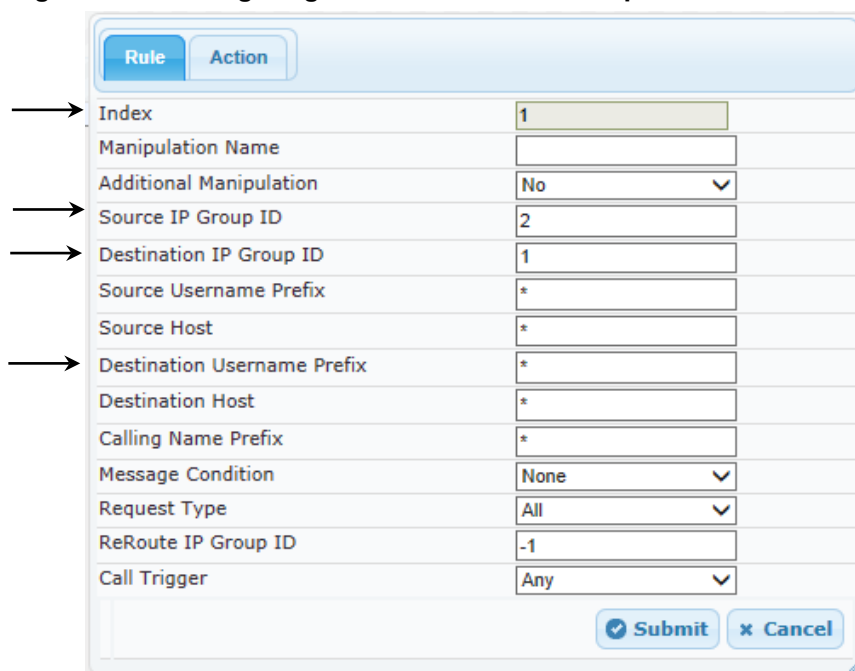
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (NextGenTel SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

➤ 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 ID	2
Destination IP Group ID	1
Destination Username Prefix	* (asterisk sign)

Figure 4-40: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



Field	Value
Index	1
Manipulation Name	
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

Submit Cancel

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

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

Figure 4-41: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

The screenshot shows the 'Action' tab of the configuration window. The 'Manipulated Item' is set to 'Destination URI' and 'Prefix to Add' is set to '+'. The 'Index' is 1. Other fields like 'Remove From Left', 'Remove From Right', 'Leave From Right', 'Suffix to Add', and 'Privacy Restriction Mode' are also visible.

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., NextGenTel SIP Trunk):

Figure 4-42: Example of Configured IP-to-IP Outbound Manipulation Rules

IP to IP Outbound Manipulation												
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.

3. If the manipulation rule Index 0 (above) is executed, then the following rule is also executed. It removes History Info Header.

Parameter	Value
Index	1
Manipulation Name	Call Forward
Manipulation Set ID	4
Action Subject	header.history-info
Action Type	Remove
Row Role	Use Previous Condition

Figure 4-44: Configuring SIP Message Manipulation Rule 1 (for NextGenTel SIP Trunk)

The screenshot shows a web-based configuration interface for SIP Message Manipulation Rule 1. The dialog box is titled "Edit Record #1" and contains the following fields:

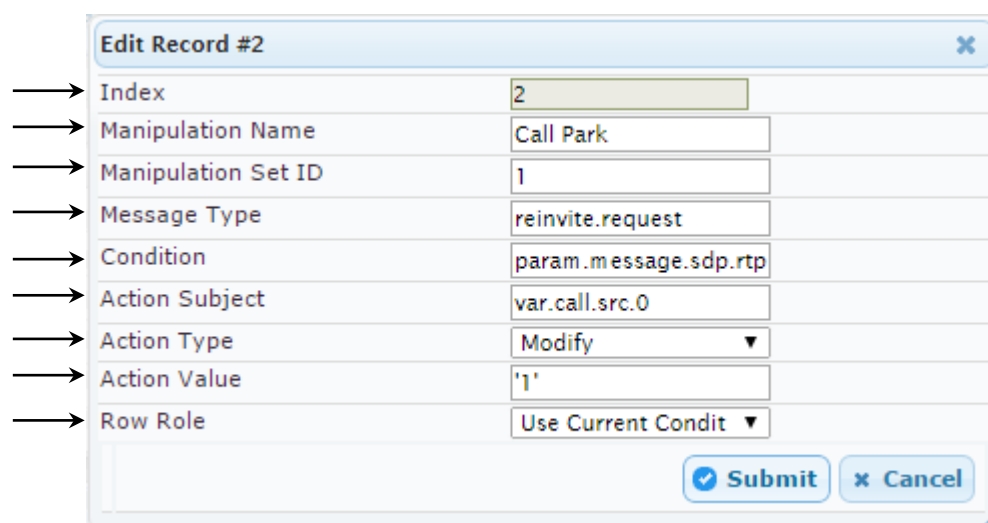
- Index: 1
- Manipulation Name: Call Forward
- Manipulation Set ID: 4
- Message Type: (empty)
- Condition: (empty)
- Action Subject: header.history-info
- Action Type: Remove
- Action Value: (empty)
- Row Role: Use Previous Condi

Arrows point to the first seven fields (Index through Action Value). At the bottom right, there are "Submit" and "Cancel" buttons.

4. For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-initiated Hold), create a variable and set it to '1'. This variable manages how the call will be handled in each state (answer, request, etc.).

Parameter	Value
Index	2
Manipulation Name	Call Park
Manipulation Set ID	1
Message Type	reinvite.request
Condition	param.message.sdp.rtpmode=='sendonly'
Action Subject	var.call.src.0
Action Type	Modify
Action Value	'1'
Row Role	Use Current Condition

Figure 4-45: Configuring SIP Message Manipulation Rule 2 (for Microsoft Lync)



Edit Record #2	
Index	2
Manipulation Name	Call Park
Manipulation Set ID	1
Message Type	reinvite.request
Condition	param.message.sdp.rtp
Action Subject	var.call.src.0
Action Type	Modify
Action Value	'1'
Row Role	Use Current Condit

Submit Cancel

5. If the manipulation rule Index 2 (above) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to “sendonly” change it to “sendrecv”.

Parameter	Value
Index	3
Manipulation Name	Call Park
Manipulation Set ID	1
Action Subject	param.message.sdp.rtpmode
Action Type	Modify
Action Value	'sendrecv'
Row Role	Use Previous Condition

Figure 4-46: Configuring SIP Message Manipulation Rule 3 (for Microsoft Lync)

Edit Record #3

Index	3
Manipulation Name	Call Park
Manipulation Set ID	1
Message Type	
Condition	
Action Subject	param.message.sdp.rtp
Action Type	Modify ▼
Action Value	'sendrecv'
Row Role	Use Previous Condi ▼

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

Parameter	Value
Index	4
Manipulation Name	Call Park
Manipulation Set ID	2
Message Type	reinvite.response.200
Condition	var.call.src.0=="1"
Action Subject	param.message.sdp.rtpmode
Action Type	Modify
Action Value	'recvonly'
Row Role	Use Current Condition

Figure 4-47: Configuring SIP Message Manipulation Rule 4 (for Microsoft Lync)

Edit Record #4

Index	4
Manipulation Name	Call Park
Manipulation Set ID	2
Message Type	reinvite.response.200
Condition	var.call.src.0=="1"
Action Subject	param.message.sdp.rtp
Action Type	Modify
Action Value	'recvonly'
Row Role	Use Current Condit

Submit
Cancel

7. If the manipulation rule Index 4 (above) is executed, then the following rule is also executed. If the variable is determined to be set to "1" (in the previous manipulation rule), then set it to "0" in order to normalize the call processing state back. Lync now sends Music on Hold to the NextGenTel SIP Trunk even without the NextGenTel SIP Trunk knowing how to receive Music on Hold. The call is now truly on hold with Music on Hold.

Parameter	Value
Index	5
Manipulation Name	Call Park
Manipulation Set ID	2
Action Subject	var.call.src.0
Action Type	Modify
Action Value	'0'
Row Role	Use Previous Condition

Figure 4-48: Configuring SIP Message Manipulation Rule 5 (for Microsoft Lync)

The screenshot shows a web-based configuration interface for SIP Message Manipulation Rule 5. The dialog box is titled 'Edit Record #5' and contains the following fields and values:

Index	5
Manipulation Name	Call Park
Manipulation Set ID	2
Message Type	
Condition	
Action Subject	var.call.src.0
Action Type	Modify
Action Value	'0'
Row Role	Use Previous Condi

At the bottom right of the dialog are two buttons: 'Submit' and 'Cancel'.

8. Configure another manipulation rule (Manipulation Set 4) for NextGenTel SIP Trunk. This rule applies to messages sent to the NextGenTel SIP Trunk (IP Group 2). This replaces the host part of the Referred-By Header with the value from the SIP From Header.

Parameter	Value
Index	6
Manipulation Name	Call Transfer
Manipulation Set ID	4
Condition	header.referred-by exists
Action Subject	header.referred-by.url.host
Action Type	Modify
Action Value	header.from.url.host

Figure 4-49: Configuring SIP Message Manipulation Rule 7 (for NextGenTel SIP Trunk)

Edit Record #6

Index	6
Manipulation Name	Call Transfer
Manipulation Set ID	4
Message Type	
Condition	header.referred-by exists
Action Subject	header.referred-by.url.h
Action Type	Modify ▼
Action Value	header.from.url.host
Row Role	Use Current Condit ▼

9. If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. It remove prefix '+47' from the Referred-By Header.

Parameter	Value
Index	7
Manipulation Name	Call Transfer
Manipulation Set ID	4
Action Subject	header.referred-by.url.user
Action Type	Remove Prefix
Action Value	'+47'
Row Role	Use Previous Condition

Figure 4-50: Configuring SIP Message Manipulation Rule 8 (for NextGenTel SIP Trunk)

Edit Record #7

Index	7
Manipulation Name	Call Transfer
Manipulation Set ID	4
Message Type	
Condition	
Action Subject	header.referred-by.url.u
Action Type	Remove Prefix ▼
Action Value	'+47'
Row Role	Use Previous Condi ▼

10. Configure another manipulation rule (Manipulation Set 4) for NextGenTel SIP Trunk. This rule applies to messages sent to the NextGenTel SIP Trunk (IP Group 2). This rule replaces the **user** part of the **From** Header with the value from Referred-By Header.

Parameter	Value
Index	8
Manipulation Name	Call Transfer
Manipulation Set ID	4
Condition	header.referred-by exists
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.referred-by.url.user

Figure 4-51: Configuring SIP Message Manipulation Rule 8 (for NextGenTel SIP Trunk)

Edit Record #8

Index	8
Manipulation Name	Call Transfer
Manipulation Set ID	4
Message Type	
Condition	header.referred-by exists
Action Subject	header.from.url.user
Action Type	Modify
Action Value	header.referred-by.url.u
Row Role	Use Current Condit

Submit
Cancel

Figure 4-52: Example of 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	Call Forward	4		header.history-inf	header.from.url.u	Modify	\$3
1	Call Forward	4			header.history-inf	Remove	
2	Call Park	1	reinvite.request	param.message.s	var.call.src.0	Modify	'1'
3	Call Park	1			param.message.s	Modify	'sendrecv'
4	Call Park	2	reinvite.response	var.call.src.0='1	param.message.s	Modify	'recvonly'
5	Call Park	2			var.call.src.0	Modify	'0'
6	Call Transfer	4		header.referred-b	header.referred-b	Modify	header.from.url.hos
7	Call Transfer	4			header.referred-b	Remove Prefix	'+47'
8	Call Transfer	4		header.referred-b	header.from.url.u	Modify	header.referred-by.

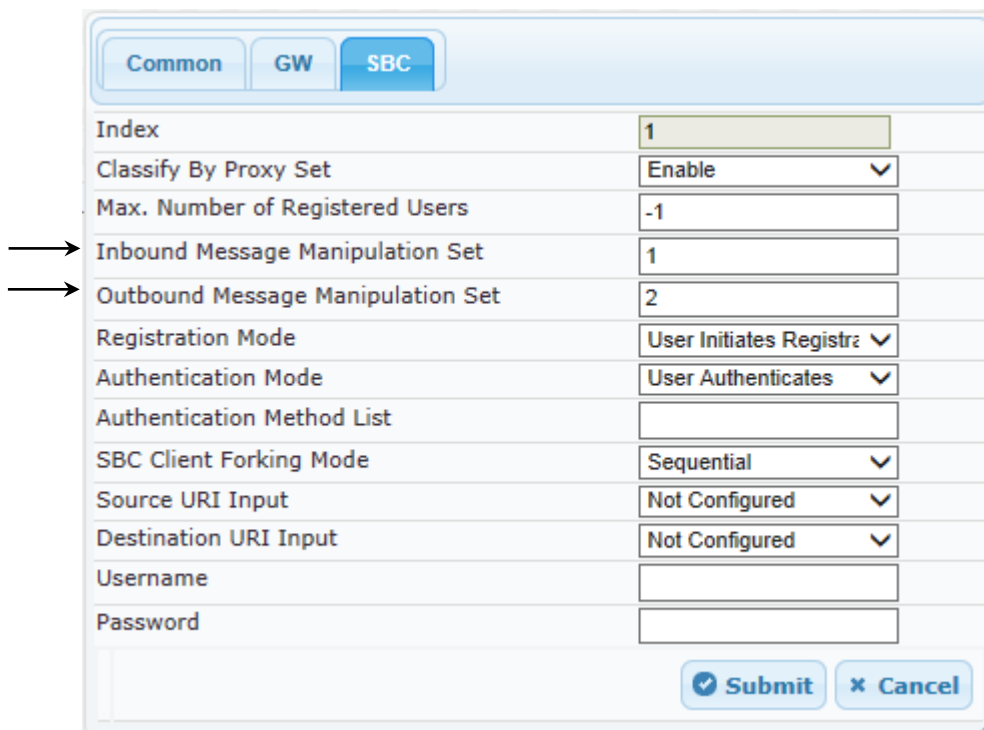
Page 1 of 1
Show 10 records per page
View 1 - 9 of 9

The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set IDs 1, 2, and 4) which are executed for messages sent to and from the NextGenTel 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 NextGenTel SIP Trunk and Lync Server 2013. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages sent to the NextGenTel SIP Trunk (IP Group 2) in a call forward scenario. This replaces the user part of the SIP From Header with the value from the SIP History-Info Header (with stripping +47).	For Call Forward scenarios, NextGenTel SIP Trunk needs that User part in SIP From Header will be NextGenTel defined number. In order to do this, User part of the SIP From Header replaced with the value from History-Info Header.
1	If the manipulation rule Index 0 (above) is executed, then the following rule is also executed. It removes History Info Header.	
2	For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-initiated Hold), create a variable and set it to '1'. This variable manages how the call will be handled in each state (answer, request, etc.).	In the Call Park scenario, Microsoft Lync sends Re-INVITE messages twice. The first message is sent with the SDP, where the RTP mode is set to "a=inactive". The second message is sent with "a=sendonly". The NextGenTel SIP Trunk has a problem recognizing two sequential Re-INVITE messages with different RTP modes. This causes the loss of the Music On Hold functionality in the Call Park scenario. These four rules are applied to work around this limitation.
3	If the previous manipulation rule (Index 0) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to "sendonly", change it to "sendrecv".	
4	This rule attempts to normalize the call processing state back to Lync 2013 for the correct reply to the initially received "sendonly". For every SIP Re-INVITE message with the variable set to '1', change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the NextGenTel SIP Trunk to the Lync-initiated Hold.	
5	If the manipulation rule Index 2 (above) is executed, then the following rule is also executed. If the variable is determined to be set to "1" (in the previous manipulation rule), then set it to "0" to normalize the call processing state. Lync now sends Music on Hold to the NextGenTel SIP Trunk even without the NextGenTel SIP Trunk knowing how to receive MoH. The call is now truly on hold with MoH.	
6	This rule applies to messages sent to the NextGenTel SIP Trunk (IP Group 2). This replaces the host part of the Referred-By Header with the value from the SIP From Header.	For Call Transfer initiated by Lync Server 2013, NextGenTel SIP Trunk needs to replace the Host part of the SIP Referred-By Header with the value from the SIP From Header and user part of the From Header with the value from Referred-By Header.
7	If the manipulation rule Index 6 (above) is executed, then the following rule is also executed. It remove prefix '+47' from the Referred-By Header.	
8	This rule applies to messages sent to the NextGenTel SIP Trunk (IP Group 2). This rule replaces the user part of the From Header with the value from Referred-By Header.	

11. 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 4-53: Assigning Manipulation Set to IP Group 1



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 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	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- f. Click **Submit**.

12. 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 4-54: 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 Registrz'. 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.

Common GW SBC	
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 Registrz
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**.

4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

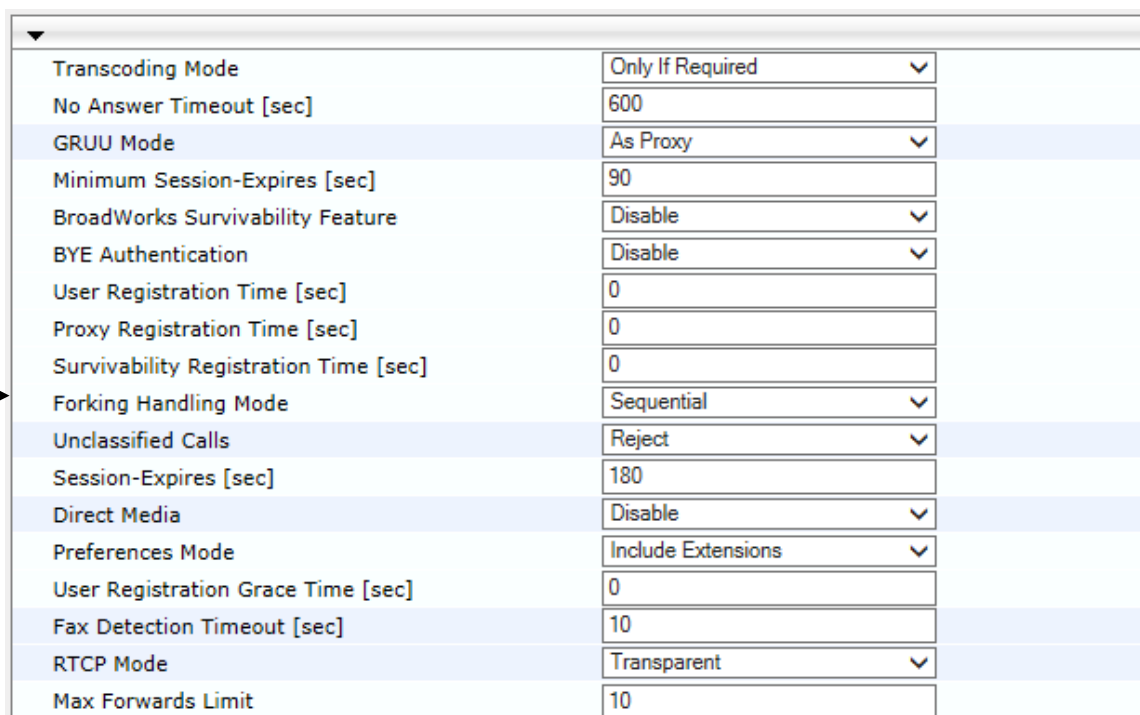
4.14.1 Step 14a: Configure Call Forking Mode

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 SIP 18x with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received SIP 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It's mandatory to set this field for the Lync Server 2013 environment.

➤ **To configure call forking:**

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-55: Configuring Forking Mode



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**.

4.14.2 Step 14b: Configure SBC Session Refreshing Policy

This step shows how to configure the 'SBC Session Refreshing Policy' parameter. In some cases, Microsoft Lync does not perform a refresh of Session Timer even when it confirms that it will be refresher. To resolve this issue, the SBC is configured as Session Expire refresher.

➤ **To configure SBC Session Refreshing Policy:**

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., <http://10.15.17.55/AdminPage>).
2. In the left pane of the page that opens, click **ini Parameters**.

Figure 4-56: Configuring SBC Session Refreshing Policy in AdminPage

Parameter Name: Enter Value:

Output Window

```
Parameter Name: SBCSESSIONREFRESHINGPOLICY
Parameter New Value: 1
Parameter Description: Defines whether Remote or SBC should be refresher when
SBC terminates the Session Expire refreshing
```

3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
SBCSESSIONREFRESHINGPOLICY	1 (enables SBC as refresher of Session Timer)

4. Click the **Apply New Value** button.

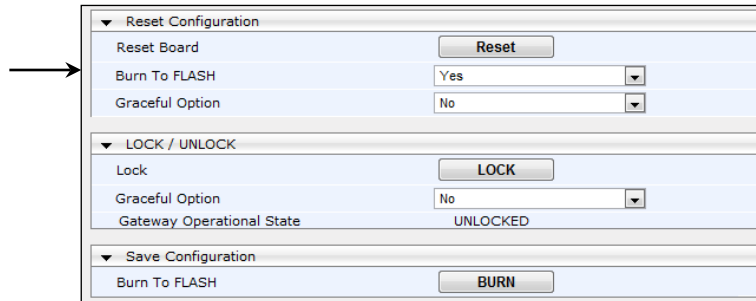
4.15 Step 15: Reset the E-SBC

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 4-57: Resetting the E-SBC



▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes ▼
Graceful Option	No ▼
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No ▼
Gateway Operational State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="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 31, is shown below:



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

```
[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'
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

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

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]

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

[PSTN Params]

[SS7 Params]
```

```
[Voice Engine Params]

ENABLEMEDIASEcurity = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'NextGenTel'
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]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCEsmode = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[ PhysicalPortsTable ]

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

[ \PhysicalPortsTable ]
```

```

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \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, 10.15.17.55, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.159, 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 0 = "SRDLan", "MRLan", 0, 0, -1, 1;
SRD 1 = "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 = "85.119.137.82:5060", 0, 2;

[ \ProxyIp ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_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_SBCRemoteMultipleAnswersMode,
IpProfile_SBCKeepVIAHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime;

IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 0, 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, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0, 300, 0, -1, -1, -1, -1;

IpProfile 2 = "NextGenTel", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 0, -1, 2,
2, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 3, 0, 1,
0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 300, 0, -1, -1, -1, -1;

[ \IpProfile ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, 0, "-1", -1, -1, "";
ProxySet 1 = "Lync", 1, 60, 1, 1, 0, 0, 0, "-1", 1, -1, "";
ProxySet 2 = "NextGenTel", 1, 60, 0, 0, 1, 0, 0, "-1", -1, -1, "503";

[ \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_SIPConnect;
IPGroup 1 = 0, "Lync", 1, "195.189.192.159", "", 0, -1, -1, 0, -1, 0,
"MRLan", 1, 1, -1, 1, 2, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "",
"", "", 0, "", "", 0;

```

```

IPGroup 2 = 0, "NextGenTel", 2, "195.189.192.159", "", 0, -1, -1, 0, -1,
1, "MRWan", 1, 2, -1, 3, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", 0, "", "", 0;

[ \IPGroup ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, 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, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to Lync", 2, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 1, "0", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]

[ SIPInterface ]

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

[ \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 0 = "Add +47 for incoming", 0, 2, -1, "*", "*",
"*, "*", "*", "", 0, -1, 0, 1, 0, 0, 255, "+47", "", 0;
IPOutboundManipulation 1 = "Remove +47 on Source", 0, 1, -1, "+", "*",
"*, "*", "*", "", 0, -1, 0, 0, 3, 0, 255, "", "", 0;
IPOutboundManipulation 2 = "+ -> 00 outgoing", 0, 1, 2, "*", "*", "+",
"*, "*", "", 0, -1, 0, 1, 1, 0, 255, "00", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup0 ]

[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g711Alaw64k";

[ \AllowedCodersGroup0 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Call Forward", 4, "", "header.history-info.0
regex (<sip:)(.47)(.*)"(.*)"(.*)", "header.from.url.user", 2, "$3", 0;
MessageManipulations 1 = "Call Forward", 4, "", "", "header.history-
info", 1, "", 1;
MessageManipulations 2 = "Call Park", 1, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;
MessageManipulations 3 = "Call Park", 1, "", "",
"param.message.sdp.rtpmode", 2, "'sendrecv'", 1;

```

```
MessageManipulations 4 = "Call Park", 2, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2, "'recvonly'", 0;
MessageManipulations 5 = "Call Park", 2, "", "", "var.call.src.0", 2,
"'0'", 1;
MessageManipulations 6 = "Call Transfer", 4, "", "header.referred-by
exists", "header.referred-by.url.host", 2, "header.from.url.host", 0;
MessageManipulations 7 = "Call Transfer", 4, "", "", "header.referred-
by.url.user", 6, "'+47'", 1;
MessageManipulations 8 = "Call Transfer", 4, "", "header.referred-by
exists", "header.from.url.user", 2, "header.referred-by.url.user", 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 ]
```

This page is intentionally left blank.



Configuration Note

