

AudioCodes® Mediant™ Series

Session Border Controller (SBC)

Interoperability Laboratory

Configuration Note

Microsoft® Lync™ Server 2013 & ITSP SIP Trunk using AudioCodes Mediant SBC



Microsoft Partner
Gold Communications



Version 6.8

May 2015

Document #: LTRT-54010

Table of Contents

1	Introduction	9
1.1	Intended Audience	9
1.2	About AudioCodes SBC Product Series	9
2	Component Information.....	11
2.1	AudioCodes SBC Version	11
2.2	Microsoft Lync Server 2013 Version	11
2.3	Deploying the SBC.....	12
2.3.1	Example Environment.....	12
2.3.2	Environment Setup	13
3	Configuring Microsoft Lync Server 2013	15
3.1	Configuring the SBC as an IP / PSTN Gateway	15
3.2	Configuring 'Route' on Lync Server 2013.....	24
4	Configuring AudioCodes SBC	35
4.1	Step 1: Configuring the SBC's Network Interfaces.....	36
4.1.1	Step 1a: Create Ethernet Port Groups for Port Redundancy	37
4.1.2	Step 1b: Configure the Native VLAN ID	38
4.1.3	Step 1c: Configure VLANs.....	39
4.1.4	Step 1d: Configure IP Network Interfaces for LAN and WAN	40
4.2	Step 2: Enable the SBC Application.....	42
4.3	Step 3: Configuring SRDs	43
4.3.1	Step 3a: Configure Media Realms.....	43
4.3.2	Step 3b: Configure SRDs	45
4.3.3	Step 3c: Configure SIP Signaling Interfaces	47
4.4	Step 4: Configure Proxy Sets.....	48
4.5	Step 5: Configure IP Groups	51
4.6	Step 6: Configure IP Profiles.....	53
4.7	Step 7: Configure Coders.....	58
4.8	Step 8: Configure SIP TLS Connection.....	61
4.8.1	Step 8a: Configure the NTP Server Address.....	61
4.8.2	Step 8b: Configure a Certificate	62
4.9	Step 9: Configure SRTP	67
4.10	Step 10: Configure IP Media	68
4.11	Step 11: Configure IP-to-IP Call Routing Rules	69
4.12	Step 12: Configure IP-to-IP Manipulation Rules	74
4.13	Step 13: Configure SIP Message Manipulation Rules	76
4.14	Step 14: Configure Registration Account	78
4.15	Step 15: Configure Miscellaneous SBC Functions	79
4.15.1	Step 15a: Configure Call Forking Mode	79
4.15.2	Step 15b: Configure SBC Alternative Routing Reasons	80
4.16	Step 16: Reset the SBC	81
A	Configuring SBC to Send 414 Request-URI Too Long.....	83

List of Figures

Figure 2-1: SBC Interworking Lync 2013 and a SIP Trunk in an Example Environment.....	12
Figure 3-1: Starting the Lync Server Topology Builder	15
Figure 3-2: Topology Builder Options.....	16
Figure 3-3: Save Topology	16
Figure 3-4: Topology Builder Displaying Downloaded Topology	17
Figure 3-5: Selecting New IP/PSTN Gateway	17
Figure 3-6: Define New IP/PSTN Gateway	18
Figure 3-7: Define the IP Address	19
Figure 3-8: Define the Root Trunk.....	20
Figure 3-9: SBC Added as an IP/PSTN Gateway and Trunk Created.....	21
Figure 3-10: Selecting 'Publish Topology' from the 'Action' Menu	21
Figure 3-11: Publish Topology	22
Figure 3-12: Publish Topology Progress Screen	23
Figure 3-13: Publish Topology Successfully Completed.....	23
Figure 3-14: Opening the Lync Server Control Panel	24
Figure 3-15: Lync Server Credentials.....	25
Figure 3-16: Microsoft Lync Server 2013 Control Panel	25
Figure 3-17: Voice Routing.....	26
Figure 3-18: Route Option.....	27
Figure 3-19: Adding New Voice Route	27
Figure 3-20: Adding New Trunk	28
Figure 3-21: List of Deployed Trunks	29
Figure 3-22: Selected SBC Trunk	29
Figure 3-23: Associating PSTN Usage with the Route	30
Figure 3-24: Confirmation of New Voice Route.....	30
Figure 3-25: Committing Voice Routes	31
Figure 3-26: Uncommitted Voice Configuration Settings	31
Figure 3-27: Confirmation of a Successful Voice Routing Configuration	31
Figure 3-28: Voice Routing Screen Displaying Committed Routes.....	32
Figure 3-29: Voice Routing Screen – Trunk Configuration Tab	32
Figure 3-30: Edit Trunk Configuration - Global.....	33
Figure 4-1: Network Interfaces	36
Figure 4-2: Configured Ethernet Groups Table Example.....	37
Figure 4-3: Configured Port Native VLAN	38
Figure 4-4: Configured VLAN IDs in Ethernet Device Table	39
Figure 4-5: Interface Table	40
Figure 4-6: Configured Network Interface in IP Interfaces Table	41
Figure 4-7: Applications Enabling.....	42
Figure 4-8: Configuring a LAN Media Realm	43
Figure 4-9: Configuring a WAN Media Realm	44
Figure 4-10: Required Media Realm Table	44
Figure 4-11: Configuring the LAN SRD Example.....	45
Figure 4-12: Configuring the WAN SRD.....	46
Figure 4-13: Configured SRDs in SRD Table.....	46
Figure 4-14: Required SIP Interface Table.....	47
Figure 4-15: Proxy Set for Microsoft Lync Server 2013	49
Figure 4-16: Configuring a Proxy Set for the ITSP SIP Trunk.....	50
Figure 4-17: Configured IP Group Table	52
Figure 4-18: Configured IP Profile for Lync Server 2013 – Common	54
Figure 4-19: Configured IP Profile for Lync Server 2013 – SBC.....	55
Figure 4-20: Configured IP Profile for SIP Trunk.....	56
Figure 4-21: Configured IP Profile for SIP – SBC	57
Figure 4-22: Configured Coder Group for Lync Server 2013.....	58
Figure 4-23: Configured Coder Group for the SIP Trunk	58
Figure 4-24: Allowed Audio Coders Group for SIP Trunk	59
Figure 4-25: SBC Preferences Mode	60
Figure 4-26: Configuring the NTP Server IP Address	61

Figure 4-27: Certificates Page - Creating CSR	62
Figure 4-28: Microsoft Certificate Services Web Page	63
Figure 4-29: Request a Certificate Page	63
Figure 4-30: Advanced Certificate Request Page	64
Figure 4-31: Submit a Certificate Request or Renewal Request Page	64
Figure 4-32: Certificate Issued Page	65
Figure 4-33: Download a CA Certificate, Certificate Chain, or CRL	65
Figure 4-34: Upload Device Certificate Files from your Computer Group	66
Figure 4-35: Importing Root Certificate into Trusted Certificates Store	66
Figure 4-36: Media Security Page	67
Figure 4-37: IP Media Settings	68
Figure 4-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab	70
Figure 4-39: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab	70
Figure 4-40: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab	71
Figure 4-41: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab	72
Figure 4-42: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab	72
Figure 4-43: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab	73
Figure 4-44: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table	73
Figure 4-45: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab	74
Figure 4-46: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab	75
Figure 4-47: Example of Configured IP-to-IP Outbound Manipulation Rules	75
Figure 4-48: Message Manipulations Page	76
Figure 4-49: Configured SIP Message Manipulation Rule	77
Figure 4-50: Assigning a Manipulation Rule to IP Group 2	77
Figure 4-51: Configuring a SIP Registration Account	78
Figure 4-52: Configuring Forking Mode	79
Figure 4-53: Alternative Routing Reasons Table - Add Record	80
Figure 4-54: Resetting the SBC	81
Figure A-1: Configuring a Condition for the Route	83
Figure A-2: IP-to-IP Routing Rule for Long-URI Calls	84
Figure A-3: IP-to-IP Routing Action for Long-URI Calls	84
Figure A-4: Manipulation Rule to Set a Variable to '1' in Case of Long-URI Call	85
Figure A-5: Manipulation Rule to Convert 408 to '414'	86
Figure A-6: Message Manipulations Page	86
Figure A-7: Assigning Manipulation Rule to IP Group 1	86

This page is intentionally left blank.

Notice

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

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

© Copyright 2015 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: May-17-2015

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Abbreviations and Conventions

Each abbreviation, unless widely used, is spelled out in full when first used.



Note: Throughout this manual, unless otherwise specified, the term *SBC* refers to AudioCodes Mediant SBC product.

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>.

Document Revision Record

LTRT	Description
54010	Added 'Encryption Support Level'.

1 Introduction

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

This document describes how to connect Microsoft Lync Server 2013 and a SIP Trunk using AudioCodes Mediant SBC product series (see Section 2.1 on page 11).



Note: Throughout this manual, unless otherwise specified, the term *SBC* refers to AudioCodes Mediant SBC product.

1.1 Intended Audience

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

1.2 About AudioCodes SBC Product Series

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

The 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 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' 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 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 2600 E-SBC▪ Mediant 3000 Gateway & E-SBC▪ Mediant 4000 SBC▪ Mediant 9000 SBC
Software Version	SIP_6.80A or later
Protocol	<ul style="list-style-type: none">▪ SIP/UDP (to the ITSP's SIP Trunk)▪ SIP/TCP or TLS (to the Lync Front End Server)
Additional Notes	None

2.2 Microsoft Lync Server 2013 Version

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

2.3 Deploying the SBC

2.3.1 Example Environment

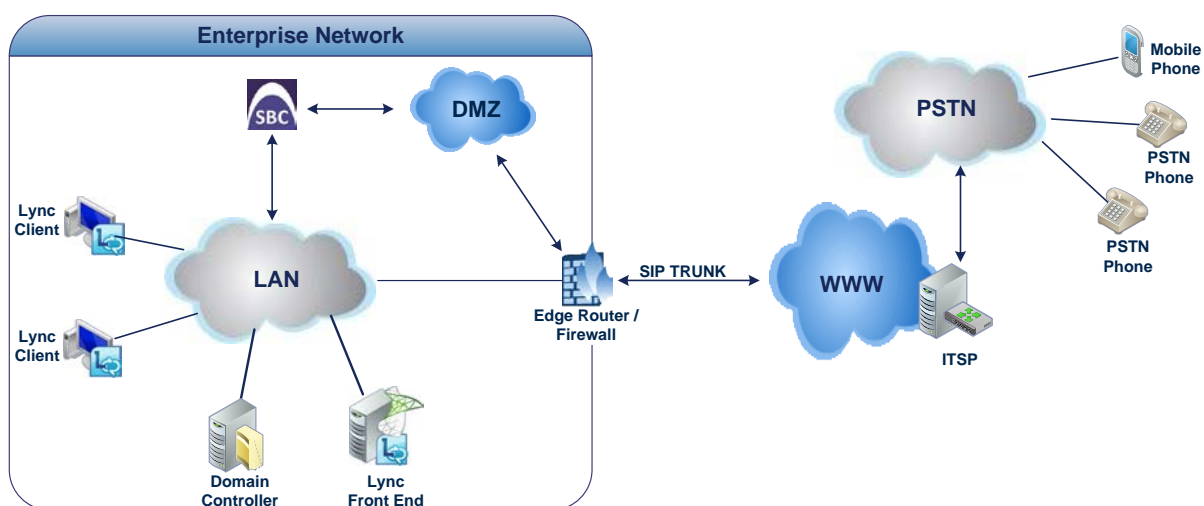
The example scenario below is referred to throughout this document in order to show how to deploy the SBC.

In the example environment:

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

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

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



2.3.2 Environment Setup

The example scenario includes the following environment setup:

Area	Setup
Network	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 environment is located in the enterprise's LAN▪ The SIP Trunk is located in the WAN
Signaling Transcoding	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 functions with SIP-over-TLS transport type▪ The SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders▪ The SIP Trunk supports G.711A-law, G.711U-law and G.729 coders
Media Transcoding	<ul style="list-style-type: none">▪ Microsoft Lync Server 2013 operates with SRTP media type▪ The SIP trunk operates with RTP media type

This page is intentionally left blank.

3 Configuring Microsoft Lync Server 2013

The procedure below describes how to configure Microsoft Lync Server 2013 to operate with AudioCodes' SBC.



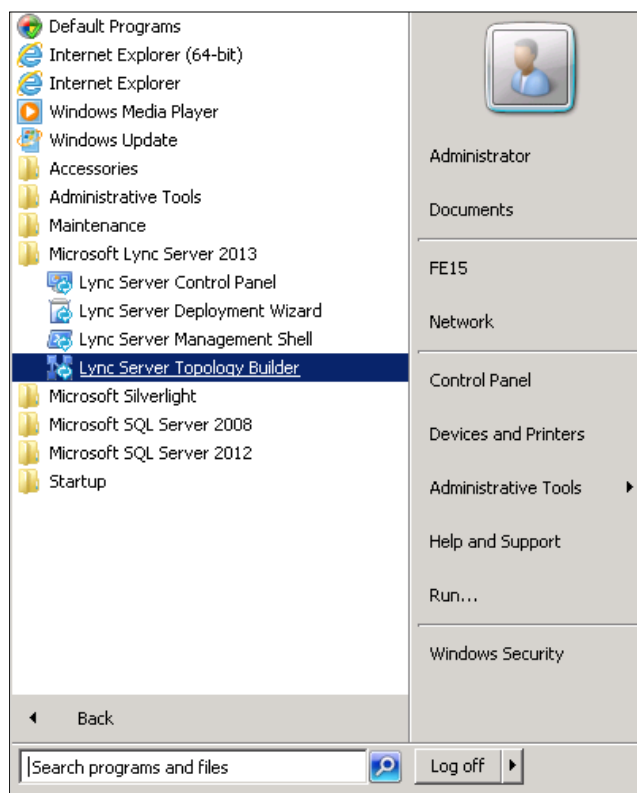
Note: Dial plans, voice policies, and PSTN usages are also necessary for enterprise voice deployment but are beyond the scope of this document.

3.1 Configuring the SBC as an IP / PSTN Gateway

The procedure below describes how to configure the SBC as an IP / PSTN Gateway.

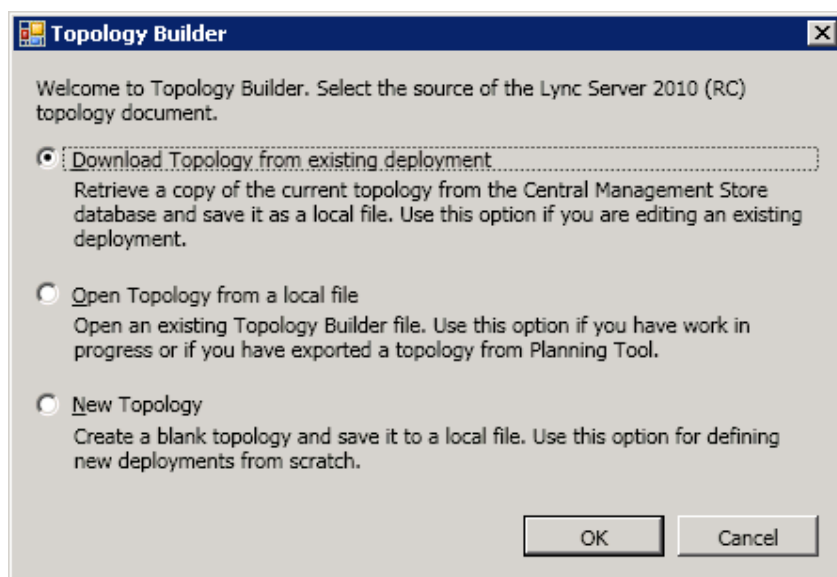
- **To configure the SBC as an IP/PSTN Gateway and associate it with a Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder: Click the Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**.

Figure 3-1: Starting the Lync Server Topology Builder



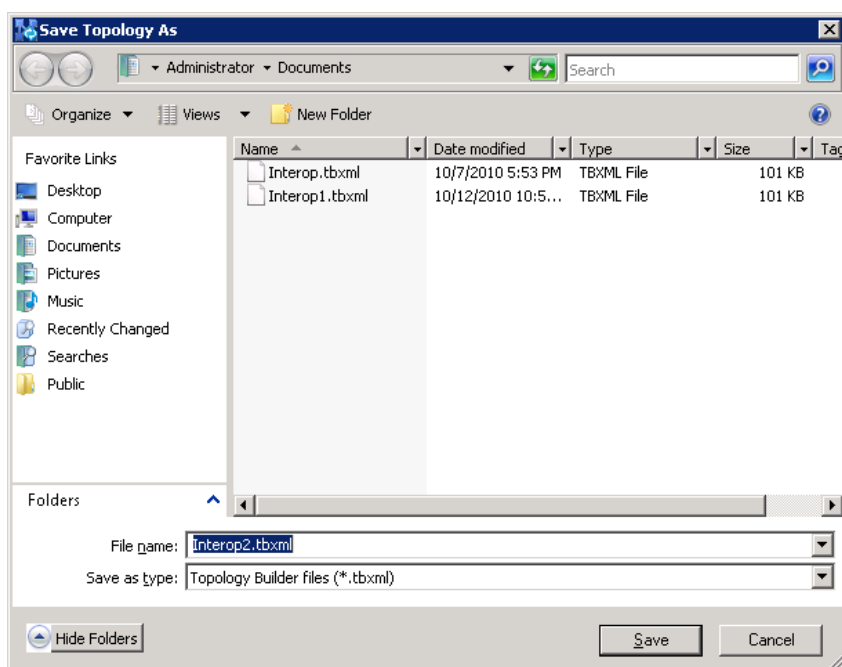
This screen is displayed:

Figure 3-2: Topology Builder Options



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

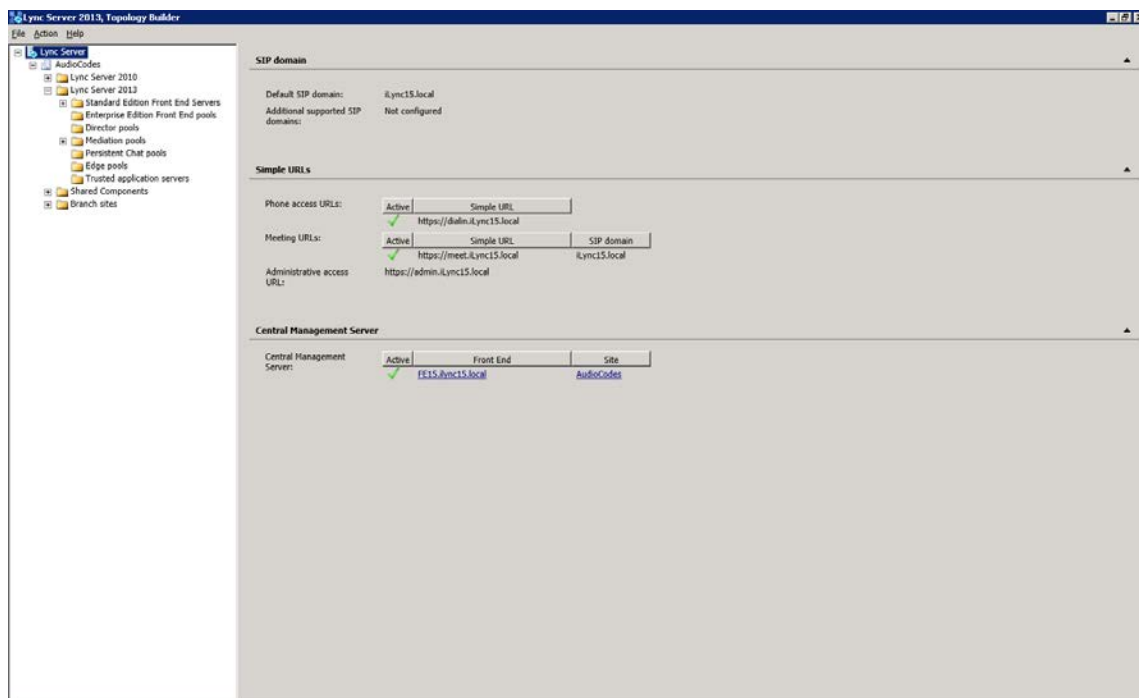
Figure 3-3: Save Topology



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

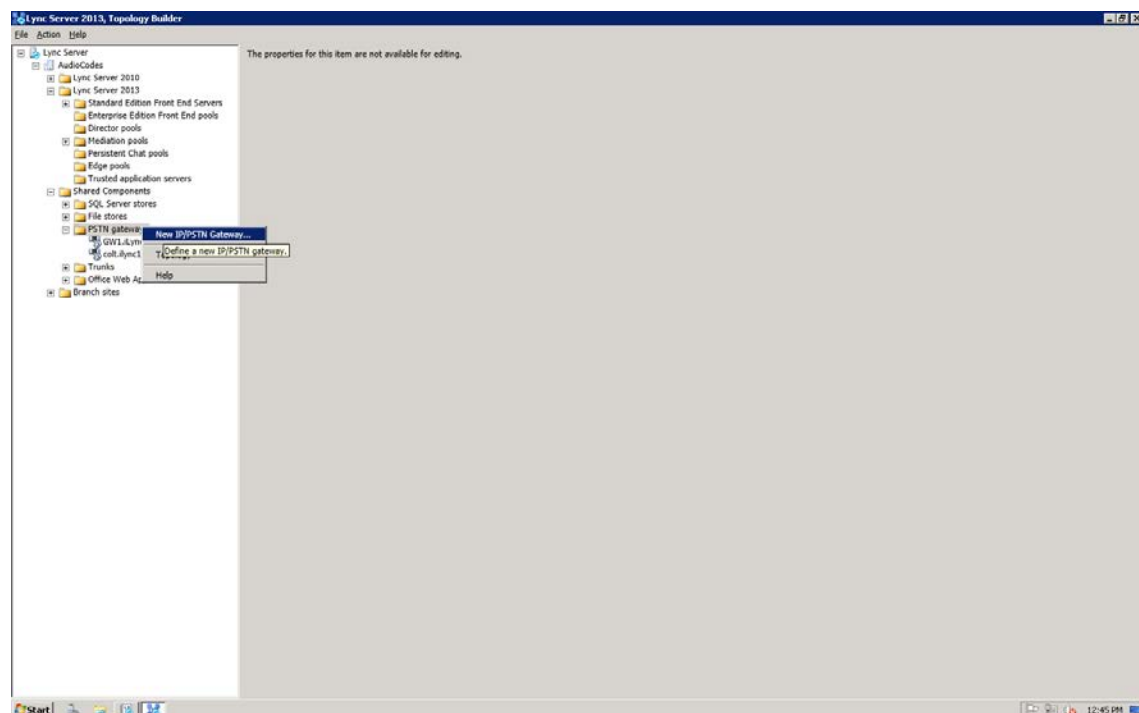
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Topology Builder Displaying Downloaded Topology



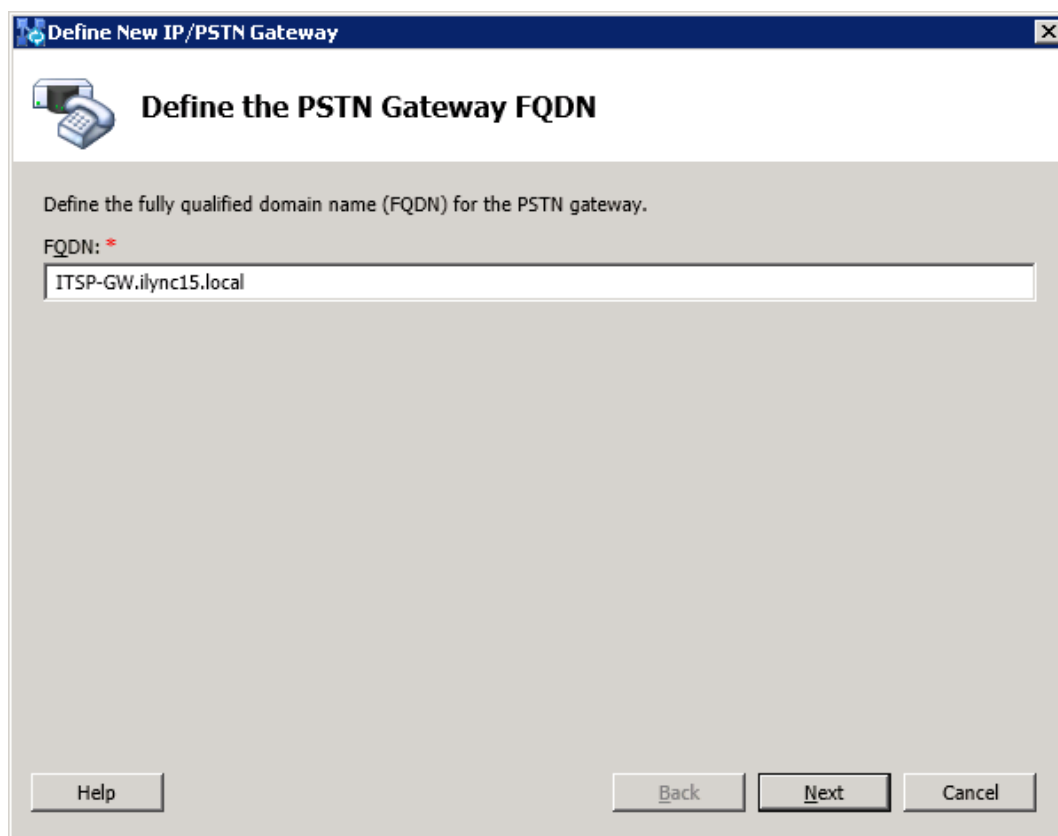
4. In the tree, expand Lync Server 2013 > your site name > Shared Components.
5. Right-click the **PSTN Gateways** folder and select **New IP/PSTN Gateway** from the popup menu:

Figure 3-5: Selecting New IP/PSTN Gateway



The following dialog opens:

Figure 3-6: Define New IP/PSTN Gateway



Define New IP/PSTN Gateway

Define the PSTN Gateway FQDN

Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

ITSP-GW.ilync15.local

Help Back Next Cancel

6. Enter the Fully Qualified Domain Name (FQDN) of the SBC (e.g., ITSP-GW.ilync15.local). This FQDN should be updated in the relevant DNS record and then, click **Next**.

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

Figure 3-7: Define the IP Address

Define New IP/PSTN Gateway

Define the IP address

☒ **Enable IPv4**

☒ Use all configured IP addresses.

☐ Limit service usage to selected IP addresses.

PSTN IP address:

☐ **Enable IPv6**

☒ Use all configured IP addresses.

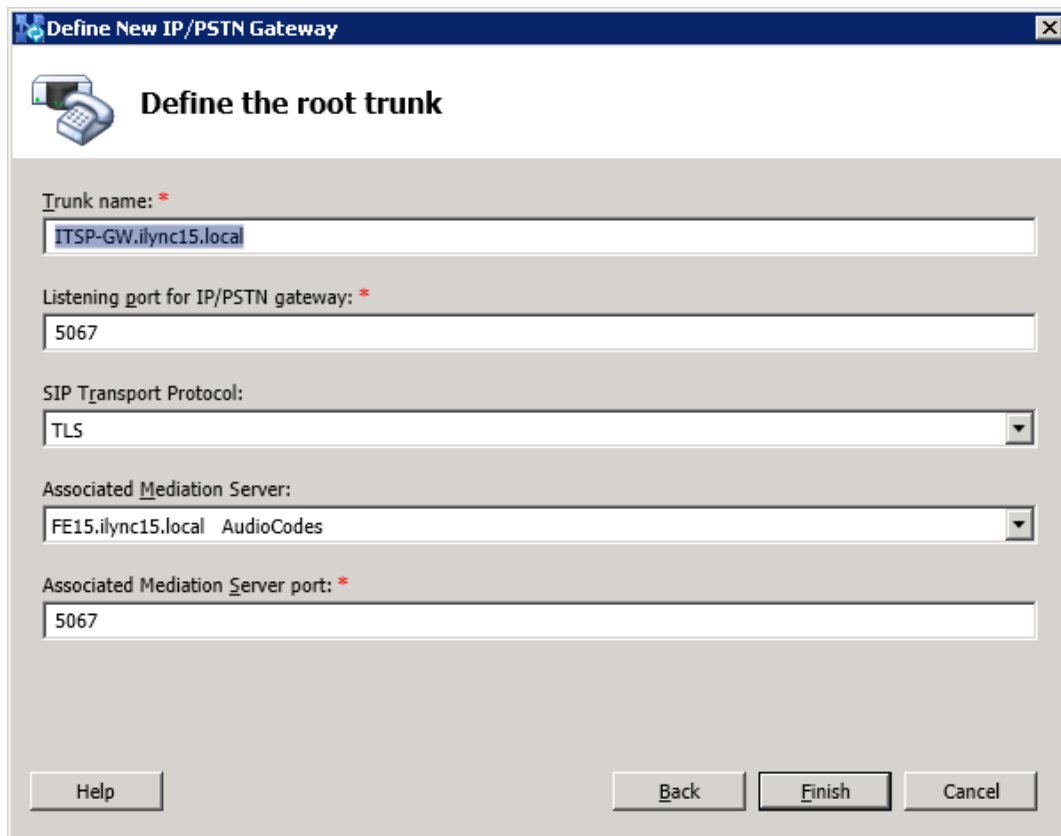
☐ Limit service usage to selected IP addresses.

PSTN IP address:

Help Back Next Cancel

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

Figure 3-8: Define the Root Trunk



Define the root trunk

Trunk name: *

ITSP-GW.ilync15.local

Listening port for IP/PSTN gateway: *

5067

SIP Transport Protocol:

TLS

Associated Mediation Server:

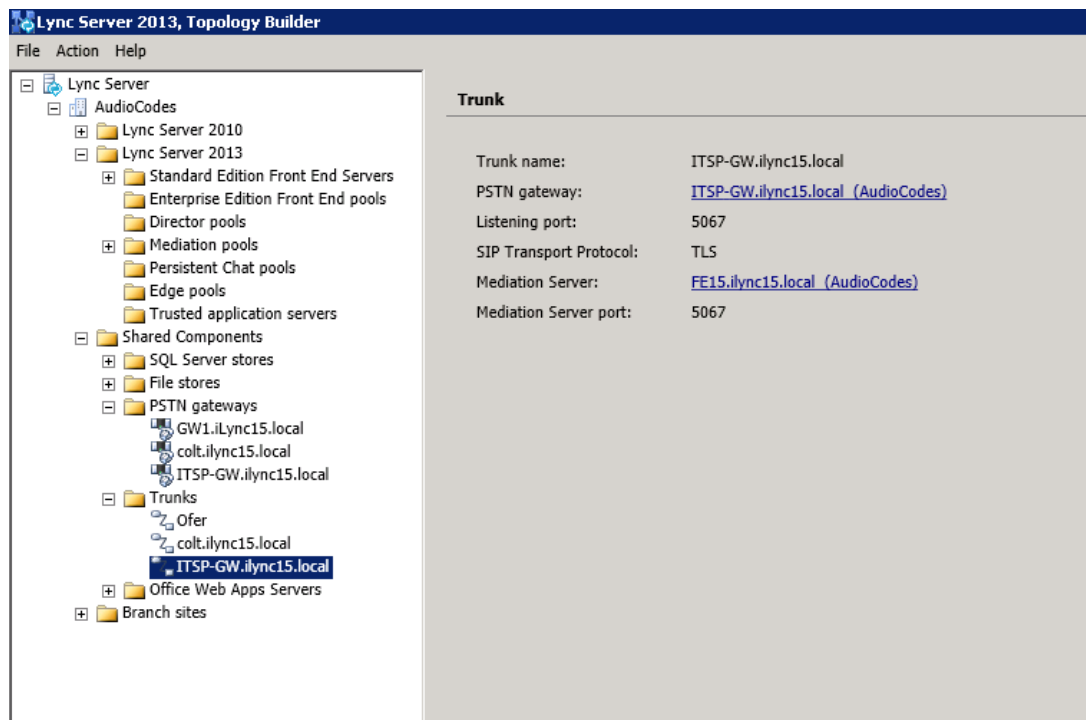
FE15.ilync15.local AudioCodes

Associated Mediation Server port: *

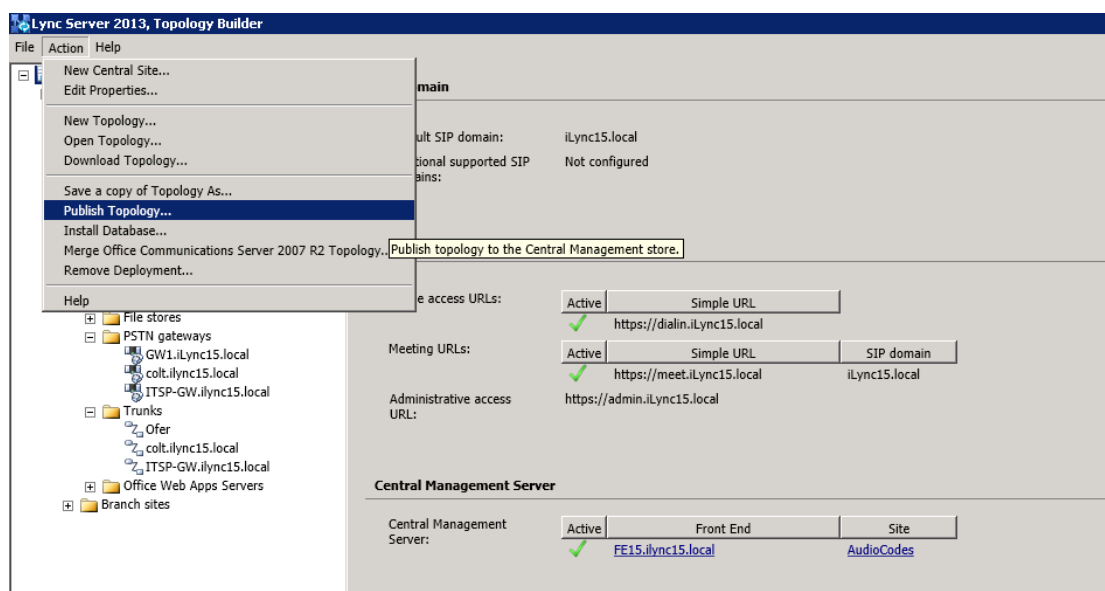
5067

Help Back Finish Cancel

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

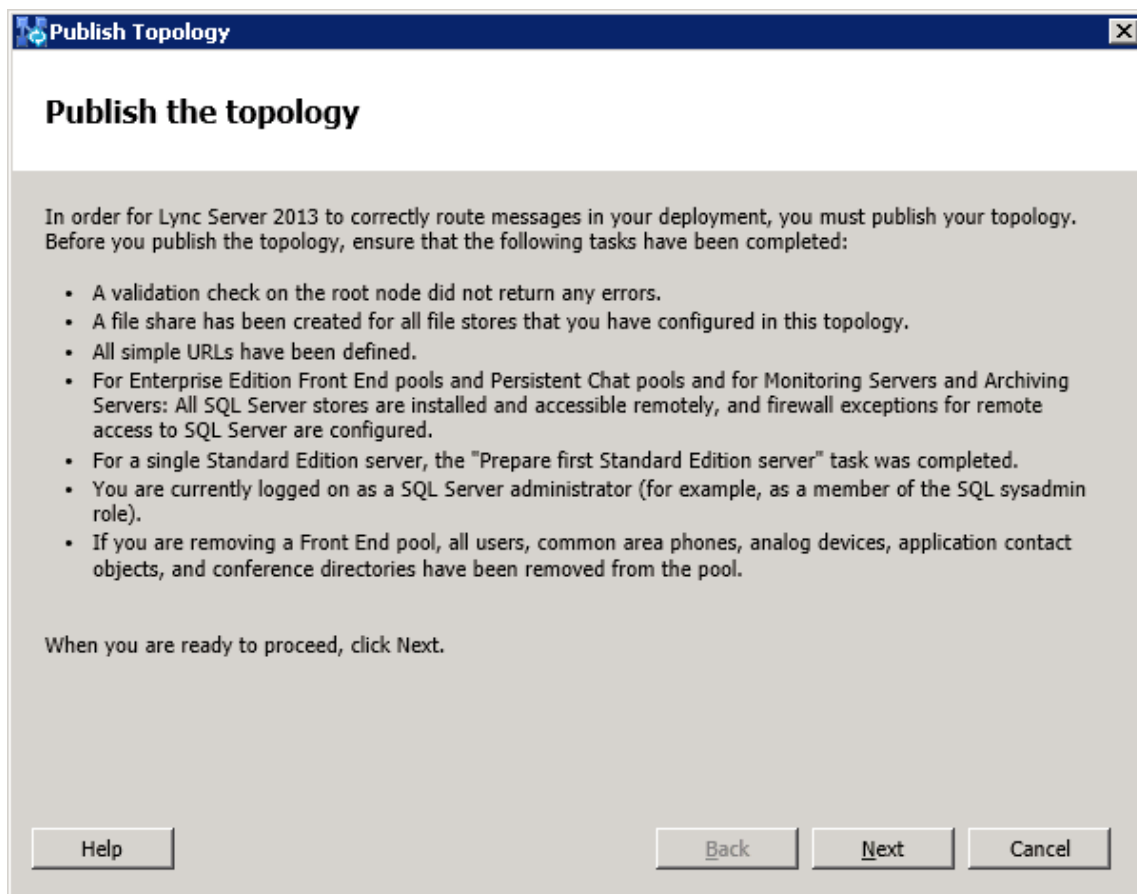
Figure 3-9: SBC Added as an IP/PSTN Gateway and Trunk Created

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

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

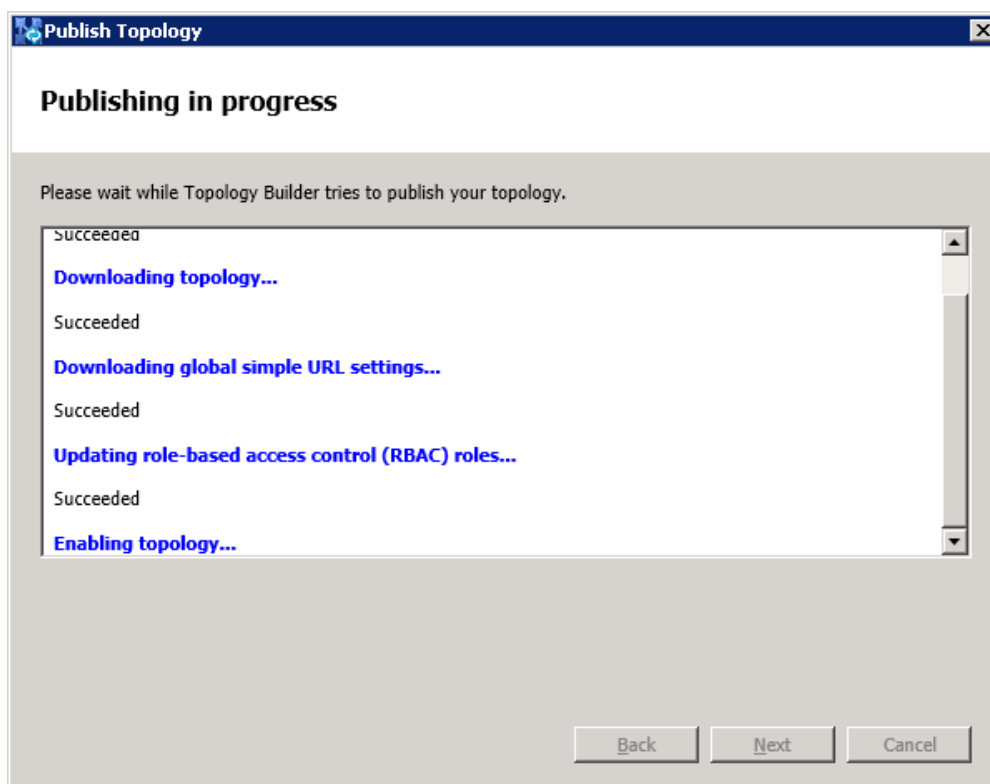
The Publish Topology screen is displayed:

Figure 3-11: Publish Topology



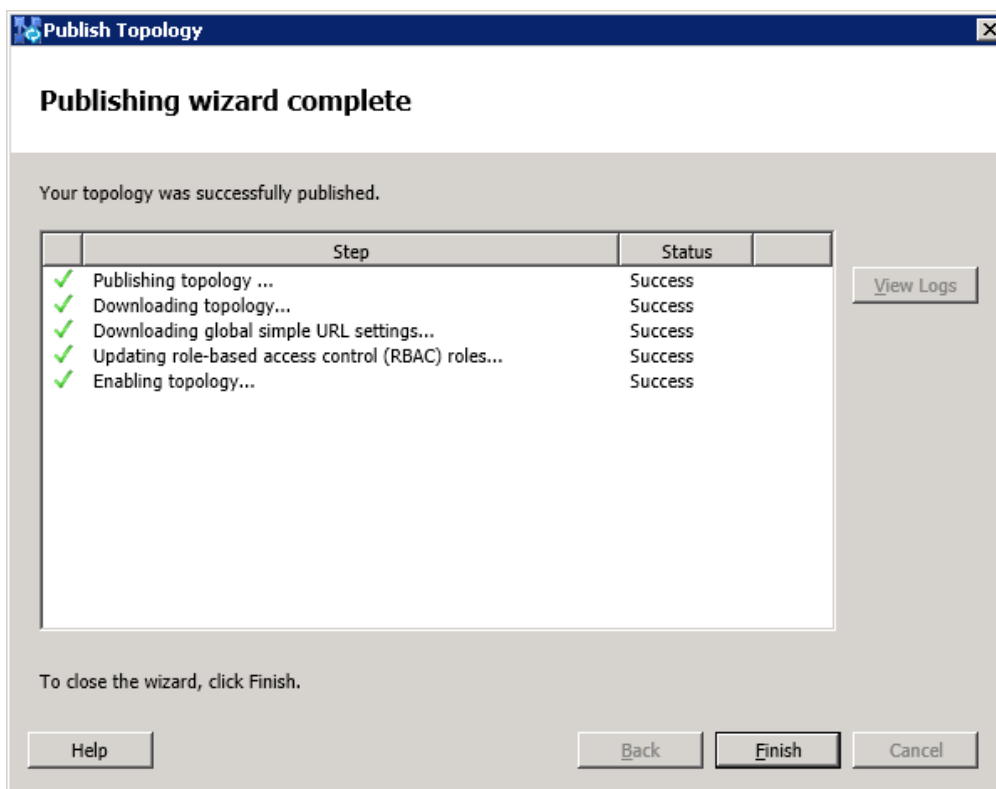
11. Click **Next**; the Topology Builder starts publishing your topology:

Figure 3-12: Publish Topology Progress Screen



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

Figure 3-13: Publish Topology Successfully Completed



13. Click **Finish**.

3.2 Configuring 'Route' on Lync Server 2013

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

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

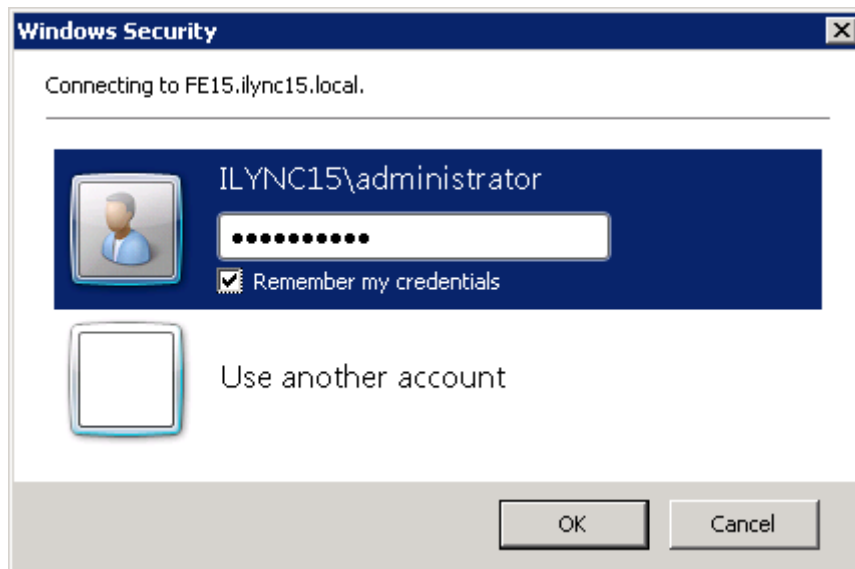
1. Start the Microsoft Lync Server 2013 Control Panel: Click **Start > All Programs > Microsoft Lync Server 2013** and then click **Lync Server Control Panel**:

Figure 3-14: Opening the Lync Server Control Panel



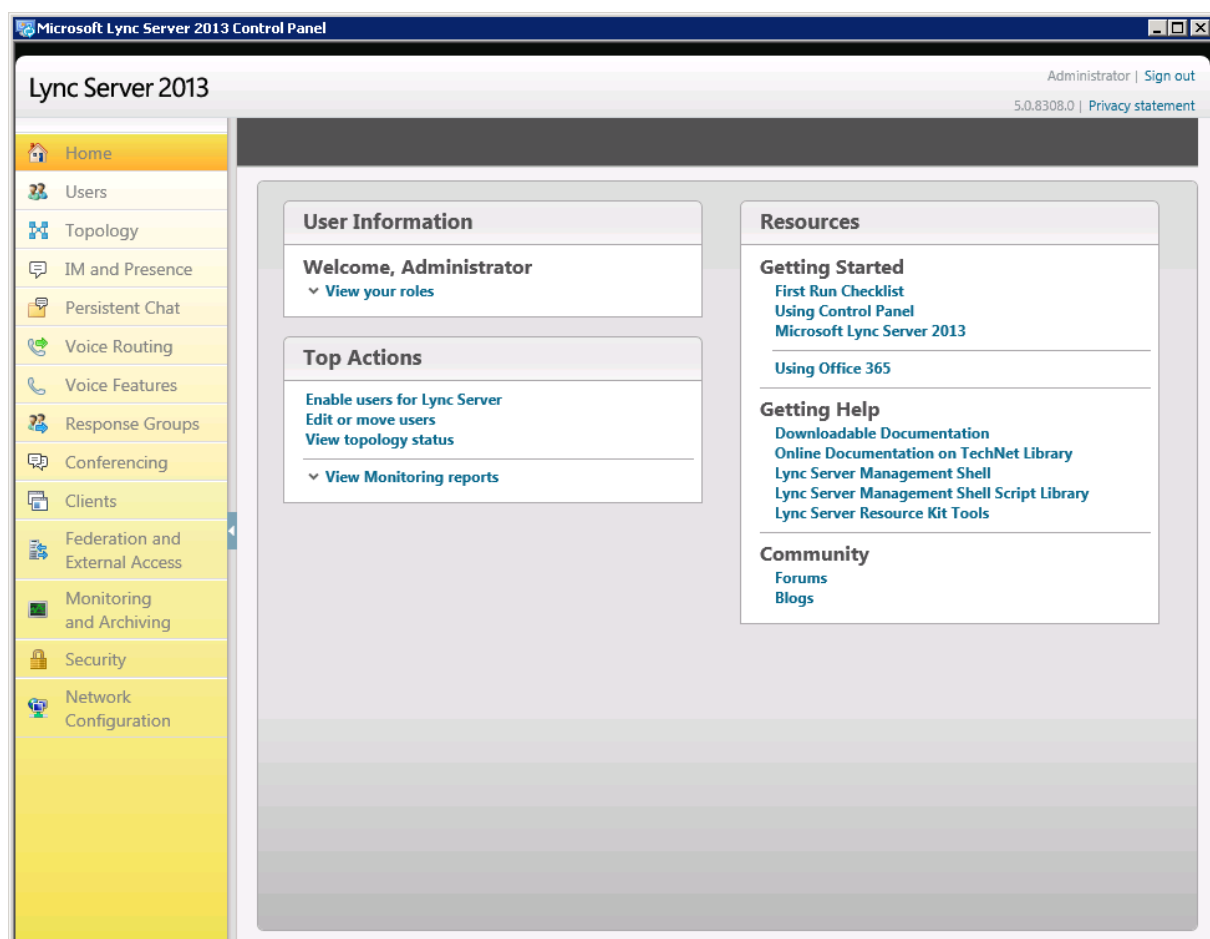
2. You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials

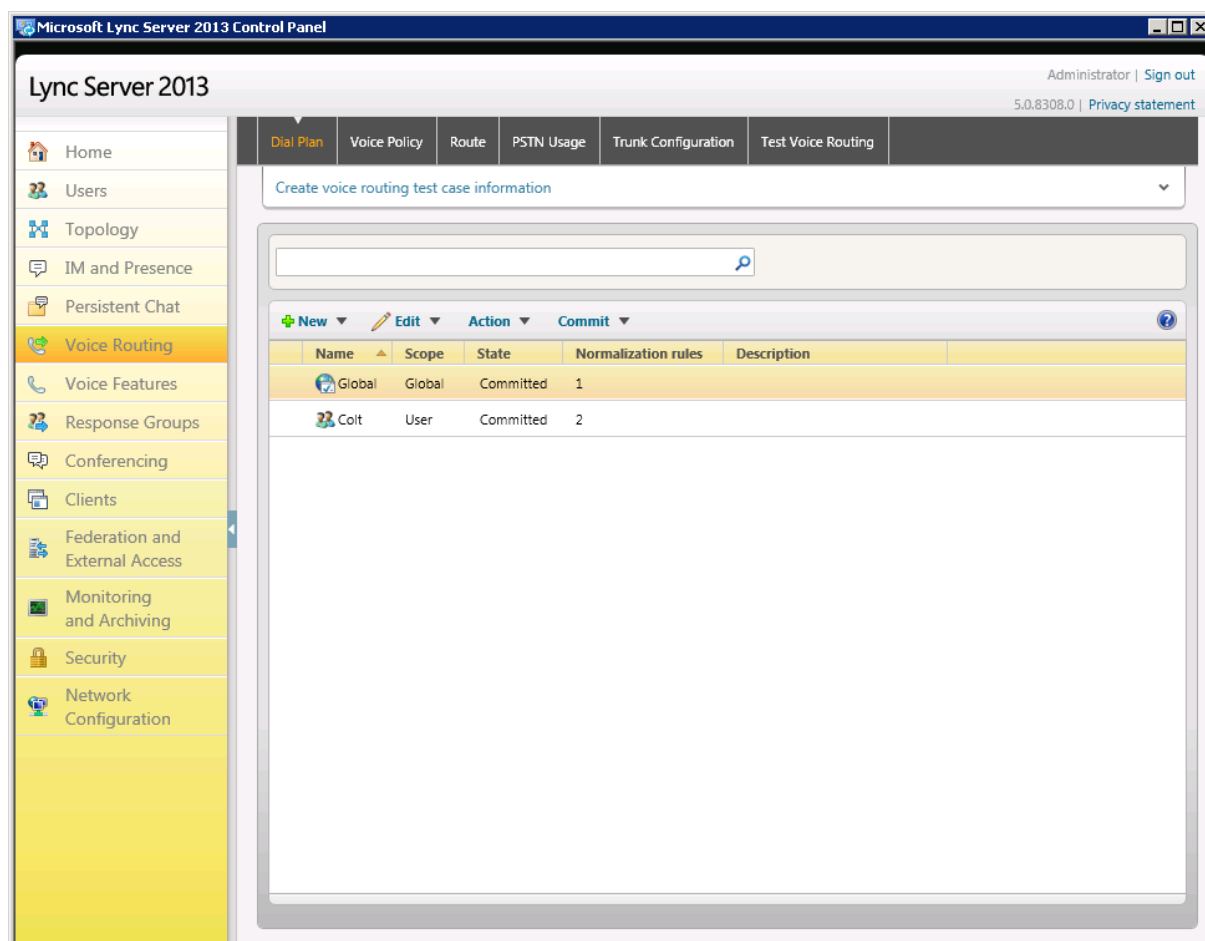


3. Enter your domain 'User name' and 'Password' and click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel

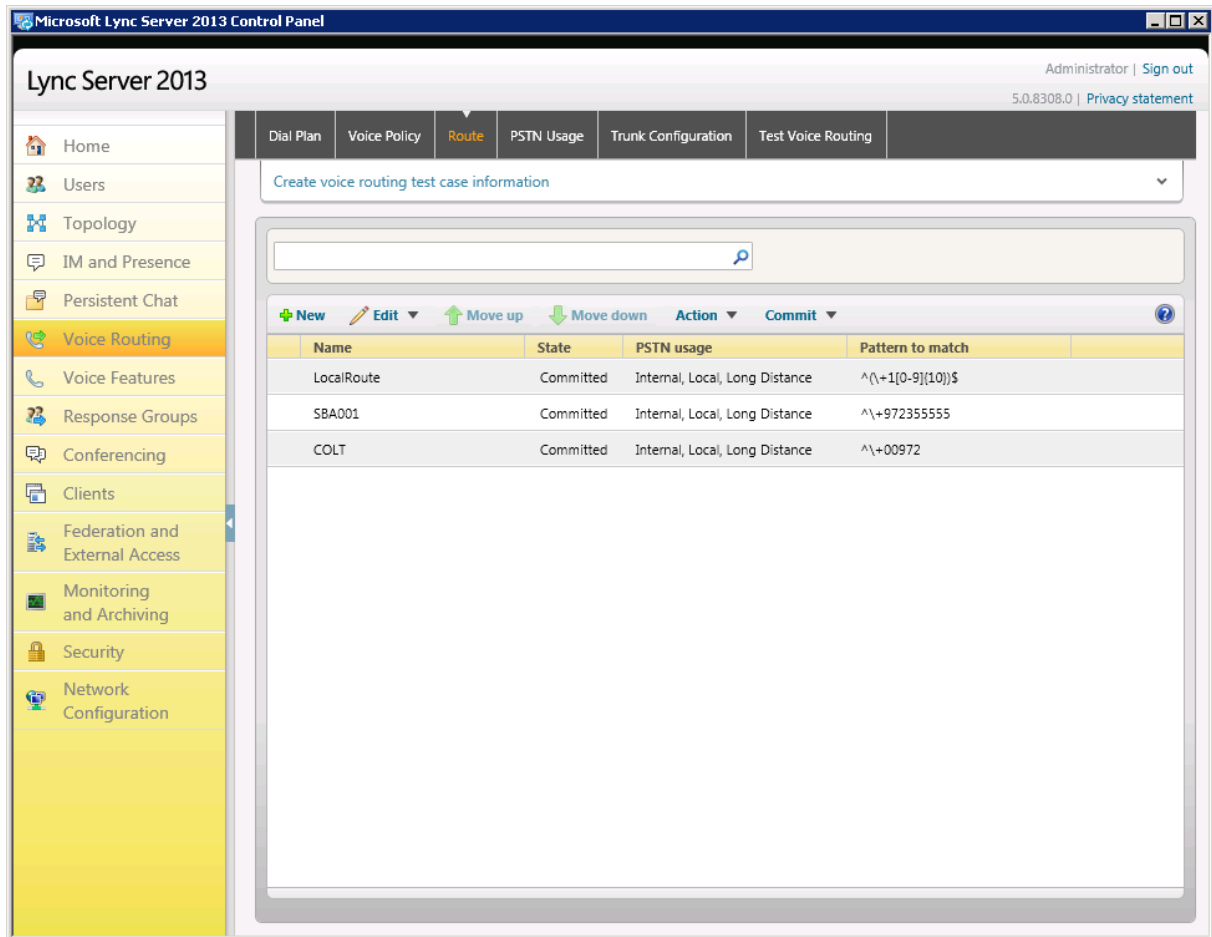


4. In the left navigation pane, select **Voice Routing**:

Figure 3-17: Voice Routing


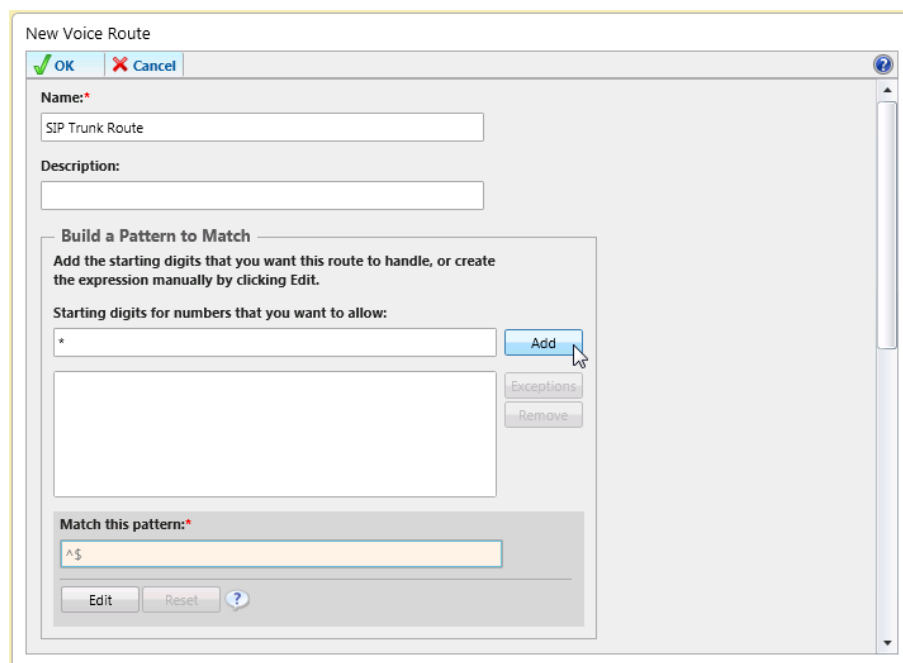
5. In the Voice Routing page, click the **Route** tab:

Figure 3-18: Route Option



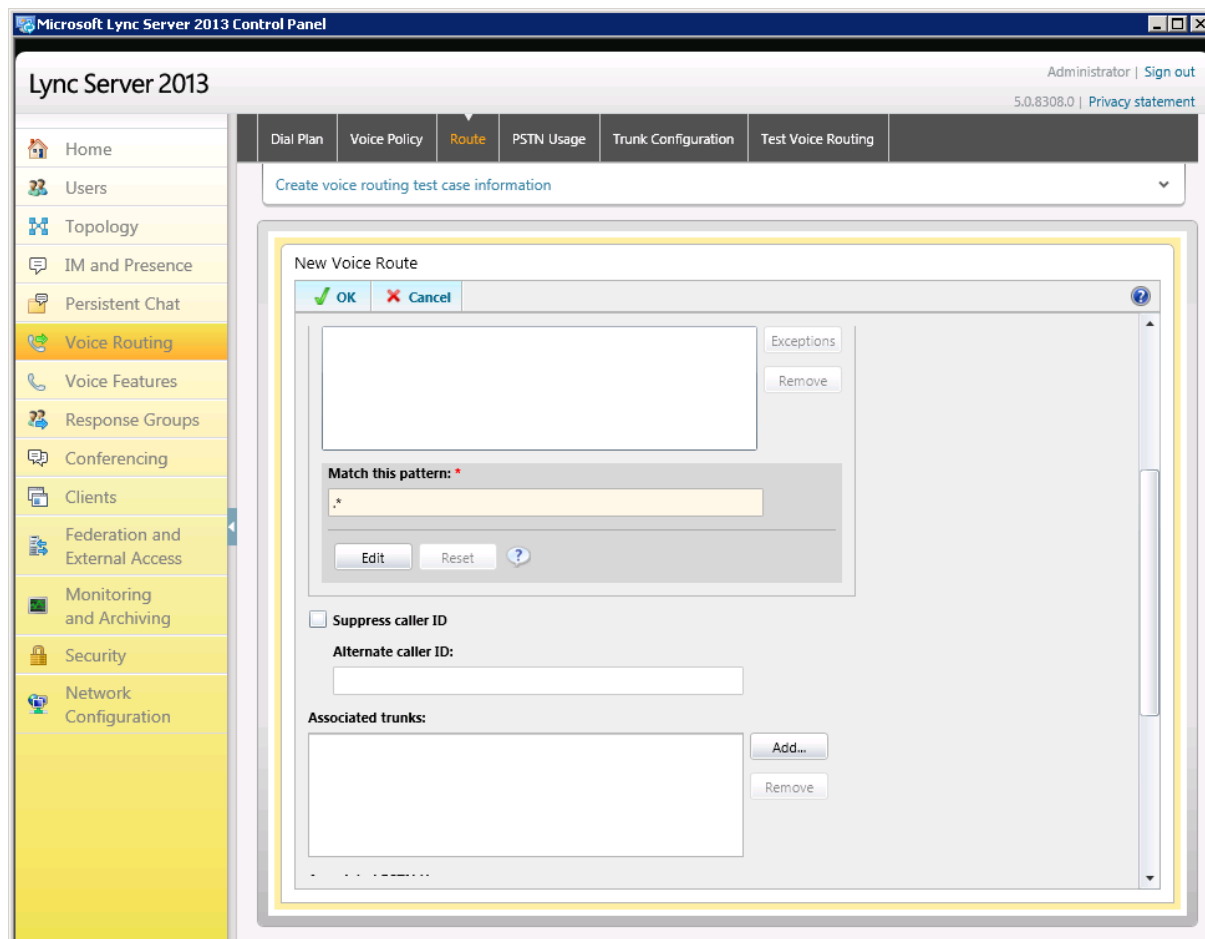
6. Click **New**; the New Voice Route dialog opens:

Figure 3-19: Adding New Voice Route

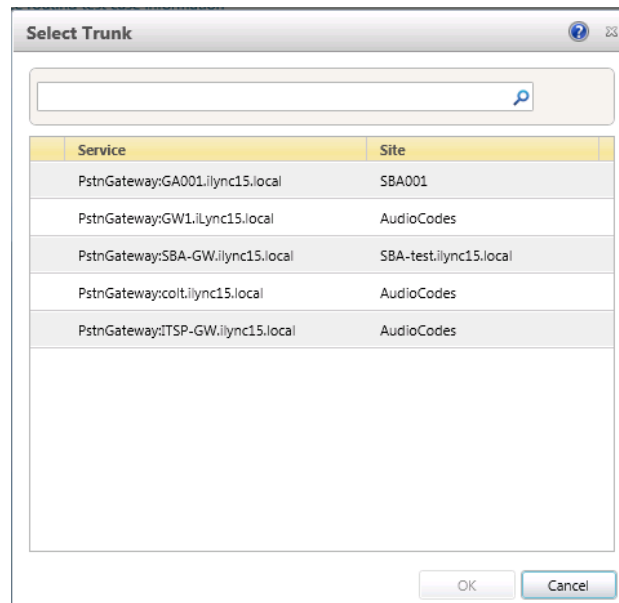


7. In the 'Name' field, enter a name for this route (e.g., SIP Trunk Route).
8. In the 'Build a Pattern to Match' field, enter the starting digits you want this route to handle (e.g., *, i.e., to match all numbers).
9. Click **Add**.

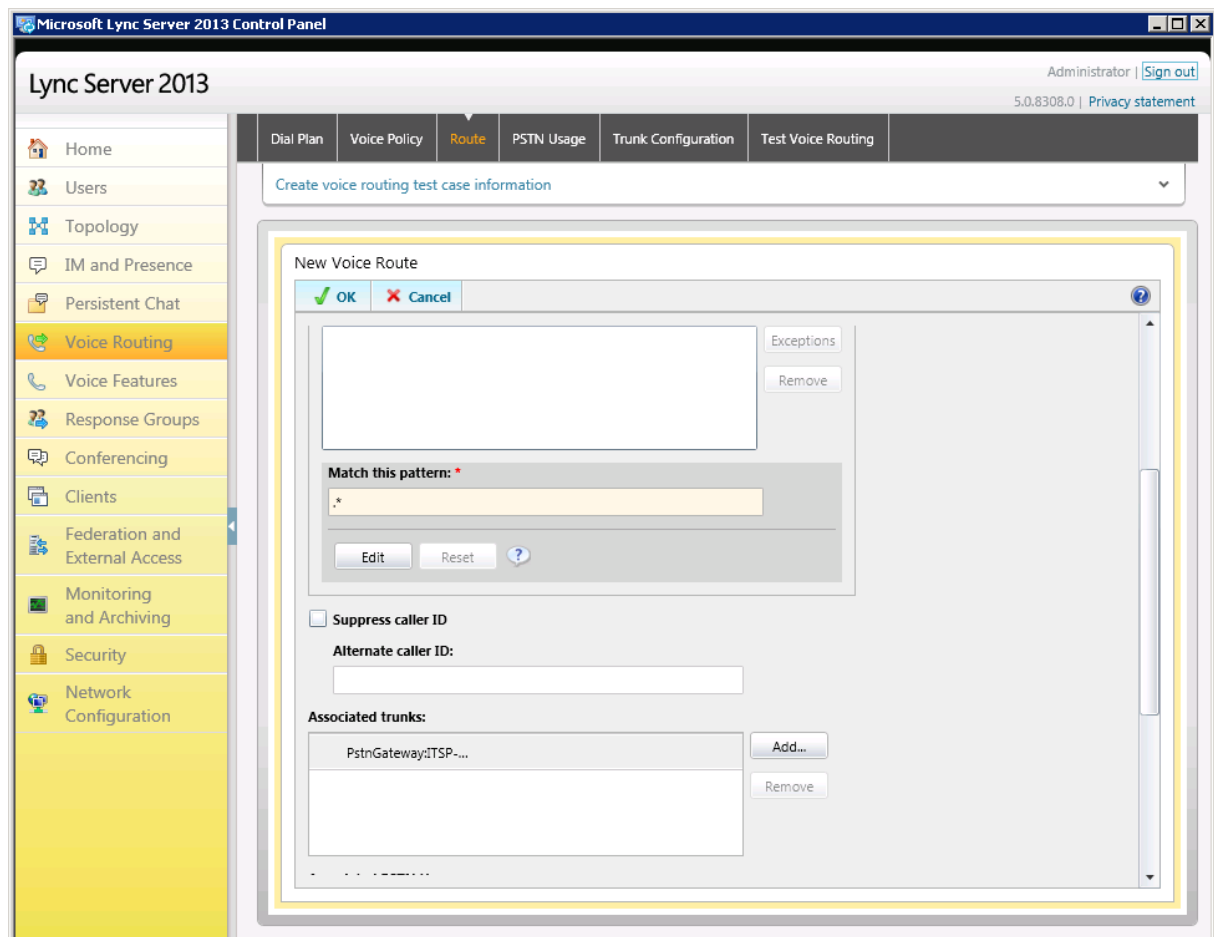
Figure 3-20: Adding New Trunk



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

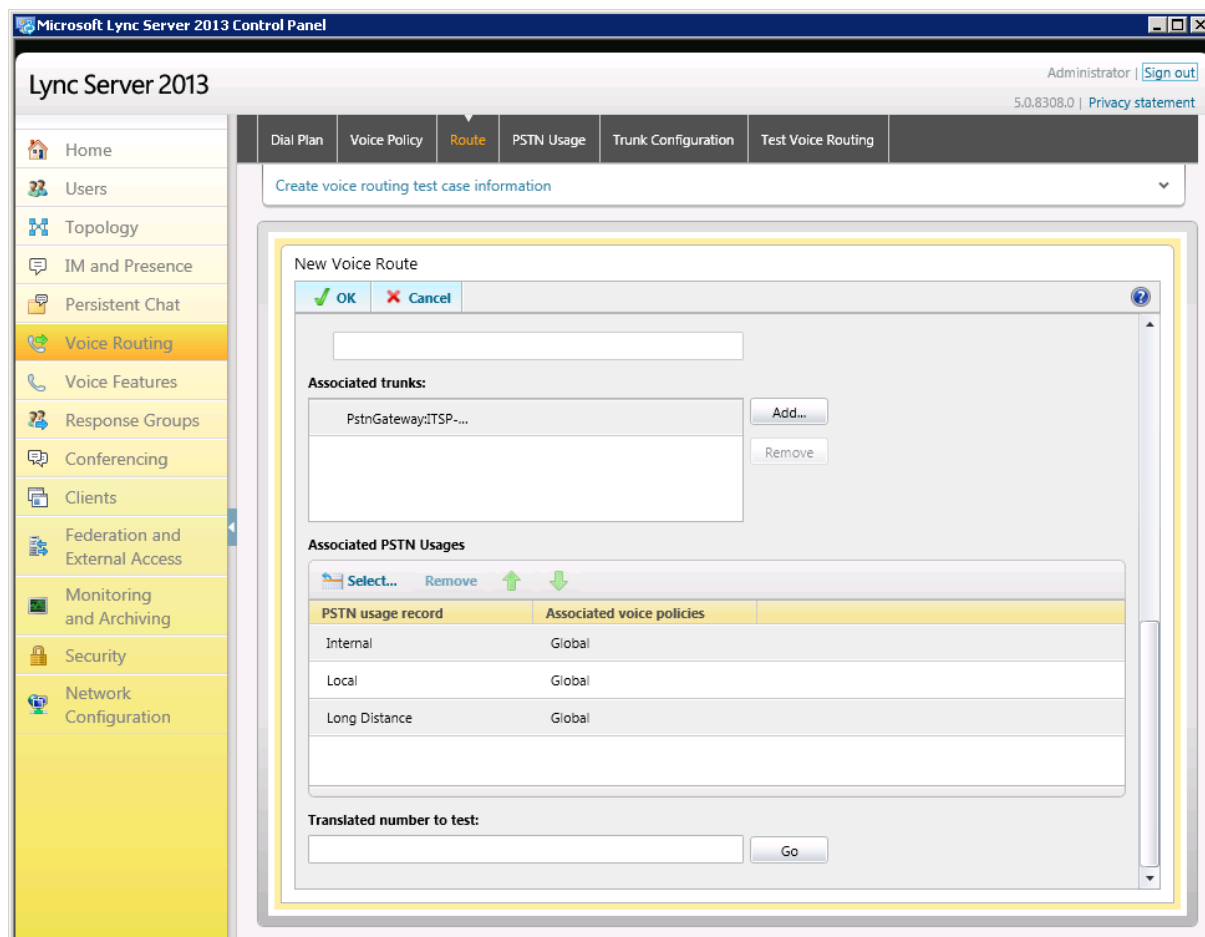
Figure 3-21: List of Deployed Trunks

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

Figure 3-22: Selected SBC Trunk

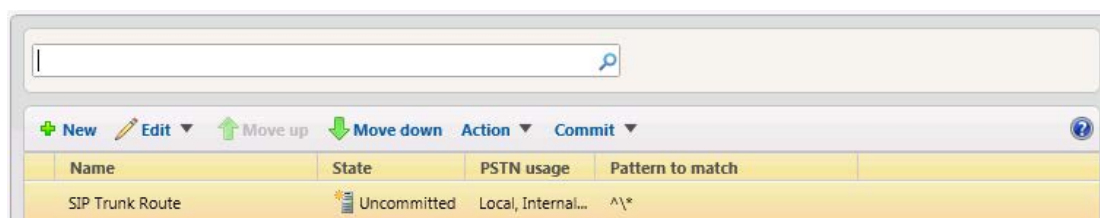
11. Associate a PSTN Usage with this route: In the Associated PSTN Usages group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage with the Route



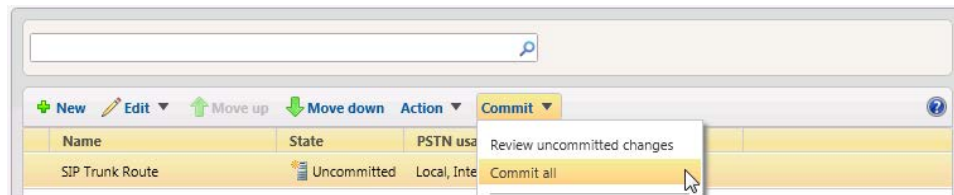
12. Click **OK** (located under the New Voice Route section); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



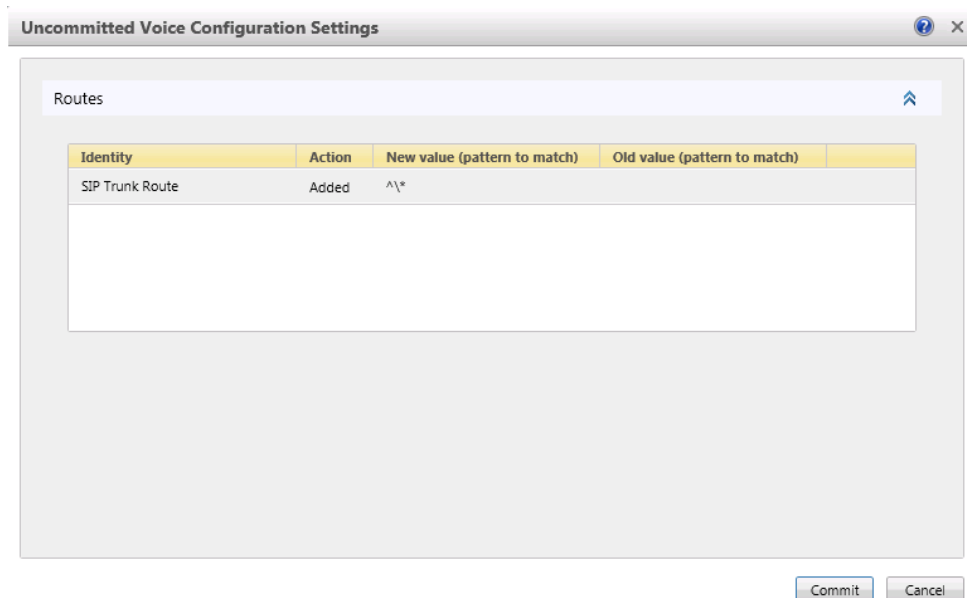
13. From the **Commit** drop-down list, choose **Commit all**:

Figure 3-25: Committing Voice Routes



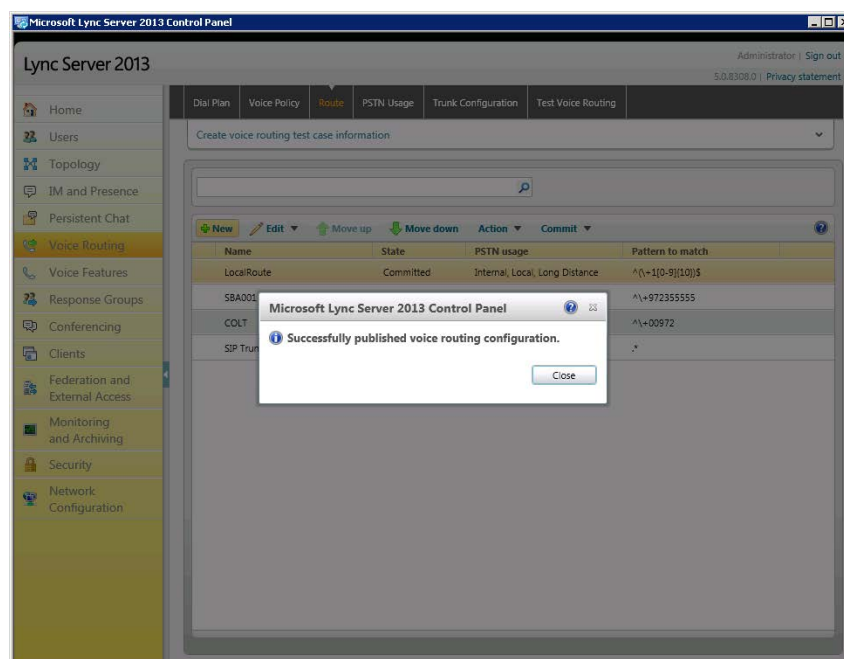
The Uncommitted Voice Configuration Settings dialog opens:

Figure 3-26: Uncommitted Voice Configuration Settings



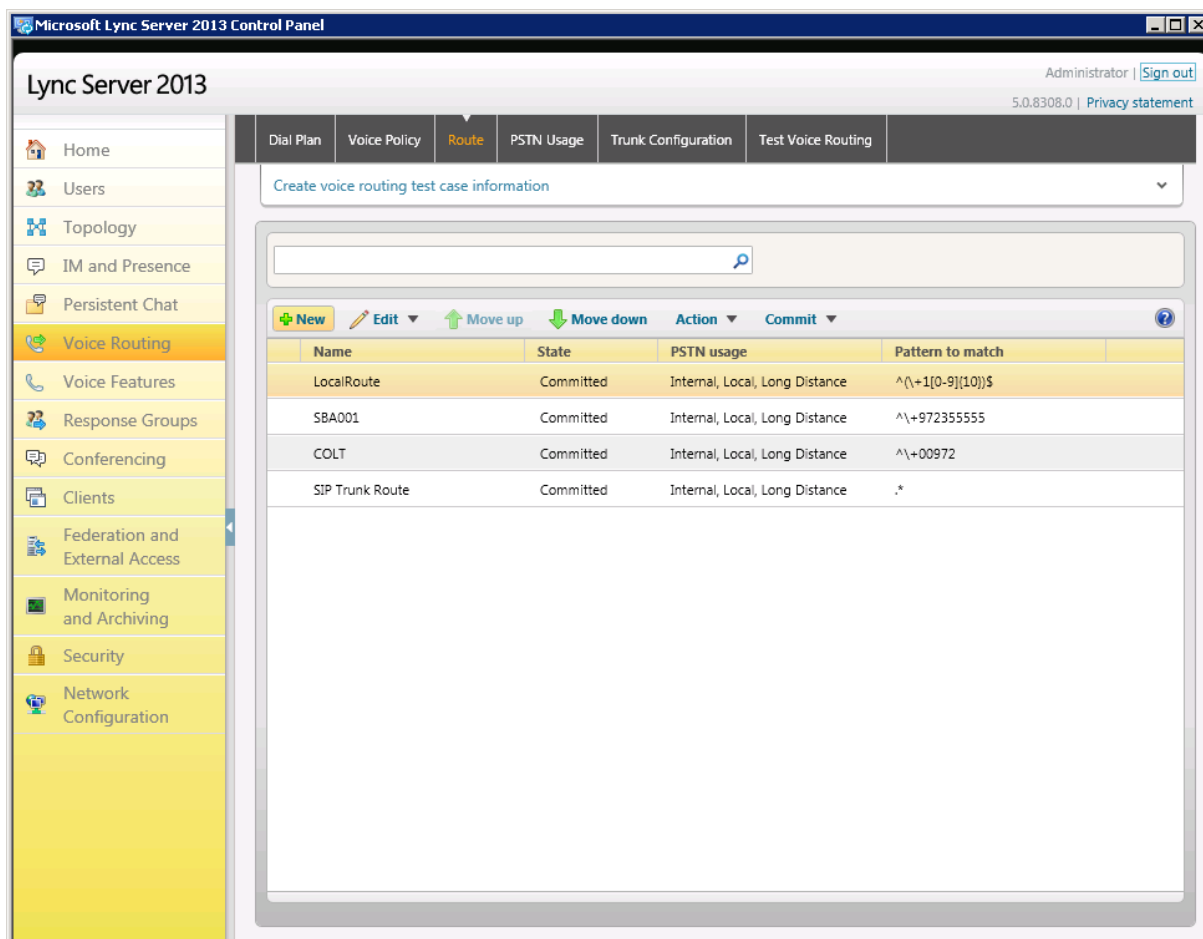
14. Click **Commit**; a message is displayed confirming a successful voice routing configuration:

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



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

Figure 3-28: Voice Routing Screen Displaying Committed Routes



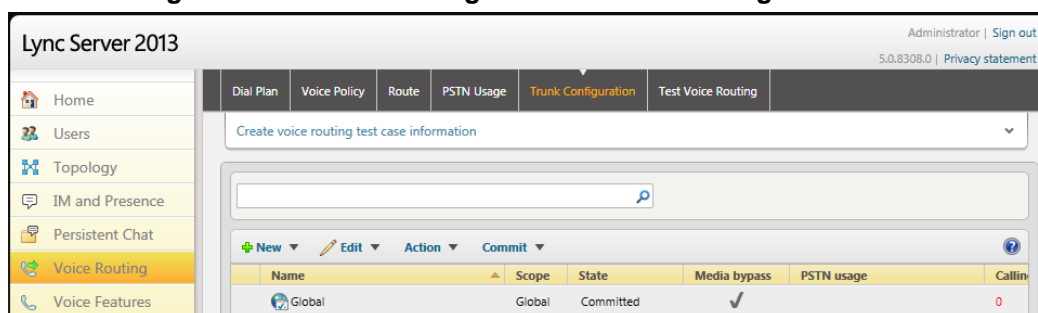
16. For ITSPs that implement a call identifier, continue with the following steps:



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 ITSP SIP Trunk in the P-Asserted-Identity header. Using a Message Manipulation rule (see Section 4.12 on page 74), 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:

Figure 3-30: Edit Trunk Configuration - Global

- c. Select the **Enable media bypass** option.
- d. Select one of the following options from the the 'Encryption Support Level' dropdown:
- ◆ Required - SRTP encryption will be used to help protect traffic between the Mediation Server and the gateway or private branch exchange (PBX).
 - ◆ Optional - SRTP encryption will be used if the service provider or equipment manufacturer supports it.
 - ◆ Not Supported - SRTP encryption is not supported by the service provider or equipment manufacturer and will therefore not be used.

The option selected depends on customer configuration / requirements.

- ◆ If you set 'Encryption Support Level' to **Optional**, make sure the encryption is enabled in PowerShell (<https://support.microsoft.com/en-us/kb/2761579>):

```
Get-CsMediaConfiguration | Set-CsMediaConfiguration -EncryptionLevel
SupportEncryption
Identity                : Global
EnableQoS                : False
EncryptionLevel       : SupportEncryption
EnableSiren              : False
MaxVideoRateAllowed     : VGA600K
```

- e. Select the **Enable forward call history** check box, and then click **OK**.
- f. Repeat Steps 13 through 15 to commit your settings.

This page is intentionally left blank.

4 Configuring AudioCodes SBC

The procedure below describes how to configure AudioCodes' SBC for interworking between Microsoft Lync Server 2013 and an ITSP's SIP Trunk:

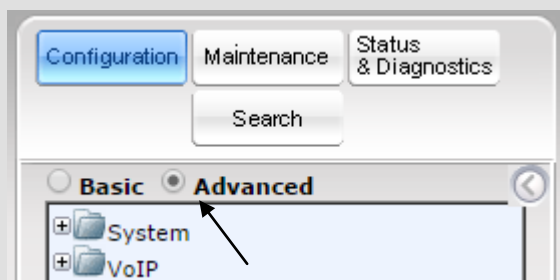
- SBC WAN interface: SIP Trunking environment
- SBC LAN interface: Lync Server 2013 environment

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

Notes:

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

For more information about the Key, contact your AudioCodes representative.
- The scope of this document does *not* cover security aspects of connecting a SIP Trunk to the Microsoft Lync environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, see the *Recommended Security Guidelines Technical Note*.
- The SBC must be installed with SIP firmware version 6.8 or later.
- Before beginning to configure the SBC, select the **Advanced** option in the Web interface to display the full Navigation tree:



When the SBC is reset, the Web interface reverts to **Basic** display.

- This document applies to Microsoft Lync 2013 *and* to Microsoft Lync 2010.

4.1 Step 1: Configuring the SBC's Network Interfaces

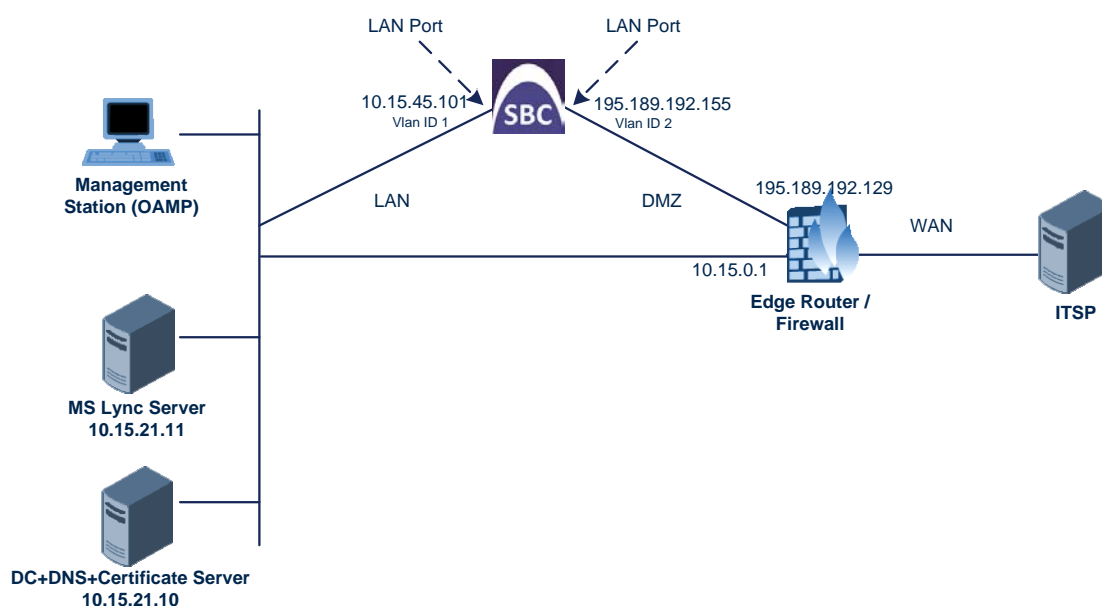
The procedure below describes how to configure the SBC's network interfaces. Several methods can be used. The scenario exemplified in this document uses this method:

- The SBC interfaces are between the Lync servers located on the LAN and the SIP Trunk located on the WAN.
- The SBC connects to the WAN through a DMZ network.

The type of physical LAN connection depends on the method used to connect to the enterprise's network. In this example, the SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and network cables).

In addition, the SBC uses two logical network interfaces; one to the LAN (VLAN ID 1) and one to the WAN (VLAN ID 2).

Figure 4-1: Network Interfaces



4.1.1 Step 1a: Create Ethernet Port Groups for Port Redundancy

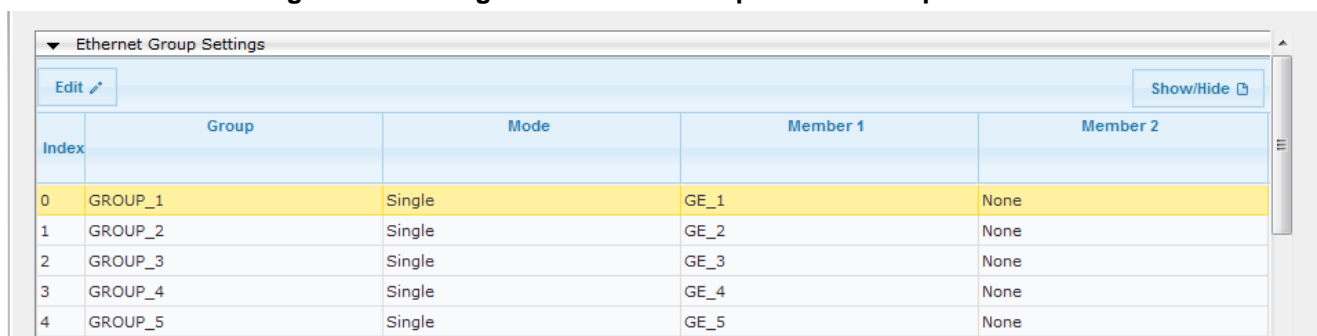
The procedure below describes how to create Ethernet Groups for port redundancy. In our example, two Ethernet Groups need to be configured as follows:

- GROUP_1 with ports 1 (GE_1) and 2 (GE_2)
- GROUP_2 with ports 3 (GE_3) and 4 (GE_4)

➤ To create Ethernet Groups for port redundancy:

1. Open the Ethernet Group Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Groups Table**).

Figure 4-2: Configured Ethernet Groups Table Example



Index	Group	Mode	Member 1	Member 2
0	GROUP_1	Single	GE_1	None
1	GROUP_2	Single	GE_2	None
2	GROUP_3	Single	GE_3	None
3	GROUP_4	Single	GE_4	None
4	GROUP_5	Single	GE_5	None

2. For GROUP_1 do the following:
 - a. Select the index row of GROUP_2 and then click **Edit**.
 - b. Remove port GE_2 from this group by setting the 'Member 1' field to **None**.
 - c. Select the index row of GROUP_1 and then click **Edit**.
 - d. Add port GE_2 to this group by setting the 'Member 2' field to **GE_2**.
3. For GROUP_2 do the following:
 - a. Remove ports GE_3 and GE_4 from GROUP_3 and GROUP_4 respectively.
 - b. Assign these ports to GROUP_2.

4.1.2 Step 1b: Configure the Native VLAN ID



The procedure below describes how to configure the Native VLAN ID for the two network interfaces (LAN and WAN). In the example, the following Native VLAN IDs are used:

- LAN (GROUP_1 ports): Native VLAN ID 1
- WAN (GROUP_2 ports): Native VLAN ID 2

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

1. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Table**).
2. For each of the ports belonging to GROUP_1, do the following:
 - a. Select the port and then click **Edit**.
 - b. Set the native VLAN field to **1**.
3. For each of the ports belonging to GROUP_2, do the following:
 - a. Select the port and then click **Edit**.
 - b. Set the native VLAN field to **2**.

Figure 4-3: Configured Port Native VLAN

▼ Physical Ports Settings							
Edit 						Show/Hide 	
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Active
2	GE_3	Enable	1	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4	Enable	1	Auto Negotiation	User Port #3	GROUP_2	Active

4.1.3 Step 1c: Configure VLANs

The procedure below describes how to define VLANs for the two network interfaces (LAN and WAN). In the example, the following VLAN IDs are used:

- LAN (GROUP_1 ports): VLAN ID 1
- WAN (GROUP_2 ports): VLAN ID 2

➤ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).

2. Configure the VLAN for GROUP_1:

- a. Click **Add**.
- b. Configure the Ethernet Device as shown below:

Parameter	Value
VLAN ID	1
Underlying Interface	GROUP_1 (Ethernet Group)
Name	vlan 1

3. Configure the VLAN for GROUP_2:

- a. Click **Add**.
- b. Configure the Ethernet Device as shown below:

Parameter	Value
VLAN ID	2
Underlying Interface	GROUP_2 (Ethernet Group)
Name	vlan 2

Figure 4-4: 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
<div> ⏪ ⏩ Page 1 of 1 ⏪ ⏩ Show 10 records per page View 1 - 2 of 2 </div>			

4.1.4 Step 1d: Configure IP Network Interfaces for LAN and WAN

The procedure below describes how to configure the IP network interfaces. In the example, the following IP network interfaces are required:

- LAN VoIP (assigned the identification string "Voice"). This interface is assigned to the Ethernet Device that is configured with Ethernet Group 1 and VLAN 1.
- WAN VoIP (assigned the identification string "WANSP"). This interface is assigned to the Ethernet Device that is configured with Ethernet Group 2 and VLAN 2.

➤ To configure the interfaces:

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

Figure 4-5: Interface Table



Index #	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media + C	IPv4 Manual	10.15.7.95	16	10.15.0.1	Voice	0.0.0.0	0.0.0.0	vlan 1

2. Modify the existing LAN network interface:
 - a. Select the row index of the **OAMP + Media + Control** Application Type, and then click **Edit**.
 - b. Configure the interface as shown below:

Parameter	Example Setting for IPv4	Example Setting for IPv6
Application Type	OAMP + Media + Control	Media + Control (Note: The OAMP application can be configured only with IPv4.)
Interface Mode	See IPv4 in the SBC documentation.	See IPv6 in the SBC documentation.
IP Address	10.15.7.95	2001::101 (only a global address can be entered)
Prefix Length	16 for 255.255.0.0 (subnet mask, in bits)	64 (only 64 is supported)
Default Gateway	10.15.0.1	2001::1
Interface Name	Voice (arbitrary descriptive name)	IP6Voice
Primary DNS Server IP Address	0.0.0.0	2001::10
Secondary DNS Server IP Address	0.0.0.0	2001::10
Underlying Device	vlan 1	vlan 1

3. Add a network interface for the WAN:
 - a. Click **Add**.
 - b. Configure the interface as shown below:

Parameter	Example Setting for IPv4	Example Setting for IPv6
Application Type	Media + Control	Media + Control
Interface Mode	See IPv4 in the SBC documentation.	See IPv6 in the SBC documentation.
IP Address	195.189.192.155	2002::155
Prefix Length	16	64
Default Gateway	195.189.192.129	2002::129
Interface Name	WANSP	IP6WANSP
Primary DNS Server IP Address	80.179.52.100	2001:4860:4860::8888
Secondary DNS Server IP Address	80.179.55.100	2001:4860:4860::8844
Underlying Device	vlan 2	vlan 2

4. Click **Submit**.
The configured IP network interfaces are shown below:

Figure 4-6: Configured Network Interface in IP Interfaces Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media + IPv4 Manual		10.15.7.95	16	10.15.0.1	Voice	0.0.0.0	0.0.0.0	vlan 1
1	Media + Control IPv4 Manual		195.189.192.155	25	195.189.192.129	WANSP	80.179.52.100	80.179.55.100	vlan 2

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

4.2 Step 2: Enable the SBC Application

The procedure below 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 4-7: Applications Enabling

⚡ SAS Application	Disable
⚡ SBC Application	Enable
⚡ IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Reset the SBC with a **burn to flash** for this setting to take effect (see Section 4.16 on page 81).

4.3 Step 3: Configuring SRDs

The procedure below describes how to configure Signaling Routing Domains (SRDs). An SRD is a set of definitions comprising IP interfaces, SBC resources, SIP behaviors, and Media Realms.

4.3.1 Step 3a: Configure Media Realms

The procedure below describes how to configure Media Realms. A Media Realm represents a set of ports, associated with an IP interface, used by the SBC to transmit or receive media (RTP or SRTP). Media Realms are associated with SRDs or IP Groups.

Configure one Media Realm for internal (LAN) traffic and another for external (WAN) traffic as shown below.

➤ **To configure Media Realms:**

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

Parameter	Example Setting
Index	1
Media Realm Name	MRLan (an arbitrary name)
IPv4 Interface Name	Voice
IPv6 Interface Name	None Note: Only applicable if using IPv6.
Port Range Start	6000 (represents the lowest UDP port number to be used for media on the LAN)
Number of Media Session Legs	10 (media sessions assigned with the port range)

Figure 4-8: Configuring a LAN Media Realm

The screenshot shows a web form titled "Edit Record #1" with a close button (X). The form contains the following fields and values:

- Index: 1
- Media Realm Name: MRLan
- IPv4 Interface Name: Voice
- IPv6 Interface Name: None
- Port Range Start: 6000
- Number Of Media Session Legs: 10
- Port Range End: 6090
- Default Media Realm: Yes
- QoE Profile: None
- BW Profile: None

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

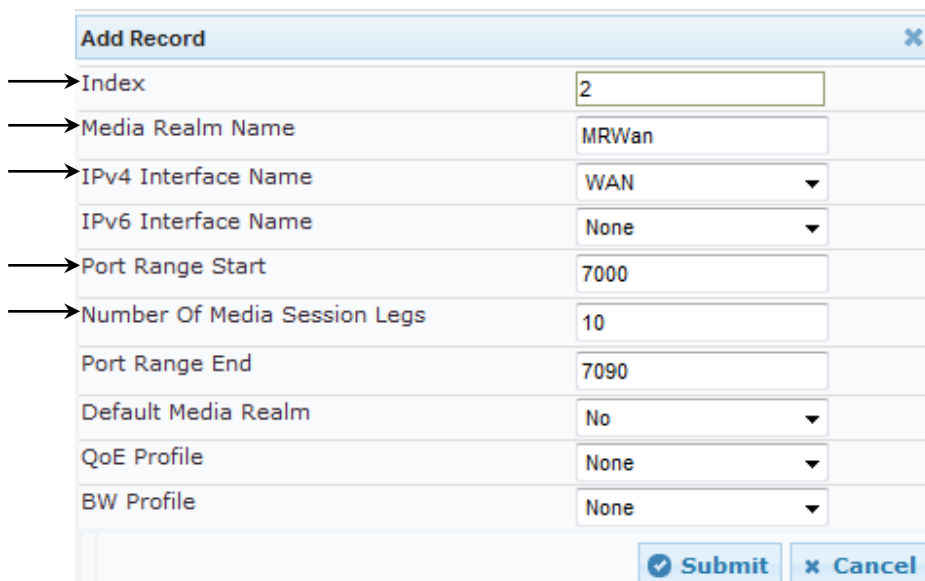
- c. Click **Submit**.

3. Add a Media Realm for the external traffic (WAN):

- a. Click **Add**.
- b. Configure like this:

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

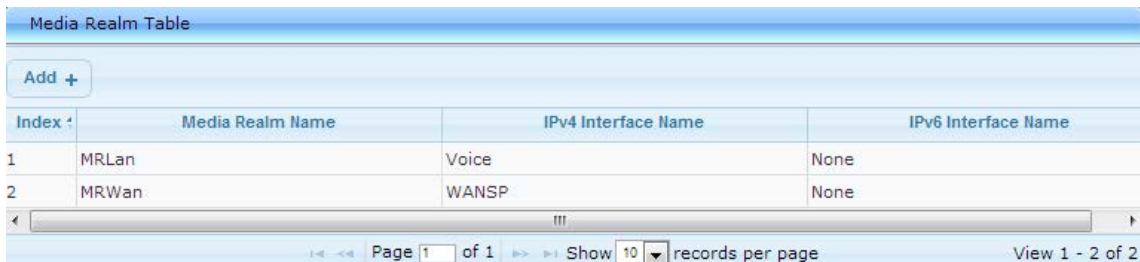
Figure 4-9: Configuring a WAN Media Realm



- c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-10: Required Media Realm Table



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

4.3.2 Step 3b: Configure SRDs

The procedure below describes how to configure SRDs.

➤ **To configure SRDs:**

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

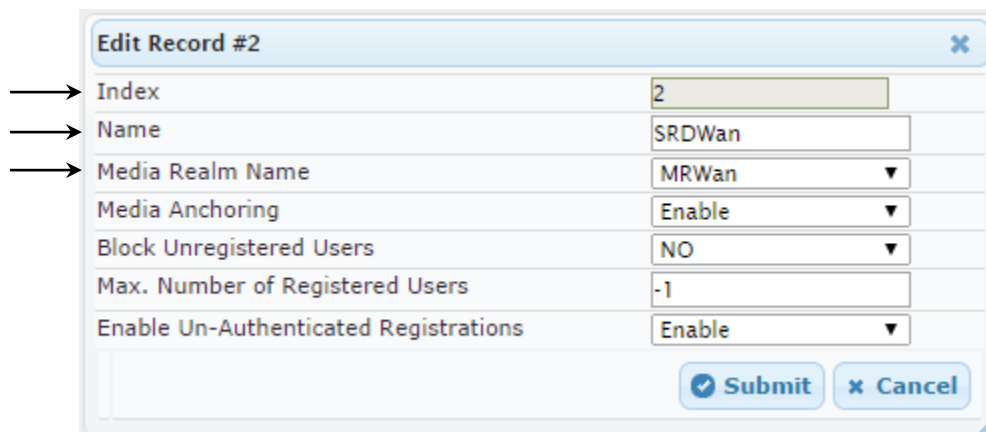
Parameter	Example Setting
Index	1
Name	SRDLan (descriptive name for the SRD)
Media Realm Name	MRLan (associates the SRD with a Media Realm)

Figure 4-11: Configuring the LAN SRD Example

The screenshot shows a web-based configuration interface for editing an SRD record. The dialog box is titled 'Edit Record #1'. It contains several input fields and dropdown menus. Three arrows on the left point to the 'Index', 'Name', and 'Media Realm Name' fields, which correspond to the example settings in the table above. The 'Index' field contains the value '1'. The 'Name' field contains 'SRDLan'. The 'Media Realm Name' field contains 'MRLan'. Other fields include 'Media Anchoring' (set to 'Enable'), 'Block Unregistered Users' (set to 'NO'), 'Max. Number of Registered Users' (set to '-1'), and 'Enable Un-Authenticated Registrations' (set to 'Enable'). At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

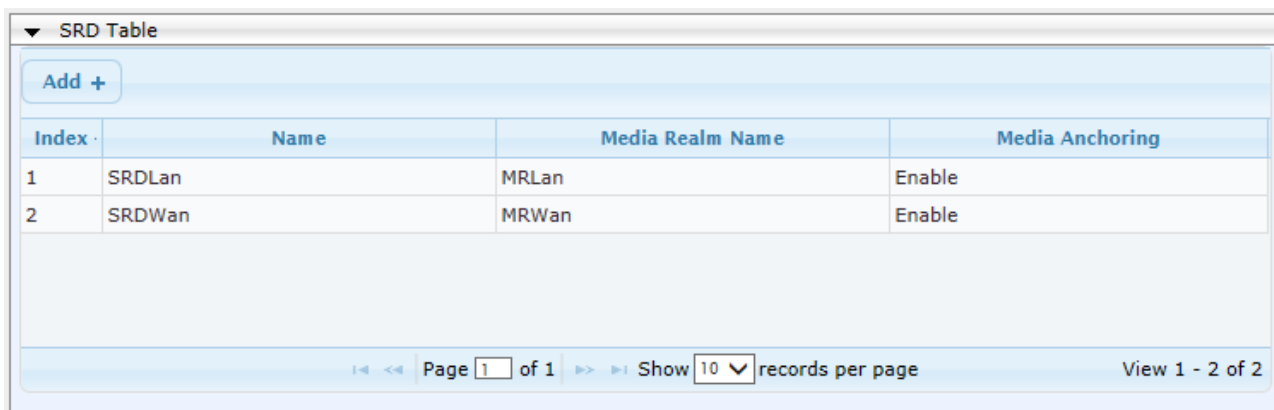
Parameter	Example Setting
SRD Index	2
SRD Name	SRDWan
Media Realm Name	MRWan

Figure 4-12: Configuring the WAN SRD


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

b. Click **Submit**.

The configured SRDs are shown in the figure below:

Figure 4-13: Configured SRDs in SRD Table


Index	Name	Media Realm Name	Media Anchoring
1	SRDLan	MRLan	Enable
2	SRDWan	MRWan	Enable

4.3.3 Step 3c: Configure SIP Signaling Interfaces

The procedure below describes how to add SIP interfaces. In the example scenario, an internal and external SIP interface must be added for the SBC.

A SIP Interface consists of a combination of ports (UDP, TCP, and TLS) associated with a specific IP network interface. The SIP Interface is associated with an SRD.

➤ **To add SIP interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).

2. Add a SIP interface for the LAN:

- a. Click **Add**.
- b. Configure these parameters:

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

- c. Click **Submit**.

3. Add a SIP interface for the WAN:

- a. Click **Add**.
- b. Configure these parameters:

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

- c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-14: Required SIP Interface Table

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

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

4.4 Step 4: Configure Proxy Sets

The procedure below describes how to configure the Proxy Sets. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). In the example scenario, two Proxy Sets must be configured for:

- Microsoft Lync Server 2013
- SIP Trunk

These Proxy Sets will later be associated with IP Groups.

➤ To add Proxy Sets:

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

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

Figure 4-15: 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	1
Classification Input	IP only
TLS Context Index	-1

b. Click **Submit**.

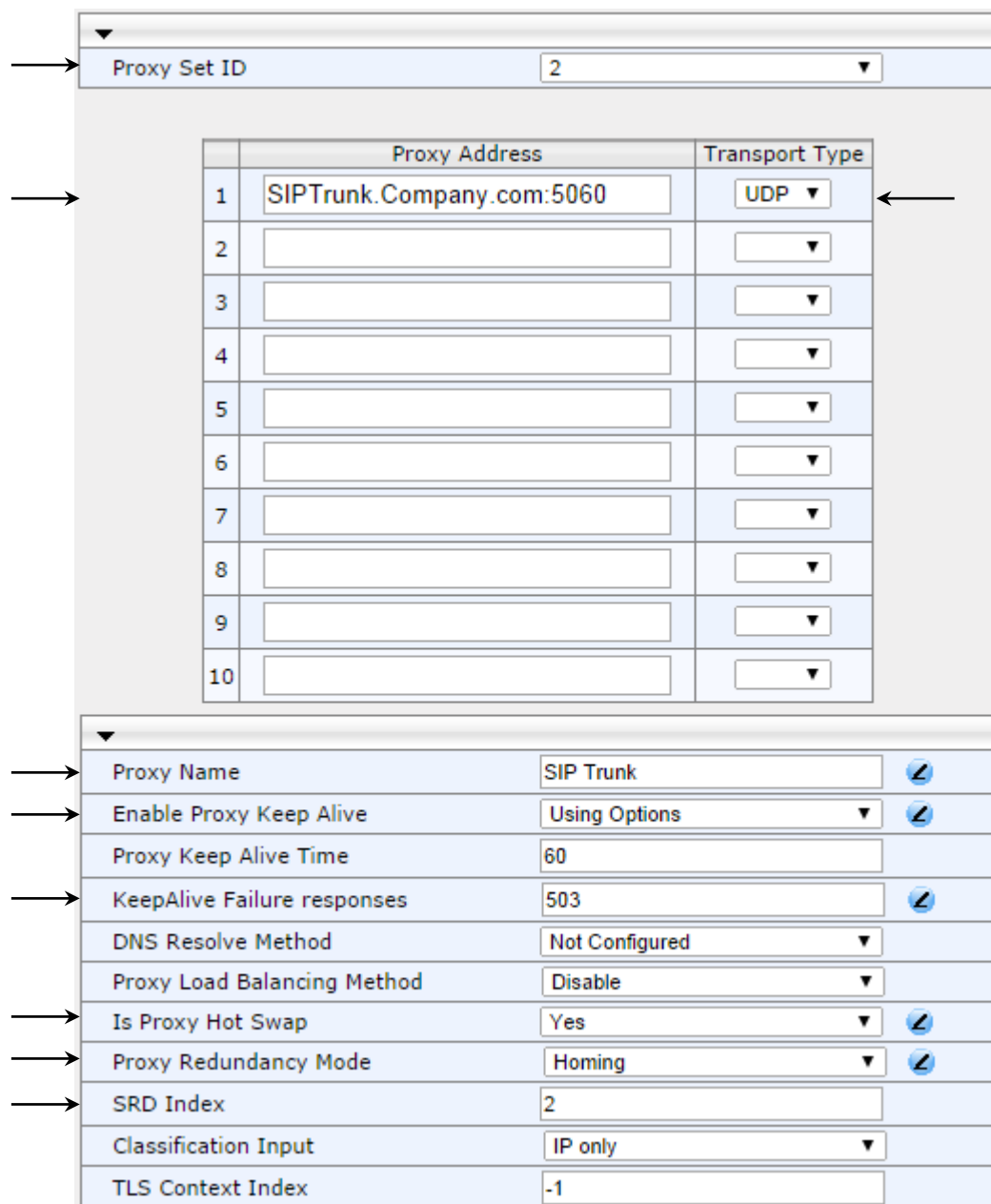
3. Add a Proxy Set for the SIP Trunk:

a. Configure these parameters:

Parameter	Example Setting
Proxy Set ID	2
Proxy Address	SIPTrunk.Company.com:5060 (SIP Trunk IP address or FQDN and destination port)
Transport Type	UDP
Proxy Name	SIP Trunk
Enable Proxy Keep Alive	Using Options
KeepAlive Failure responses	503 (If this is received in response to a keep-alive message using SIP OPTIONS, the SBC considers the proxy as down and tries the next proxy.)
Is Proxy Hot Swap	Yes

Proxy Redundancy Mode	Homing
SRD Index	2 (enables classification by Proxy Set for this SRD in the IP Group belonging to the SIP Trunk)

Figure 4-16: Configuring a Proxy Set for the ITSP SIP Trunk



Proxy Set ID: 2

	Proxy Address	Transport Type
1	SIPTrunk.Company.com:5060	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: SIP Trunk

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: Yes

Proxy Redundancy Mode: Homing

SRD Index: 2

Classification Input: IP only

TLS Context Index: -1

b. Click **Submit**.

4.5 Step 5: Configure IP Groups

The procedure below describes how to create IP Groups. An IP Group represents a SIP entity behavior in the SBC's network. In the example scenario, IP Groups are created for:

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

These IP Groups are later used by the SBC application for routing calls.

➤ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the Lync Server 2013 Mediation Server:
 - a. Click **Add**.
 - b. Configure the parameters like this:

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

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

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

- c. Click **Submit**.

The figure below shows the configured IP Group table:

Figure 4-17: Configured 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				No	1
2	Server	SIP Trunk	2				No	2
<div> Page 1 of 1 Show 10 records per page View 1 - 2 of 2 </div>								

4.6 Step 6: Configure IP Profiles

The procedure below describes how to configure IP Profiles. In the example scenario, the IP Profiles are used to configure the SRTP / TLS modes and other parameters that differ between the two entities - Lync Server 2013 and SIP Trunk.

Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 51).

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

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

➤ To add IP Profiles:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **IP Profile Settings**).
2. Add an IP Profile for Lync Server 2013:
 - a. Configure the parameters like this:

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

Figure 4-18: Configured IP Profile for Lync Server 2013 – Common

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

Figure 4-19: Configured IP Profile for Lync Server 2013 – SBC

Common GW SBC	
Index	1
Extension Coders Group ID	Coders Group 1
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	Extend
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	Transparent
Session Expires Mode	Transparent
→ Remote Update Support	Supported Only After i
→ Remote re-INVITE	Supported only with SI
→ Remote Delayed Offer Support	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	Don't 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	Inactive
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care

Submit Cancel

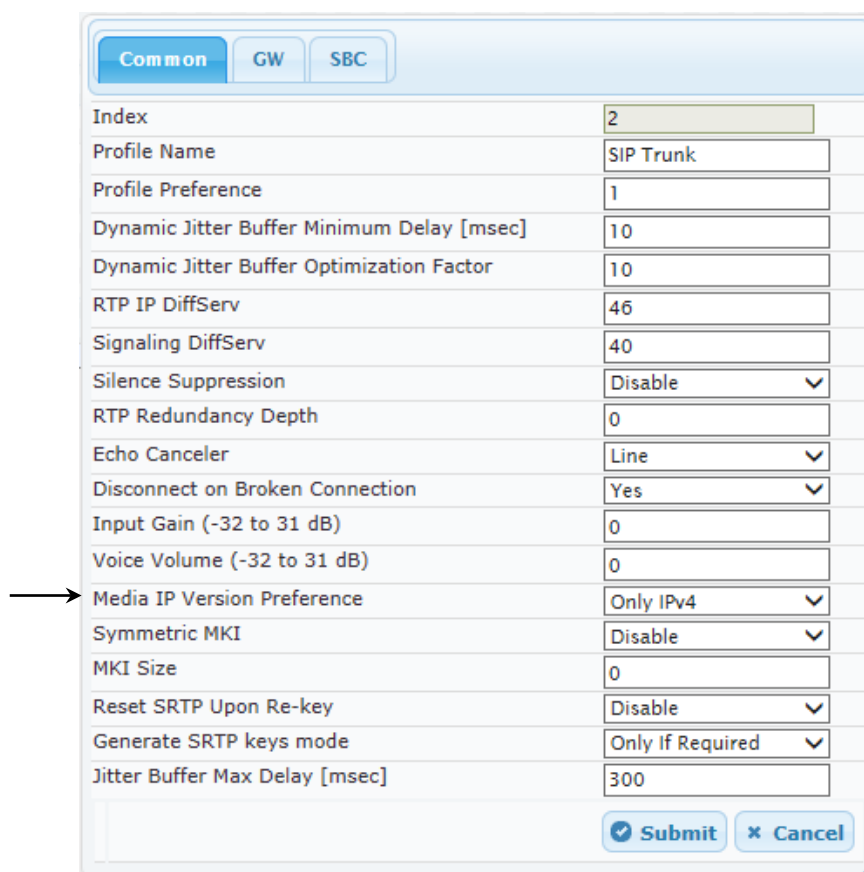
- b. Click **Submit**.
3. Add an IP Profile for the SIP Trunk:
 - a. Configure the parameters like this:

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



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

Figure 4-20: Configured IP Profile for SIP Trunk



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

Submit Cancel

Figure 4-21: Configured IP Profile for SIP – SBC

Common	GW	SBC
Index		2
Extension Coders Group ID		Coders Group 2
Transcoding Mode		Only If Required
Allowed Media Types		
Allowed Coders Group ID		Coders Group 2
Allowed Video Coders Group ID		None
Allowed Coders Mode		Preference
SBC Media Security Behavior		RTP
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		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		Transparent
SDP Ptime Answer		Remote Answer
Preferred PTime		0
Use Silence Suppression		Transparent
RTP Redundancy Behavior		AS IS
Play RBT To Transferee		No
RTCP Mode		Transparent
Jitter Compensation		Disable
Remote Renegotiate on Fax Detection		Don't Care

Submit Cancel

b. Click **Submit**.

4.7 Step 7: Configure Coders

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

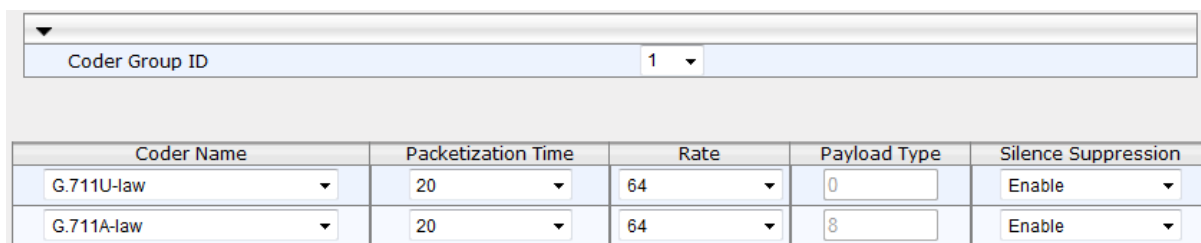
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 53).

➤ **To configure coders:**

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

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

Figure 4-22: Configured Coder Group for Lync Server 2013

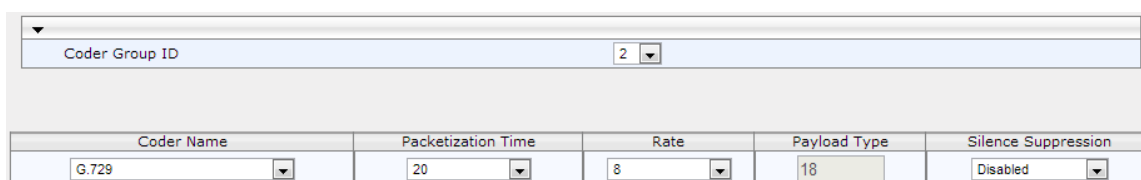


Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-law	20	64	0	Enable
G.711A-law	20	64	8	Enable

- b. Click **Submit**.
3. Add a Coder Group for SIP Trunk:
 - a. Configure the parameters like this:

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

Figure 4-23: Configured Coder Group for the SIP Trunk



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

- b. Click **Submit**.

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



Note: This Allowed Coders Group ID (and its preference) was assigned to the IP Profile belonging to the SIP Trunk in the previous step (see Section 4.6 on page 53).

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

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

Figure 4-24: Allowed Audio Coders Group for SIP Trunk

Allowed Audio Coders Group

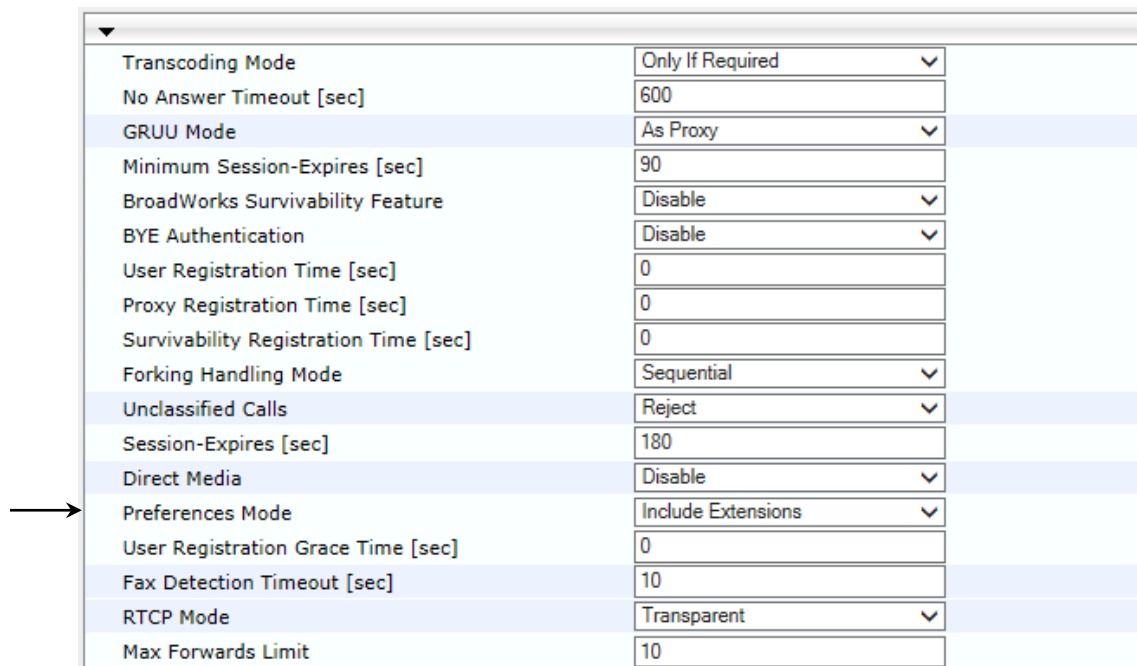
Allowed Audio Coders Group ID: 2

Coder Name: G.729

Submit

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

Figure 4-25: SBC Preferences 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

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

4.8 Step 8: Configure SIP TLS Connection

The procedure below describes how to configure the SBC to use a TLS connection with the Lync Server 2013 Mediation Server. This step is mandatory for a secure SIP TLS connection.

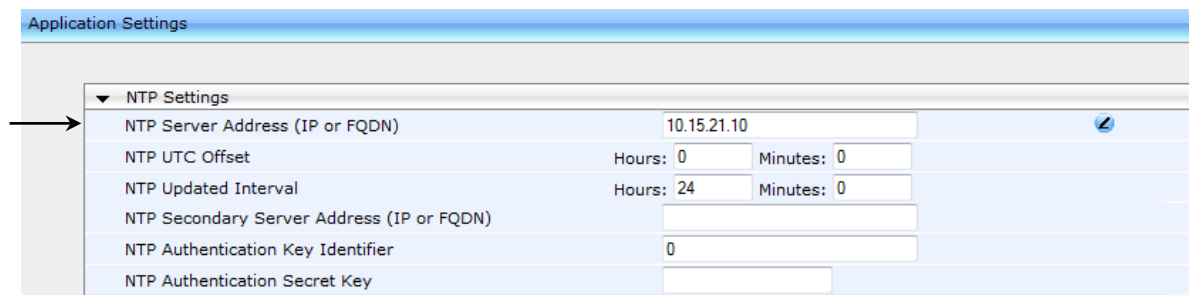
4.8.1 Step 8a: Configure the NTP Server Address

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

➤ **To configure the NTP server address:**

1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).
2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., 10.15.21.10).

Figure 4-26: Configuring the NTP Server IP Address



The screenshot shows the 'Application Settings' window with the 'NTP Settings' section expanded. An arrow points to the 'NTP Server Address (IP or FQDN)' field, which contains the value '10.15.21.10'. Other fields include 'NTP UTC Offset' (Hours: 0, Minutes: 0), 'NTP Updated Interval' (Hours: 24, Minutes: 0), 'NTP Secondary Server Address (IP or FQDN)', 'NTP Authentication Key Identifier' (0), and 'NTP Authentication Secret Key'.

NTP Settings		
NTP Server Address (IP or FQDN)	10.15.21.10	
NTP UTC Offset	Hours: 0	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**.

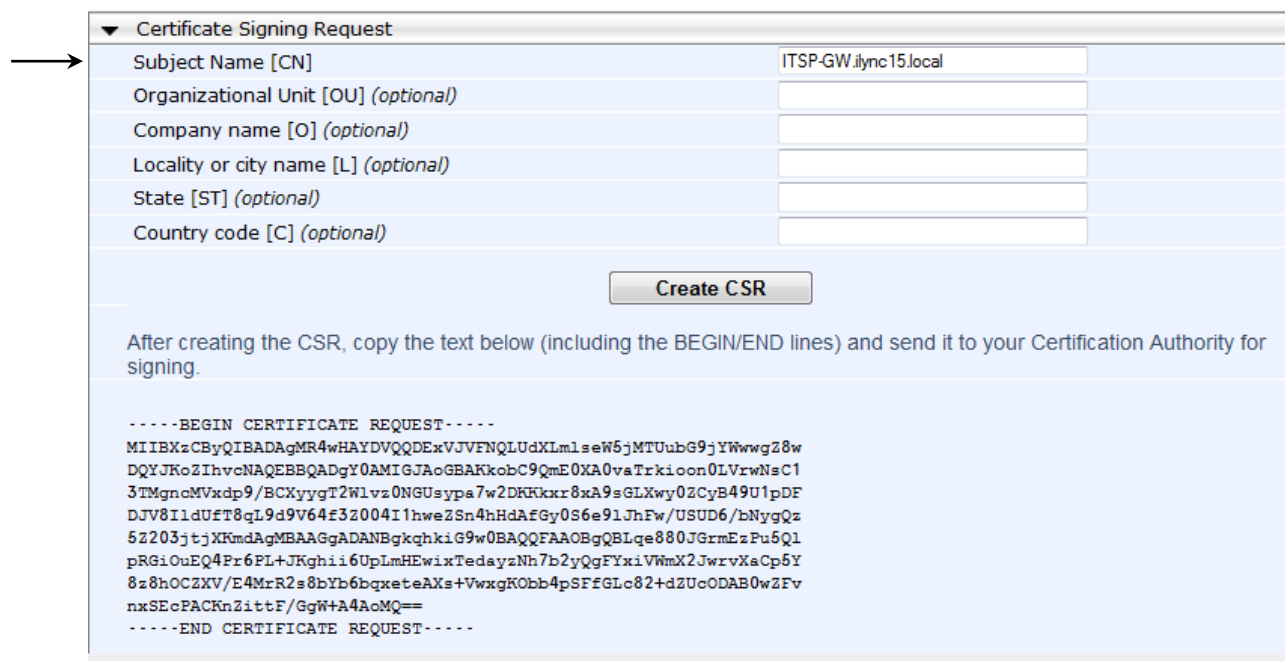
4.8.2 Step 8b: Configure a Certificate

The procedure below describes how to exchange a certificate with the Microsoft Certificate Authority (CA). The certificate is used by the SBC to authenticate the connection with the management station (i.e., the computer used to manage the SBC through its embedded Web server).

➤ **To configure a certificate:**

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

Figure 4-27: Certificates Page - 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)

Create CSR

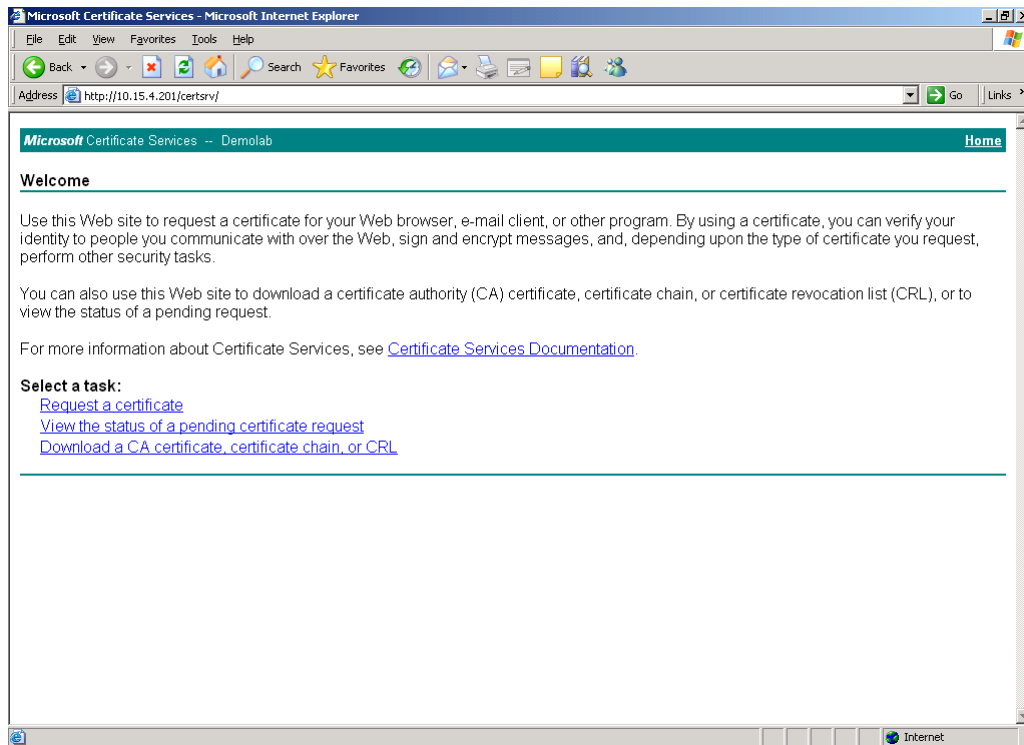
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLMlseW5jMTUubG9jYWwwZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCXyygT2Wlvz0NGUsypa7w2DKKkxr8xA9sGLXwy0ZCyB49U1pDF
DJV8IldUFT8qL9d9V64f3Z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAAgADANBgkqhkiG9w0BAQQFAAQBqBLqe880JGxmEzPu5Q1
pRGiOueQ4Pr6PL+JKghii6UpLmHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y
8z8hOCZXV/E4MrR2s8bYb6bqxeteAXs+VwxgKObb4pSFfGLc82+dZUoODAB0wZFv
nxSEcPACKnZittF/GgW+A4AoMQ==
-----END CERTIFICATE REQUEST-----
```

2. In the 'Subject Name' field, enter the media gateway name (e.g., ITSP-GW.ilync15.local). This name must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 15).
3. Click **Create CSR**; a certificate request is generated.
4. Copy the CSR (from the line ----BEGIN CERTIFICATE to the line END CERTIFICATE REQUEST----) to a text file (such as Notepad) and save it to a folder on your computer with the file name *certreq.txt*.

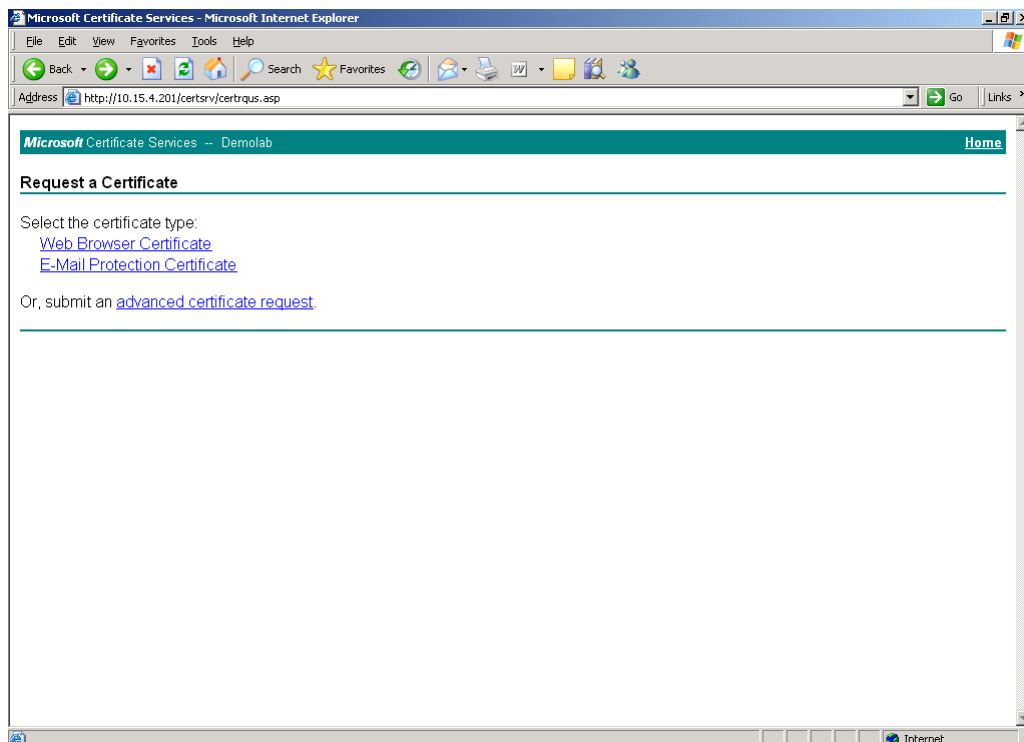
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-28: Microsoft Certificate Services Web Page

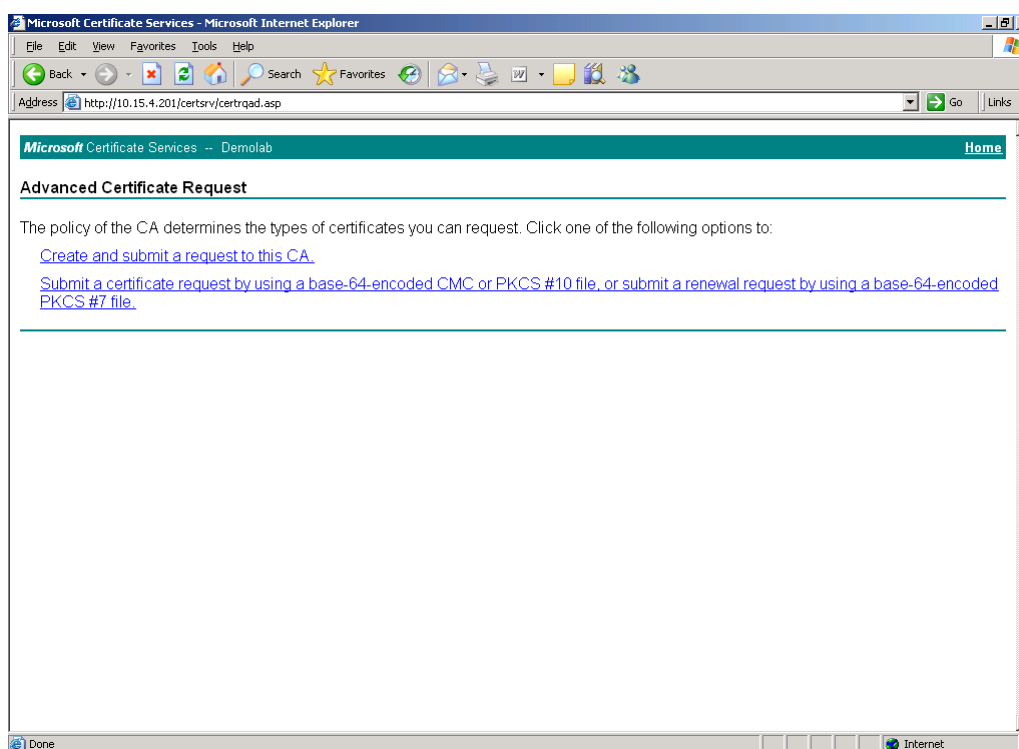


6. Click **Request a certificate**.

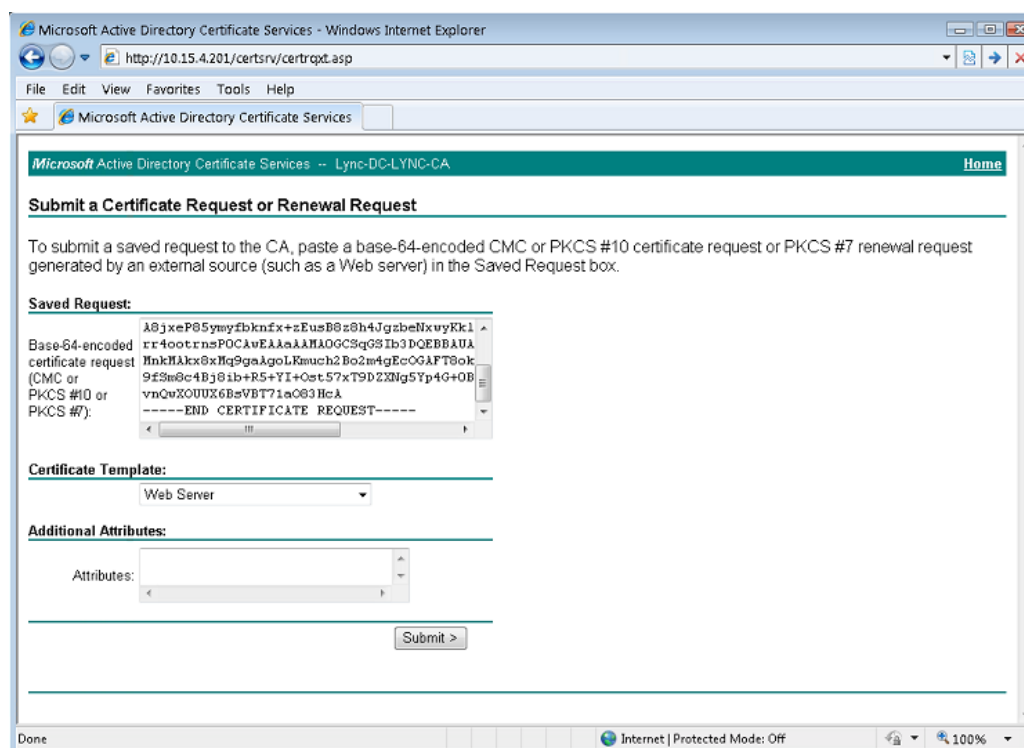
Figure 4-29: Request a Certificate Page



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

Figure 4-30: Advanced Certificate Request Page


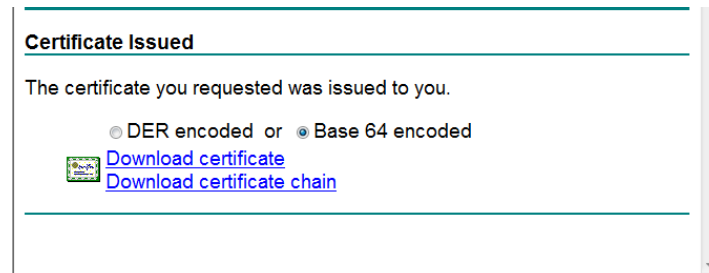
8. Click **Submit a certificate request...** and click **Next**.

Figure 4-31: Submit a Certificate Request or Renewal Request Page


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

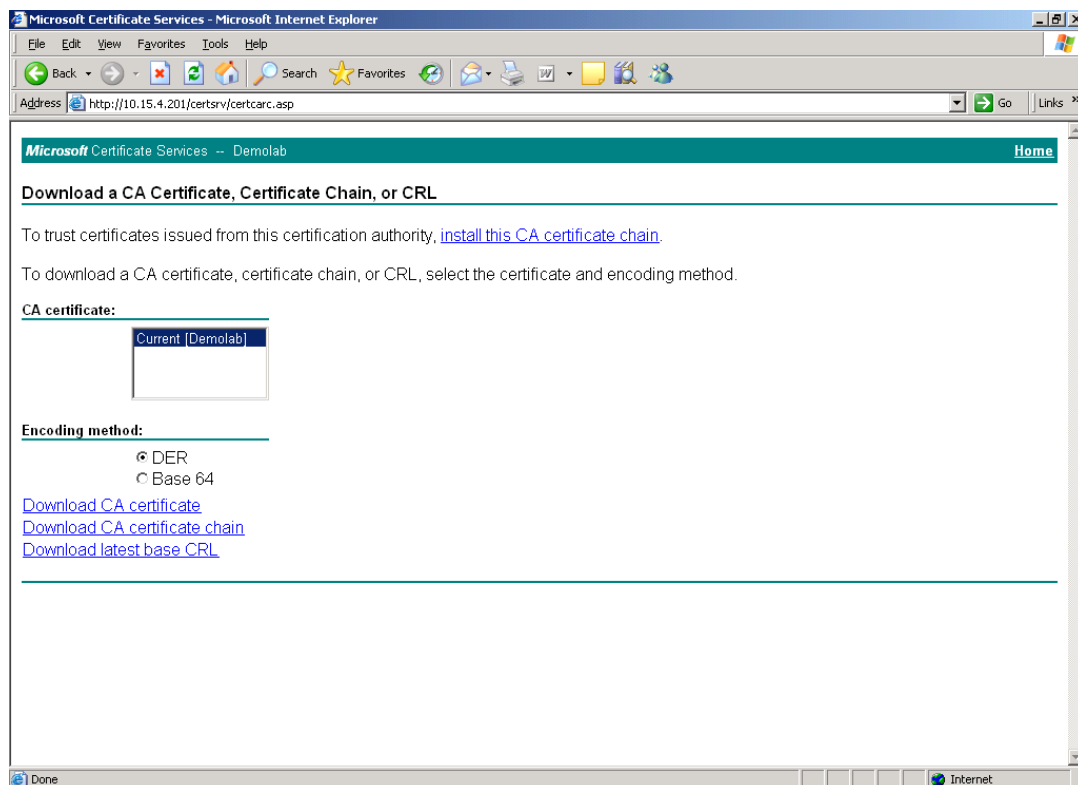
11. Click **Submit**.

Figure 4-32: Certificate Issued Page



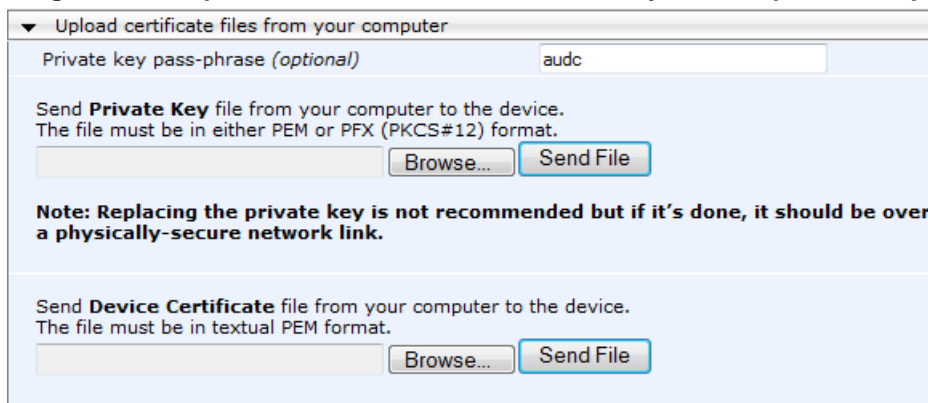
12. Select the **Base 64 encoded** option for encoding and click **Download certificate**.
13. Save the file with the name *gateway.cer* to a folder on your computer.
14. Click the **Home** button (or navigate to the certificate server at <http://<Certificate Server>/CertSrv>).

Figure 4-33: Download a CA Certificate, Certificate Chain, or CRL



15. Under the 'Encoding method' group, select the **Base 64** option for encoding.
16. Click **Download CA certificate**.
17. In the 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 13, and then click **Send File** to upload the certificate to the SBC.

Figure 4-34: 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.


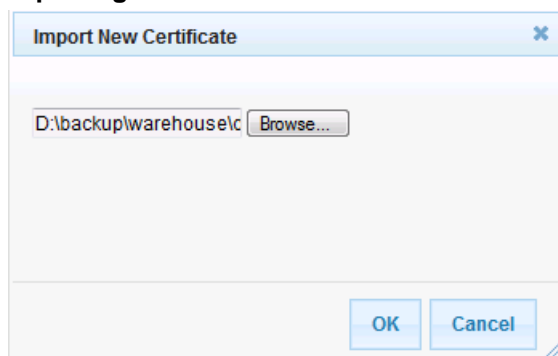
- b. In the SBC's Web interface, return to the **TLS Contexts** page.
- c. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates**  button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.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

Figure 4-35: Importing Root Certificate into Trusted Certificates Store



Import New Certificate

18. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
19. Reset the SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 81).

4.9 Step 9: Configure SRTP

The procedure below describes how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), configure the SBC to do so as well.

Note that SRTP was enabled for Lync Server 2013 when you added an IP Profile for Lync Server 2013 (see Section 4.6 on page 53).

➤ **To configure media security:**

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

Figure 4-36: Media Security Page

General Media Security Settings		
Media Security	Enable	
Media Security Behavior	Preferable	
Authentication On Transmitted RTP Packets	Active	
Encryption On Transmitted RTP Packets	Active	
Encryption On Transmitted RTCP Packets	Active	
SRTP Tunneling Authentication for RTP	Disable	
SRTP Tunneling Authentication for RTCP	Disable	

SRTP Setting		
Master Key Identifier (MKI) Size	1	
Symmetric MKI Negotiation	Enable	

2. Configure the parameters like this:

Parameter	Example Setting
Media Security	Enable
Master Key Identifier (MKI) Size	"1"
Symmetric MKI Negotiation	Enable

3. Click **Submit**.
4. Reset the SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 81).



Note: If you are implementing SRTP, make sure that you also configure the Lync server for SRTP 'Encryption Support Level'. For more information, see [here](#).

4.10 Step 10: Configure IP Media

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

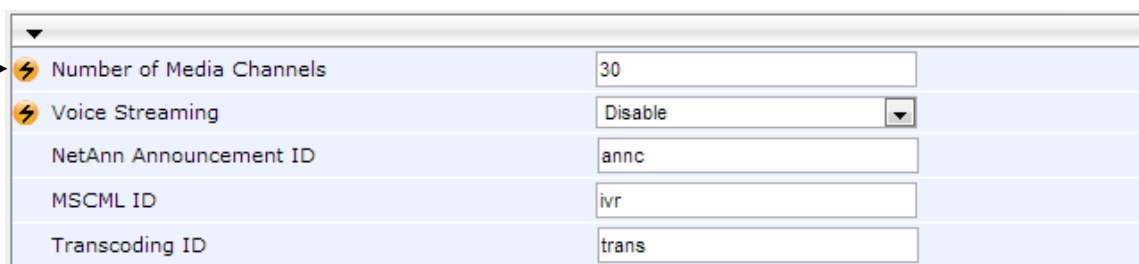


Note: This step is required *only* if transcoding is required.

➤ **To configure IP media:**

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

Figure 4-37: IP Media Settings



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

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

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 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 51, IP Group 1 represents Lync Server 2013, and IP Group 2 represents ITSP 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 ITSP SIP Trunk (WAN):

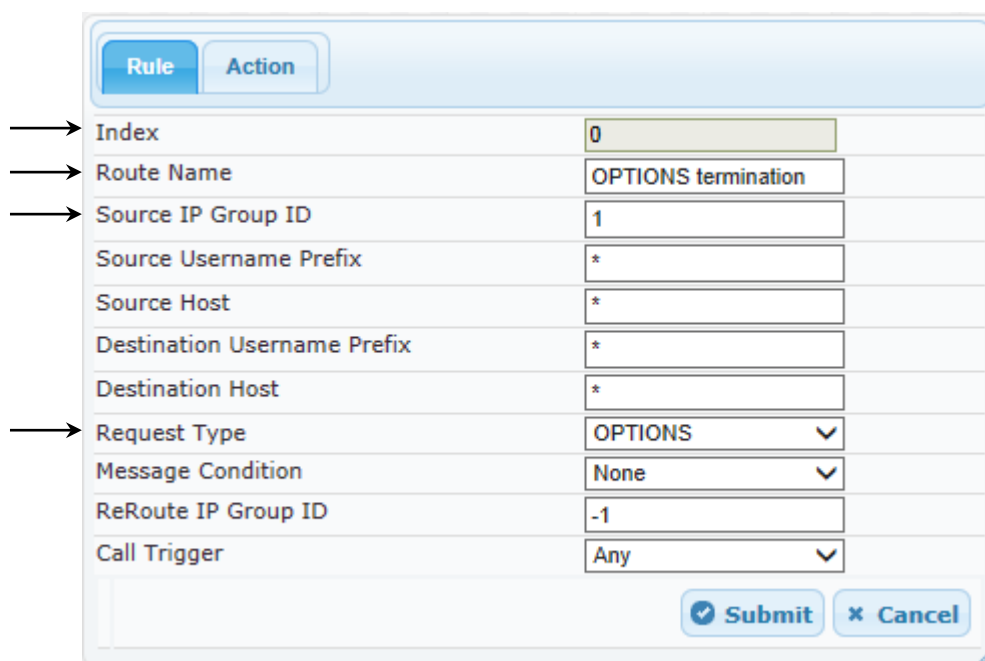
- Terminate SIP OPTIONS messages on the SBC that are received from the LAN
- Calls from Lync Server 2013 to ITSP SIP Trunk
- Calls from ITSP SIP Trunk to Lync Server 2013

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

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
3. Click **Add**.
4. Click the **Rule** tab, and then configure the parameters as follows:

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

Figure 4-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab

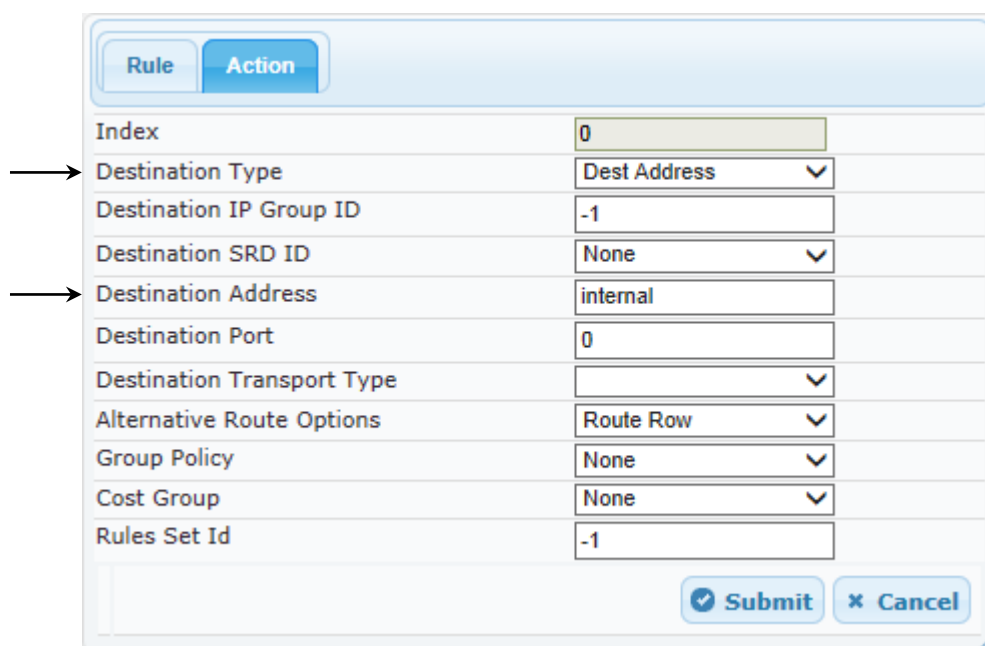


Parameter	Value
Index	0
Route Name	OPTIONS termination
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-39: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



Parameter	Value
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

- Configure a rule to route calls from Lync Server 2013 to ITSP SIP Trunk:
- Click **Add**.

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

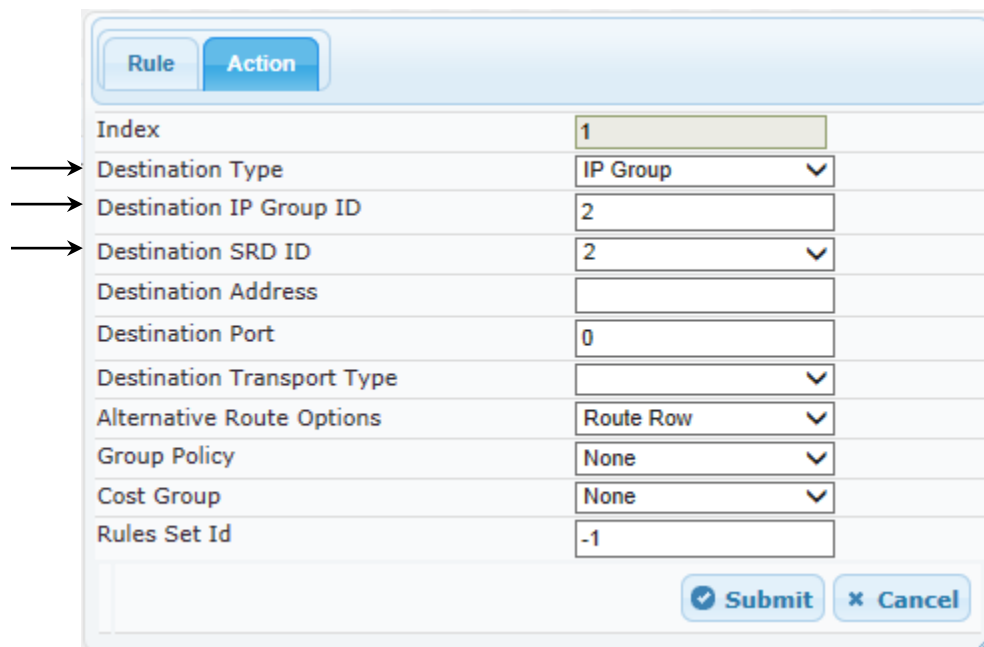
Parameter	Value
Index	1
Route Name	Lync to ITSP (arbitrary descriptive name)
Source IP Group ID	1

Figure 4-40: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab

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

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

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

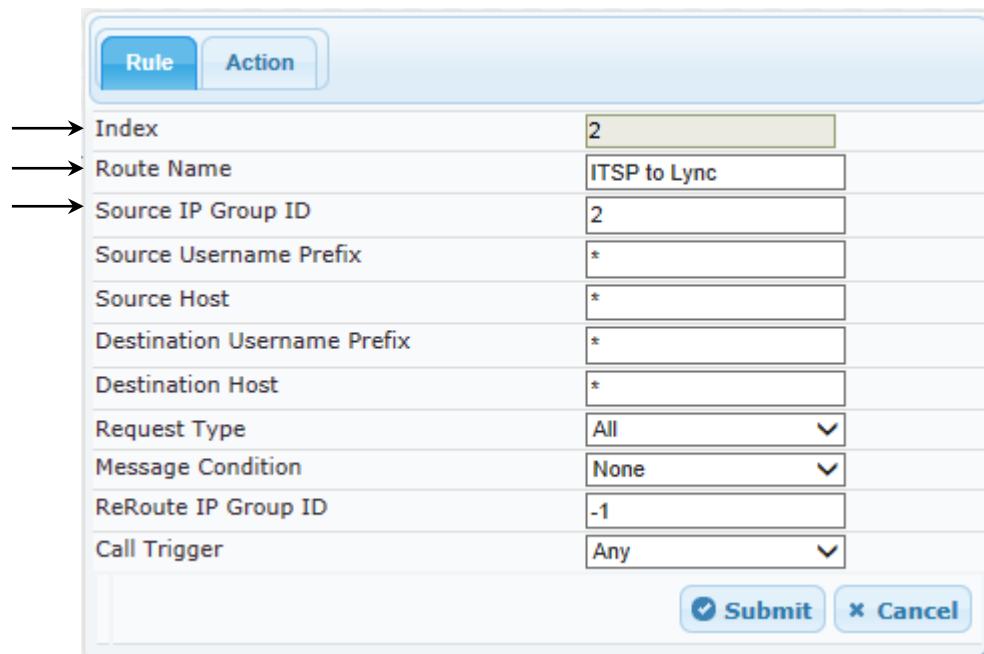
Figure 4-41: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab


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

Submit Cancel

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

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

Figure 4-42: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab


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

Submit Cancel

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

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

Figure 4-43: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab

The screenshot shows the 'Action' tab of the IP-to-IP Routing Rule configuration window. The fields are as follows:

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

Buttons: Submit, Cancel

The configured routing rules are shown in the figure below:

Figure 4-44: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table

Add + Insert +

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

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



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

4.12 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 51, IP Group 1 represents Lync Server 2013, and IP Group 2 represents ITSP SIP Trunk.



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

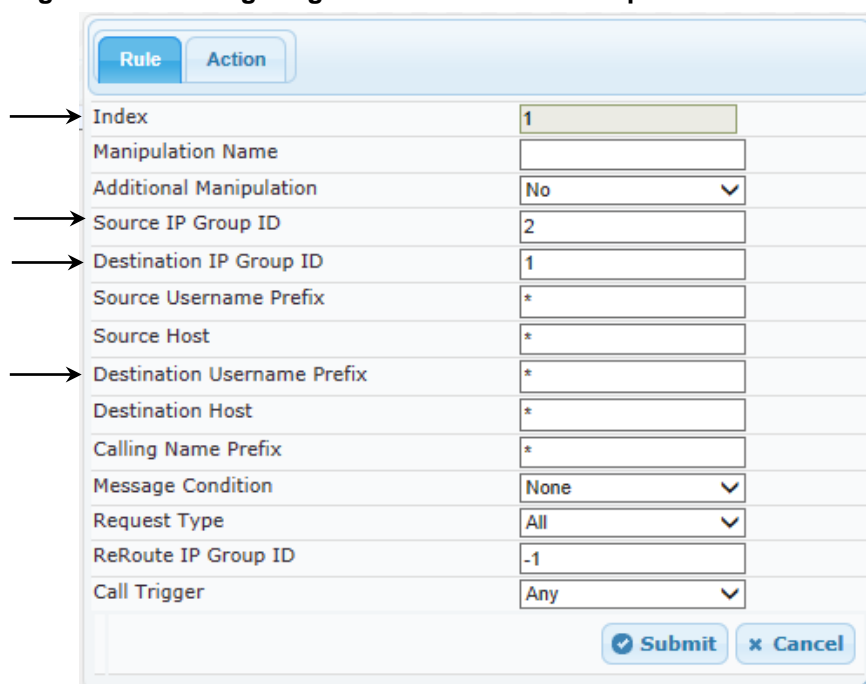
For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (ITSP SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

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

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

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

Figure 4-45: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



Parameter	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 4-46: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

5. Click **Submit**.

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

Figure 4-47: Example of Configured IP-to-IP Outbound Manipulation Rules

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

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

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

4.13 Step 13: Configure SIP Message Manipulation Rules

The procedure below describes how to configure SIP message manipulation rules (configured in the Message Manipulations table).

SIP message manipulation rules can include insertion, removal and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. After configuring the SIP message manipulation rules assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

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

➤ To configure SIP message manipulation rules:

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

Figure 4-48: Message Manipulations Page

Message Manipulations							
Add +		Insert +					
Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	0	any	header.referred-by exists	header.p-asserted-identity	Modify	'<'+header.referred-by.U	Use Current Condition
Page 1 of 1							

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

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

Figure 4-49: Configured SIP Message Manipulation Rule

Add Record	
Index	0
Manipulation Name	
Manipulation Set ID	0
Message Type	any
Condition	header.referred-by exists
Action Subject	header.p-asserted-identity
Action Type	Modify
Action Value	<'+header.referred-by.UR
Row Role	Use Current Condition
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Click **Submit**.
4. Assign the Manipulation Set ID 0 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 click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Outbound Message Manipulation Set' field to "0".

Figure 4-50: Assigning a Manipulation Rule to IP Group 2

Common Gateway SBC	
Index	2
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	0
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
Enable SBC Client Forking	No
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- e. Click **Submit**.

4.14 Step 14: Configure Registration Account

The procedure below describes how to configure SIP registration accounts (in the Account Table page) so that the SBC can register with the SIP Trunk on behalf of Lync Server 2013.



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

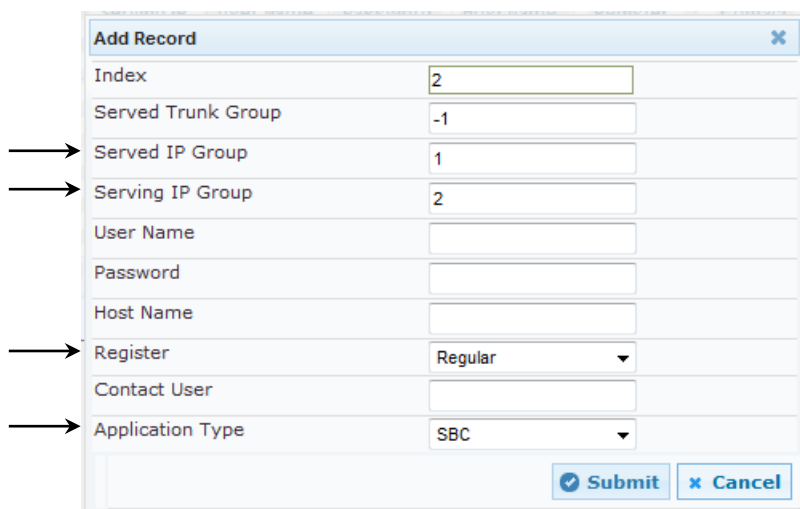
In this example, the Served IP Group is Lync Server 2013 (IP Group 1) and the Serving IP Group is SIP Trunk (IP Group 2).

➤ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Click **Add**.
3. Configure the account according to the information provided by the SIP Trunk provider, for example:

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

Figure 4-51: Configuring a SIP Registration Account



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

- Index: 2
- Served Trunk Group: -1
- Served IP Group: 1 (indicated by an arrow)
- Serving IP Group: 2 (indicated by an arrow)
- User Name: (empty)
- Password: (empty)
- Host Name: (empty)
- Register: Regular (indicated by an arrow)
- Contact User: (empty)
- Application Type: SBC (indicated by an arrow)

Buttons at the bottom: Submit, Cancel.

4. Click **Submit**.

4.15 Step 15: Configure Miscellaneous SBC Functions

The procedures below describe miscellaneous SBC configuration functions.

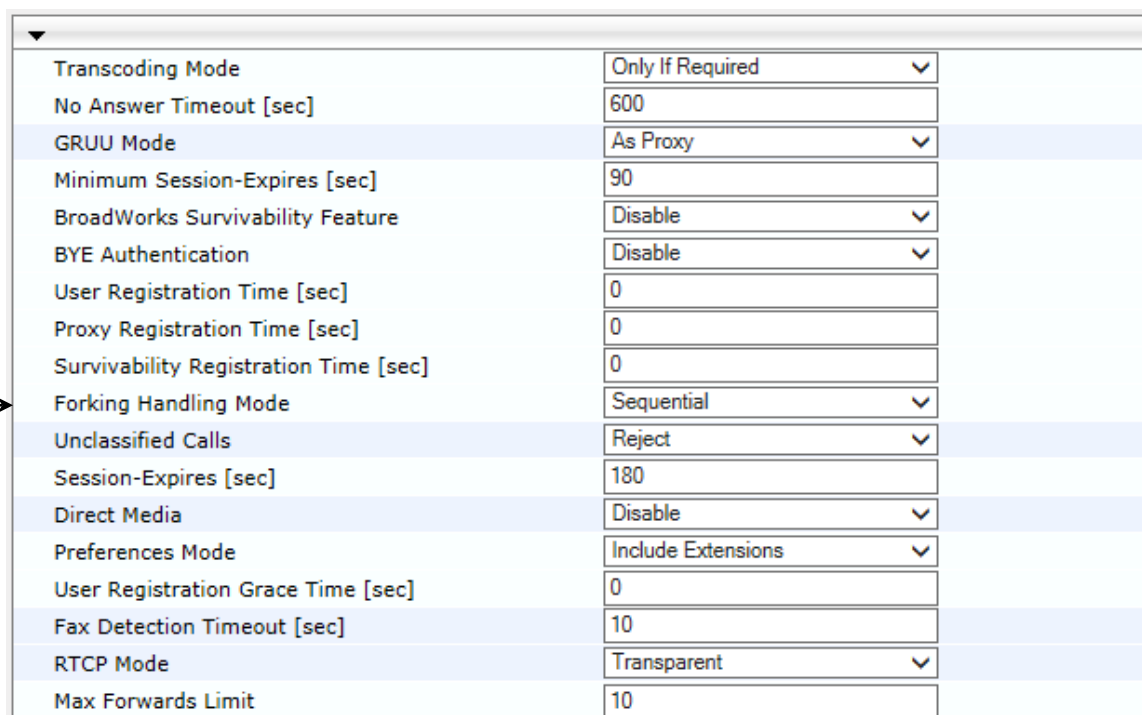
4.15.1 Step 15a: Configure Call Forking Mode

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

Figure 4-52: Configuring Forking Mode



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

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

3. Click **Submit**.

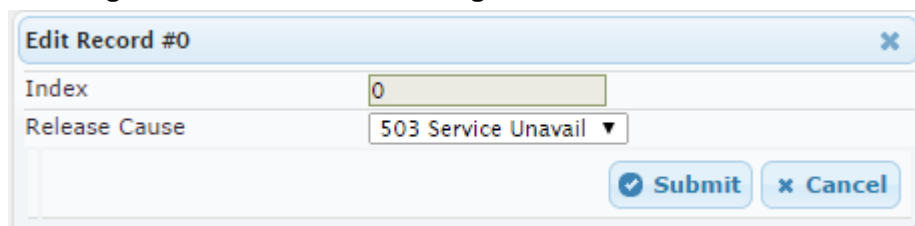
4.15.2 Step 15b: Configure SBC Alternative Routing Reasons

This step describes how to configure the SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case, the SBC attempts to locate an alternative route for the call.

➤ **To configure SIP reason codes for alternative IP routing:**

1. Open the SBC Alternative Routing Reasons page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Alternative Routing Reasons**).
2. Click **Add**; the following dialog box appears:

Figure 4-53: Alternative Routing Reasons Table - Add Record



Edit Record #0	
Index	0
Release Cause	503 Service Unavail ▼
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Click **Submit**.

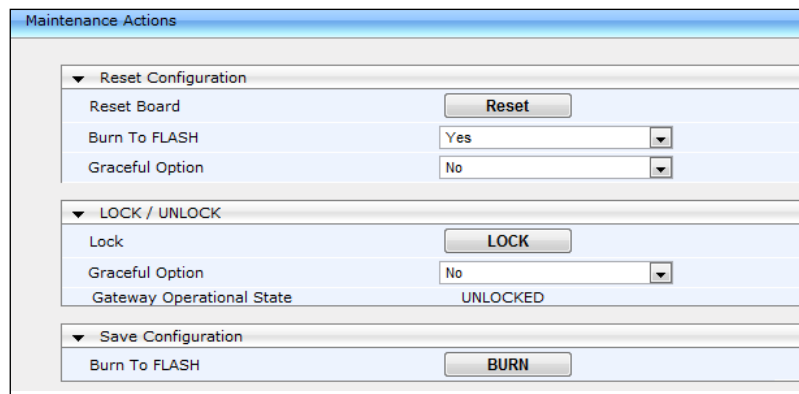
4.16 Step 16: Reset the SBC

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

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

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

Figure 4-54: Resetting the SBC



The screenshot shows the 'Maintenance Actions' page. It contains three main sections: 'Reset Configuration', 'LOCK / UNLOCK', and 'Save Configuration'. The 'Reset Configuration' section has a 'Reset Board' button, a 'Burn To FLASH' dropdown set to 'Yes', and a 'Graceful Option' dropdown set to 'No'. The 'LOCK / UNLOCK' section has a 'Lock' button, a 'Graceful Option' dropdown set to 'No', and a 'Gateway Operational State' set to 'UNLOCKED'. The 'Save Configuration' section has a 'Burn To FLASH' button.

Maintenance Actions	
▼ 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.

This page is intentionally left blank.

A Configuring SBC to Send 414 Request-URI Too Long

The procedure below describes how to configure the SBC to send a 414 Request-URI Too Long response, when it encounters a Request URI it cannot handle due to excessive length.

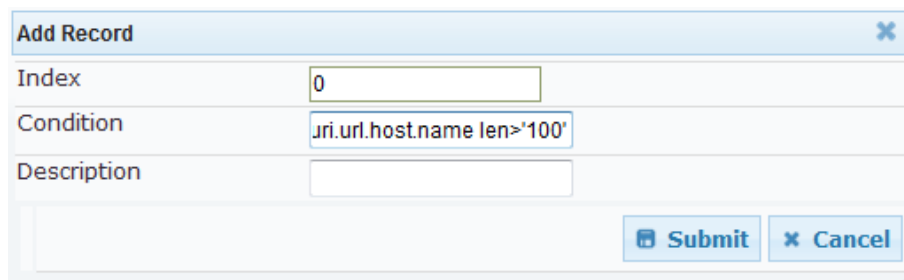
When the SBC receives an INVITE with a long Request URI (a condition rule), it routes it to an unknown destination IP address (i.e., 1.1.1.1). It sets a variable for this call to **1**. After a timeout, the SBC generates an internal 408 Request Timeout response. Using message manipulation, the SBC converts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

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

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

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

Figure A-1: Configuring a Condition for the Route



The screenshot shows a web-based 'Add Record' dialog box. It has a title bar with a close button. Inside, there are three input fields: 'Index' with the value '0', 'Condition' with the value 'header.request-uri.url.host.name len>'100'', and 'Description' which is empty. At the bottom right, there are two buttons: 'Submit' and 'Cancel'.

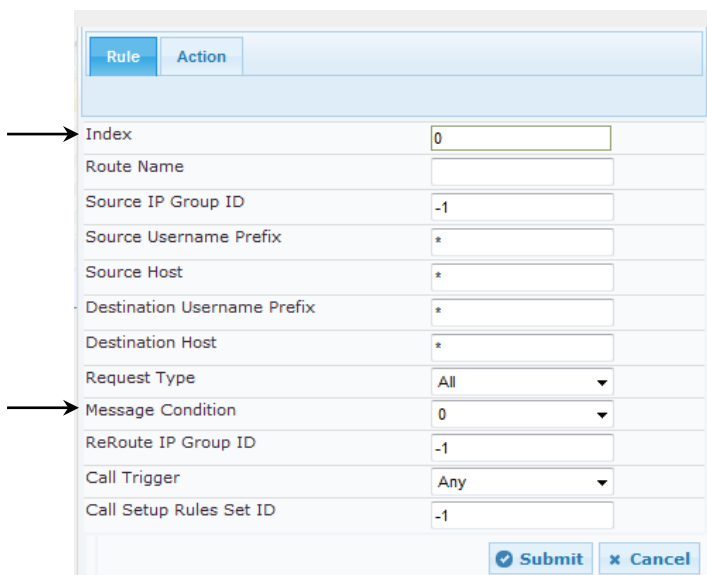
3. Click **Submit**.

➤ **To configure the route:**

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

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

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



Rule Action

Index 0

Route Name

Source IP Group ID -1

Source Username Prefix *

Source Host *

Destination Username Prefix *

Destination Host *

Request Type All

Message Condition 0

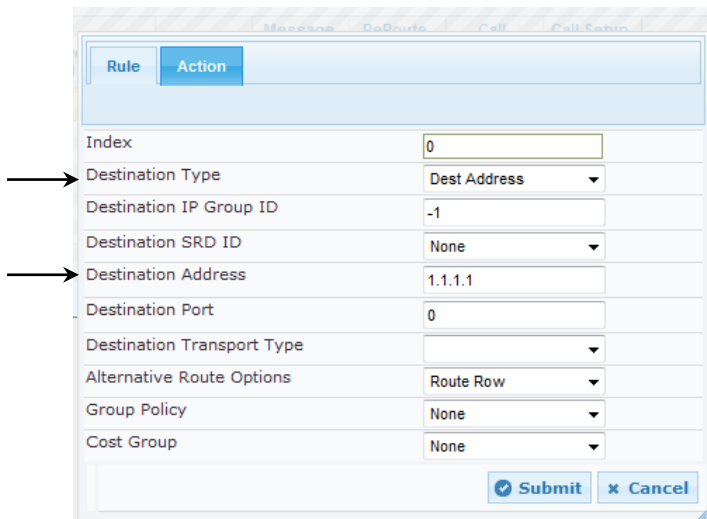
ReRoute IP Group ID -1

Call Trigger Any

Call Setup Rules Set ID -1

Submit Cancel

Figure A-3: IP-to-IP Routing Action for Long-URI Calls



Rule Action

Index 0

Destination Type Dest Address

Destination IP Group ID -1

Destination SRD ID None

Destination Address 1.1.1.1

Destination Port 0

Destination Transport Type

Alternative Route Options Route Row

Group Policy None

Cost Group None

Submit Cancel

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

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

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

Figure A-4: Manipulation Rule to Set a Variable to '1' in Case of Long-URI Call

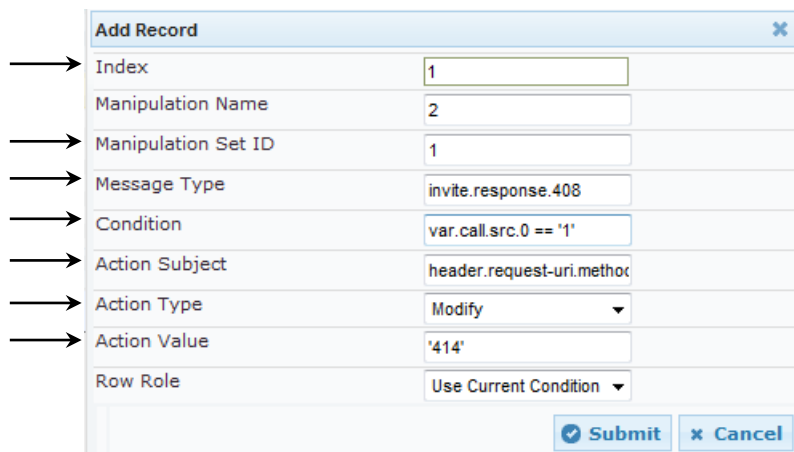
The screenshot shows the 'Add Record' dialog box with the following values entered:

- Index: 0
- Manipulation Name: (empty)
- Manipulation Set ID: 1
- Message Type: invite.request
- Condition: uri.url.host.name len>'100'
- Action Subject: var.call.src.0
- Action Type: Modify
- Action Value: 1
- Row Role: Use Current Condition

Buttons at the bottom: Submit, Cancel.

- c. Click **Submit**.
3. Add a rule to convert 408 to '414':
 - a. Click **Add**.
 - b. Configure the parameters like this:

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

Figure A-5: Manipulation Rule to Convert 408 to '414'


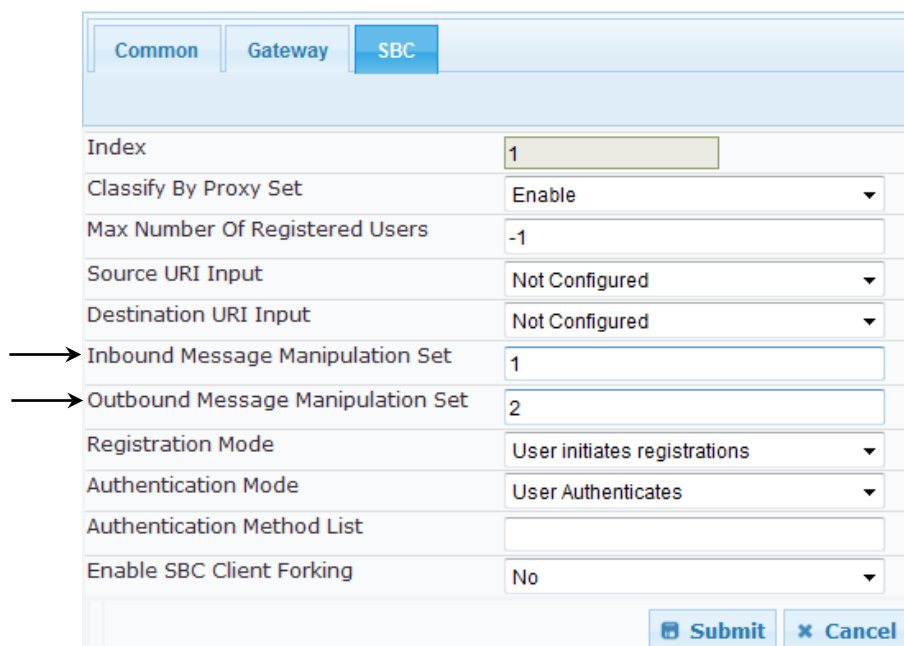
Add Record	
Index	1
Manipulation Name	2
Manipulation Set ID	1
Message Type	invite.response.408
Condition	var.call.src.0 == '1'
Action Subject	header.request-uri.method
Action Type	Modify
Action Value	'414'
Row Role	Use Current Condition
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- c. Click **Submit**.

Figure A-6: Message Manipulations Page

Message Manipulations							
Add +		Insert +					
Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	1	invite.request	header.request-uri	var.call.src.0	Modify	'1'	Use Current Condition
1	2	invite.response.408	var.call.src.0 == '1'	Header.request-uri	Modify	'414'	Use Current Condition

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

Figure A-7: Assigning Manipulation Rule to IP Group 1


Common Gateway SBC	
Index	1
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	1
Outbound Message Manipulation Set	2
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
Enable SBC Client Forking	No
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- f. Click **Submit**.

This page is intentionally left blank.



Configuration Note

