

Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

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



Microsoft Partner
Gold Communications



Version 6.8

January 2015

Document # LTRT-39338

Table of Contents

1	Introduction	9
1.1	Intended Audience	9
1.2	About AudioCodes E-SBC Product Series.....	9
2	Component Information.....	11
2.1	AudioCodes E-SBC Version	11
2.2	Virgin Media SIP Trunking Version	11
2.3	Microsoft Lync Server 2013 Version	11
2.4	Interoperability Test Topology	12
2.4.1	Environment Setup	13
2.4.2	Known Limitations.....	13
3	Configuring Lync Server 2013	15
3.1	Configuring the E-SBC as an IP / PSTN Gateway	15
3.2	Configuring the "Route" on Lync Server 2013.....	23
4	Configuring AudioCodes E-SBC.....	33
4.1	Step 1: IP Network Interfaces Configuration	34
4.1.1	Step 1a: Configure VLANs.....	35
4.1.2	Step 1b: Configure Network Interfaces.....	36
4.1.3	Step 1c: Configure the Native VLAN ID.....	38
4.2	Step 2: Enable the SBC Application	39
4.3	Step 3: Signaling Routing Domains Configuration	40
4.3.1	Step 3a: Configure Media Realms.....	40
4.3.2	Step 3b: Configure SRDs	42
4.3.3	Step 3c: Configure SIP Signaling Interfaces	43
4.4	Step 4: Configure Proxy Sets	44
4.5	Step 5: Configure IP Groups.....	48
4.6	Step 6: Configure IP Profiles	50
4.7	Step 7: Configure Coders	57
4.8	Step 8: SIP TLS Connection Configuration.....	58
4.8.1	Step 8a: Configure the NTP Server Address.....	58
4.8.2	Step 8b: Configure a Certificate	59
4.9	Step 9: Configure SRTP	64
4.10	Step 10: Configure IP-to-IP Call Routing Rules	65
4.11	Step 11: Configure IP-to-IP Manipulation Rules.....	79
4.12	Step 12: Configure Message Manipulation Rules	81
4.13	Step 13: Configure Registration Accounts	84
4.14	Step 14: Miscellaneous Configuration.....	86
4.14.1	Step 14a: Configure Call Forking Mode	86
4.15	Step 15: Reset the E-SBC	87
A	AudioCodes INI File	89

List of Figures

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Lync with Virgin Media SIP Trunk.....	12
Figure 3-1: Starting the Lync Server Topology Builder	15
Figure 3-2: Topology Builder Dialog Box.....	16
Figure 3-3: Save Topology Dialog Box.....	16
Figure 3-4: Downloaded Topology	17
Figure 3-5: Choosing New IP/PSTN Gateway	17
Figure 3-6: Define the PSTN Gateway FQDN.....	18
Figure 3-7: Define the IP Address	18
Figure 3-8: Define the Root Trunk.....	19
Figure 3-9: E-SBC added as IP/PSTN Gateway and Trunk Created.....	20
Figure 3-10: Choosing Publish Topology	20
Figure 3-11: Publish the Topology	21
Figure 3-12: Publishing in Progress	21
Figure 3-13: Publishing Wizard Complete.....	22
Figure 3-14: Opening the Lync Server Control Panel	23
Figure 3-15: Lync Server Credentials.....	24
Figure 3-16: Microsoft Lync Server 2013 Control Panel	24
Figure 3-17: Voice Routing Page	25
Figure 3-18: Route Tab	25
Figure 3-19: Adding New Voice Route	26
Figure 3-20: Adding New Trunk	26
Figure 3-21: List of Deployed Trunks	27
Figure 3-22: Selected E-SBC Trunk.....	27
Figure 3-23: Associating PSTN Usage to Route	28
Figure 3-24: Confirmation of New Voice Route.....	28
Figure 3-25: Committing Voice Routes	29
Figure 3-26: Uncommitted Voice Configuration Settings	29
Figure 3-27: Confirmation of Successful Voice Routing Configuration	29
Figure 3-28: Voice Routing Screen Displaying Committed Routes	30
Figure 3-29: Voice Routing Screen – Trunk Configuration Tab	30
Figure 4-1: Network Interfaces in Interoperability Test Topology.....	34
Figure 4-2: Configured VLAN IDs in Ethernet Device Table.....	35
Figure 4-3: Configured Network Interface in IP Interfaces Table	37
Figure 4-4: Configured Port Native VLAN	38
Figure 4-5: Enabling SBC Application	39
Figure 4-6: Configuring Media Realm for LAN	40
Figure 4-7: Configuring Media Realm for WAN.....	41
Figure 4-8: Configured Media Realms in Media Realm Table	41
Figure 4-9: Configuring LAN SRD	42
Figure 4-10: Configuring WAN SRD.....	42
Figure 4-11: Configured SIP Interfaces in SIP Interface Table	43
Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013.....	45
Figure 4-13: Configuring Proxy Set for Virgin Media SIP Trunk A	46
Figure 4-14: Configuring Proxy Set for Virgin Media SIP Trunk B	47
Figure 4-15: Configured IP Groups in IP Group Table.....	49
Figure 4-16: Configuring IP Profile for Lync Server 2013 – Common Tab	51
Figure 4-17: Configuring IP Profile for Lync Server 2013 – SBC Tab.....	53
Figure 4-18: Configuring IP Profile for Virgin Media SIP Trunk – Common Tab.....	54
Figure 4-19: Configuring IP Profile for Virgin Media SIP Trunk – SBC Tab.....	56
Figure 4-20: Configuring Allowed Coders Group for Virgin Media SIP Trunk.....	57
Figure 4-21: Configuring NTP Server Address.....	58
Figure 4-22: Certificates Page - Creating CSR	59
Figure 4-23: Microsoft Certificate Services Web Page	60
Figure 4-24: Request a Certificate Page	60
Figure 4-25: Advanced Certificate Request Page	61
Figure 4-26: Submit a Certificate Request or Renewal Request Page	61

Figure 4-27: Certificate Issued Page	62
Figure 4-28: Download a CA Certificate, Certificate Chain, or CRL Page	62
Figure 4-29: Certificates Page (Uploading Certificate)	63
Figure 4-30: Configuring SRTP	64
Figure 4-31: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab	66
Figure 4-32: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab	66
Figure 4-33: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk A – Rule Tab	67
Figure 4-34: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk A – Action Tab	68
Figure 4-35: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk B – Rule Tab	69
Figure 4-36: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk B – Action Tab	70
Figure 4-37: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk A – Rule tab	71
Figure 4-38: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk A – Action tab	72
Figure 4-39: Configuring IP-to-IP Routing Rule for Virgin Media Trunk A to Lync – Rule tab	73
Figure 4-40: Configuring IP-to-IP Routing Rule for Virgin Media Trunk A to Lync – Action tab	74
Figure 4-41: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk B – Rule tab	75
Figure 4-42: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk B – Action tab	76
Figure 4-43: Configuring IP-to-IP Routing Rule for Virgin Media Trunk B to Lync – Rule tab	77
Figure 4-44: Configuring IP-to-IP Routing Rule for Virgin Media Trunk B to Lync – Action tab	78
Figure 4-45: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table	78
Figure 4-46: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab	79
Figure 4-47: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab	80
Figure 4-48: Example of Configured IP-to-IP Outbound Manipulation Rules	80
Figure 4-49: Configuring SIP Message Manipulation Rule 1 (for Virgin Media SIP Trunk A)	81
Figure 4-50: Example of Configured SIP Message Manipulation Rule	82
Figure 4-51: Assigning Manipulation Set to IP Group 2	82
Figure 4-52: Assigning Manipulation Set 4 to IP Group 3	83
Figure 4-53: Configuring SIP Registration Accounts	85
Figure 4-54: Proxy & Registration	85
Figure 4-55: Configuring Forking Mode	86
Figure 4-56: Resetting the E-SBC	87

List of Tables

Table 2-1: AudioCodes E-SBC Version	11
Table 2-2: Virgin Media Version	11
Table 2-3: Microsoft Lync Server 2013 Version	11
Table 2-4: Environment Setup	13

Notice

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

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

© Copyright 2015 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: January-5-2015

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 Terminology

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

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

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

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.80A.009.005
Protocol	▪ SIP/UDP (to the Virgin Media SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 Virgin Media SIP Trunking Version

Table 2-2: Virgin Media Version

Vendor/Service Provider	Virgin Media
SSW Model/Service	GenBand
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

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

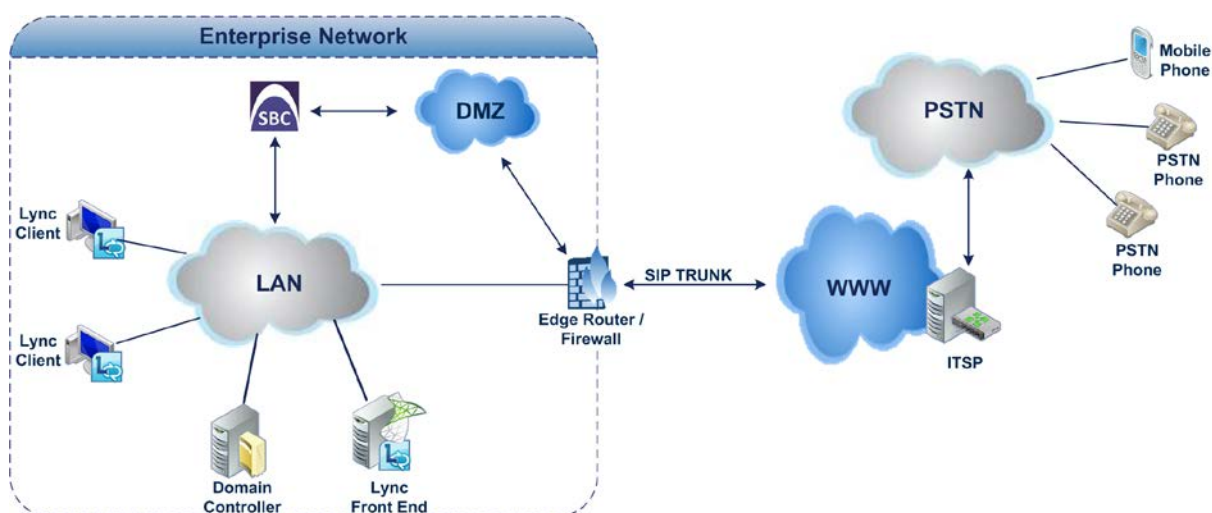
2.4 Interoperability Test Topology

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

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

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Lync with Virgin Media SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Lync Server 2013 environment is located on the Enterprise's LAN ▪ Virgin Media SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ Virgin Media SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ Virgin Media SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ Virgin Media SIP Trunk operates with RTP media type

2.4.2 Known Limitations

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

This page is intentionally left blank.

3 Configuring Lync Server 2013

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



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

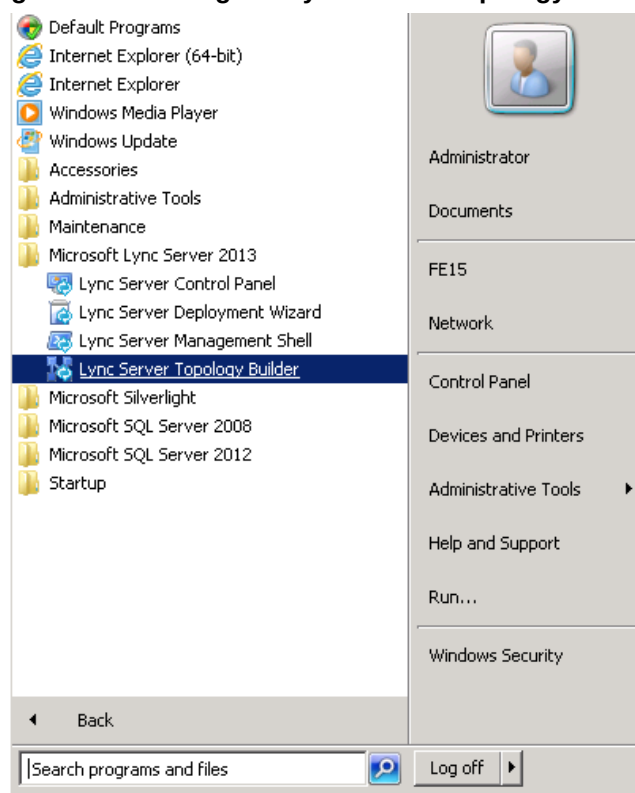
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

➤ **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**

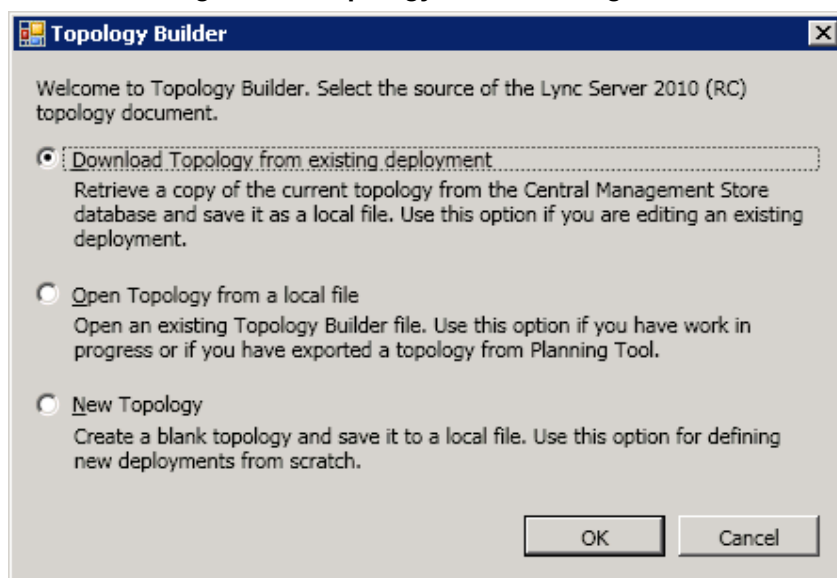
1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



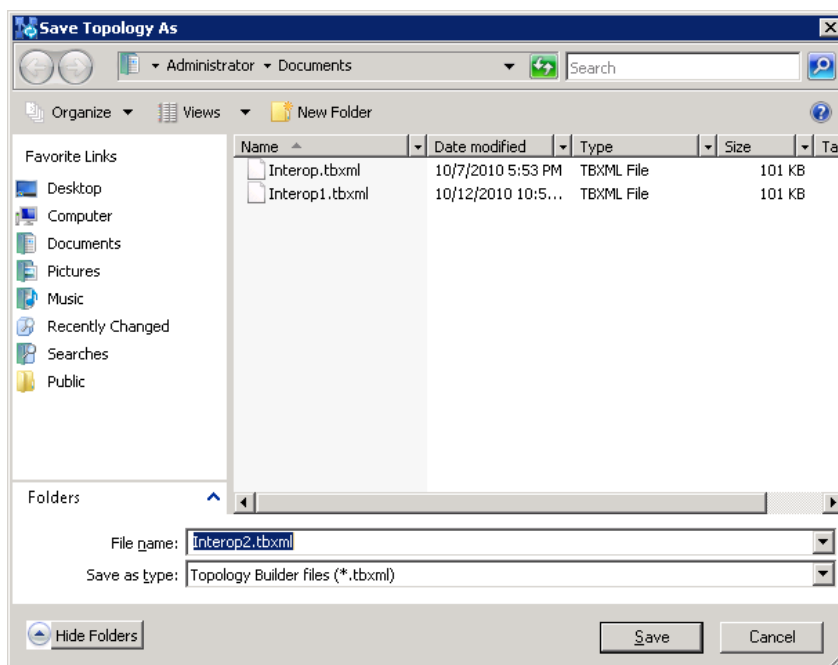
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

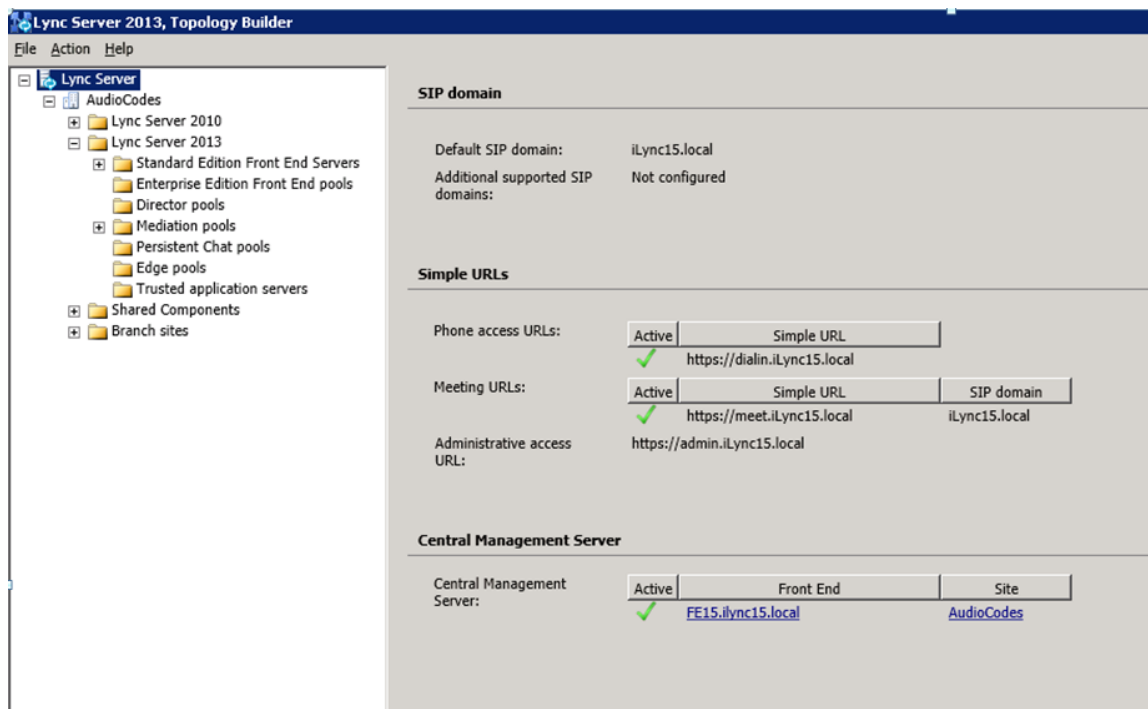
Figure 3-3: Save Topology Dialog Box



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

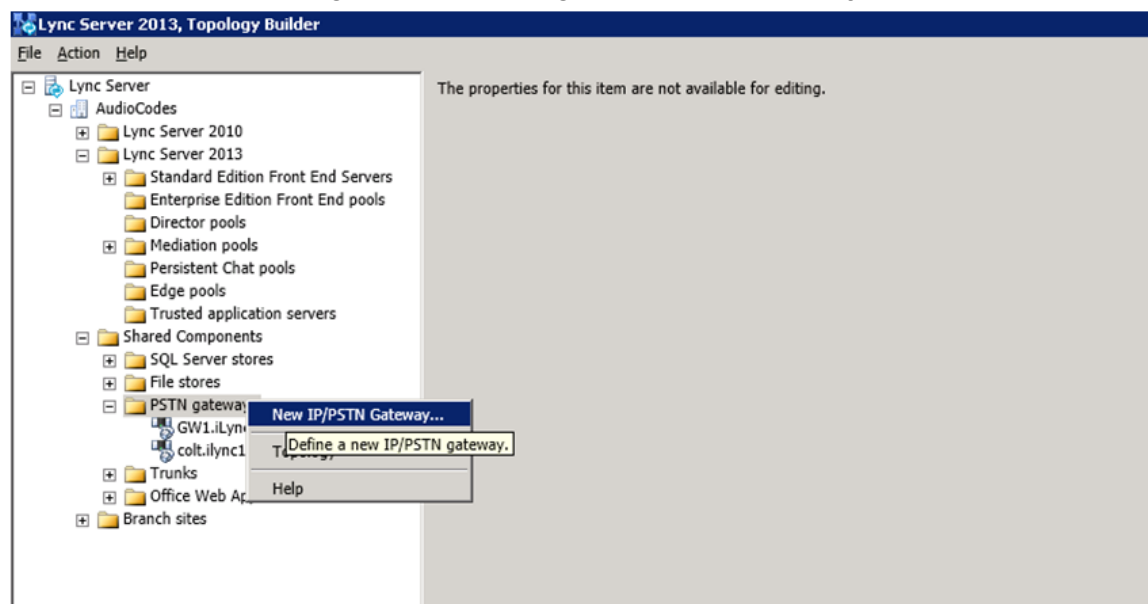
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



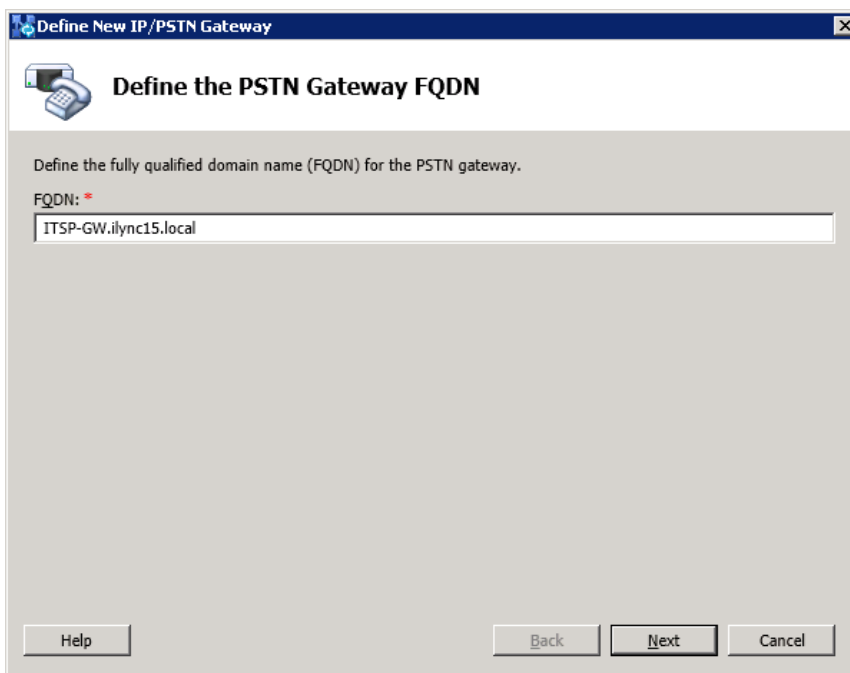
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

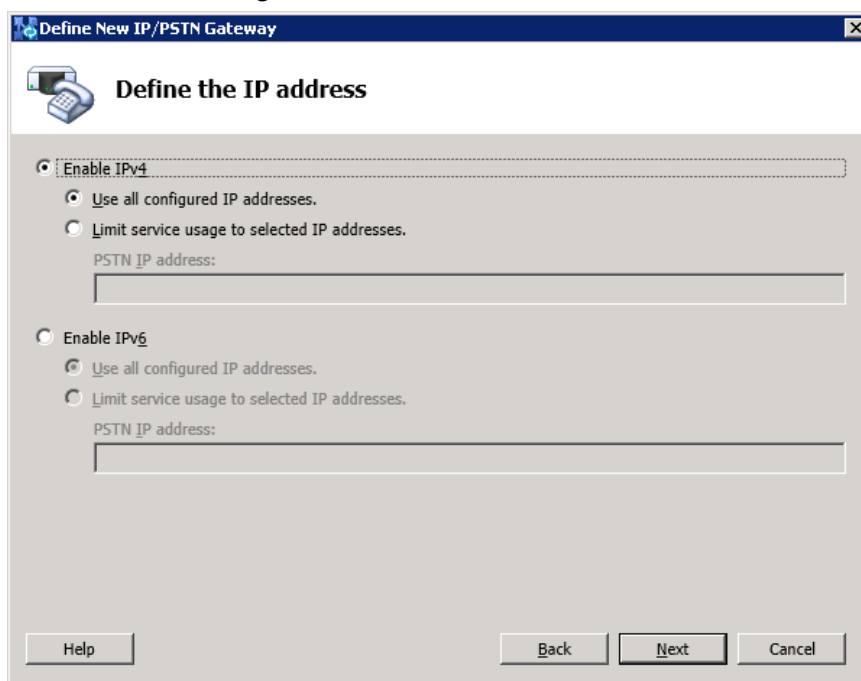
Figure 3-6: Define the PSTN Gateway FQDN



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

5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP-GW.ilync15.local**). Update this FQDN in the relevant DNS record, and then click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



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

6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.
7. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP and FQDN, and gateway listening port.

**Notes:**

- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

Figure 3-8: Define the Root Trunk

Define New IP/PSTN Gateway

Define the root trunk

Trunk name: *
ITSP-GW.ilync15.local

Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
FE15.ilync15.local AudioCodes

Associated Mediation Server port: *
5067

Help Back Finish Cancel

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

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

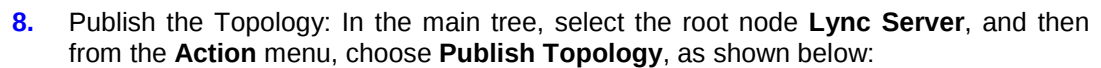
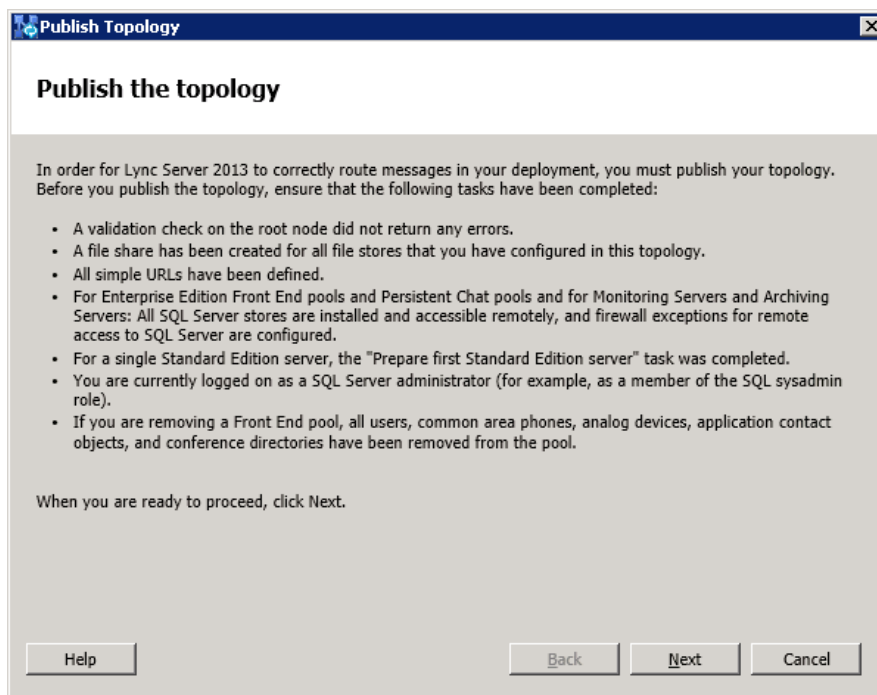


Figure 3-10: Choosing Publish Topology



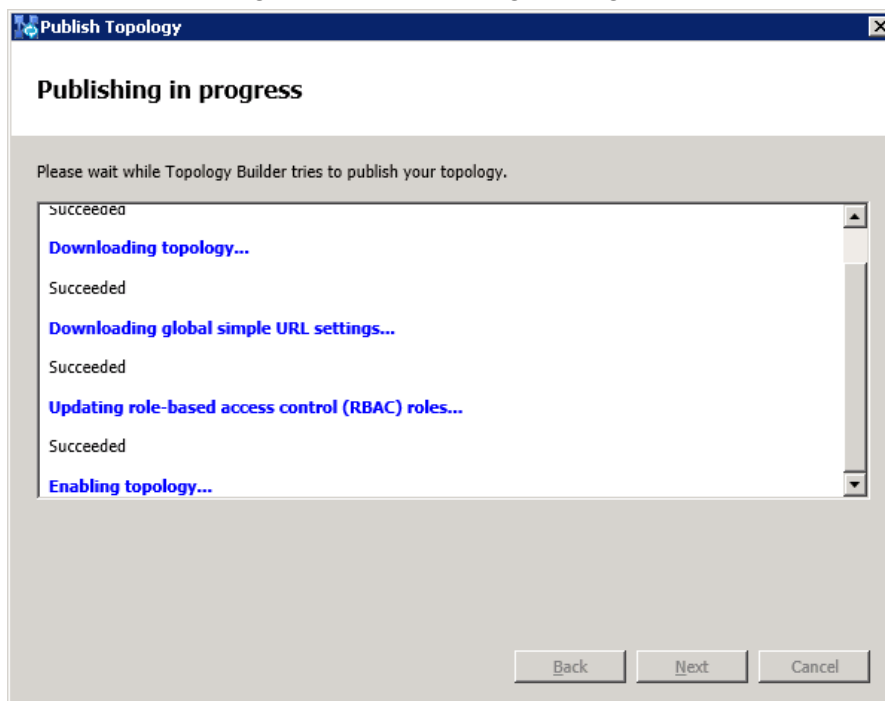
The following is displayed:

Figure 3-11: Publish the Topology



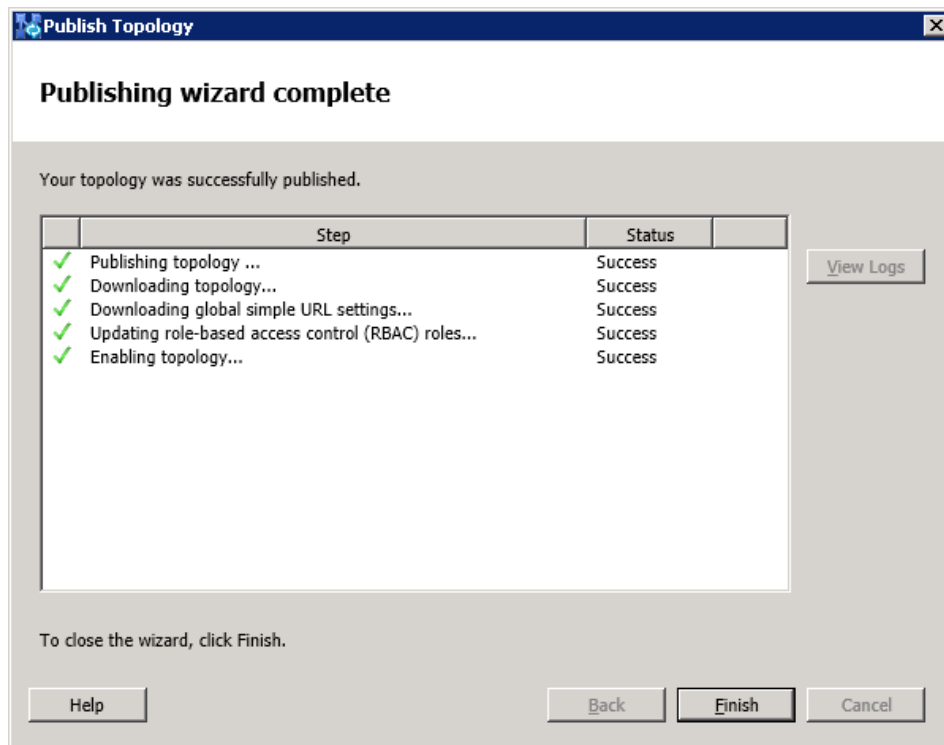
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

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

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

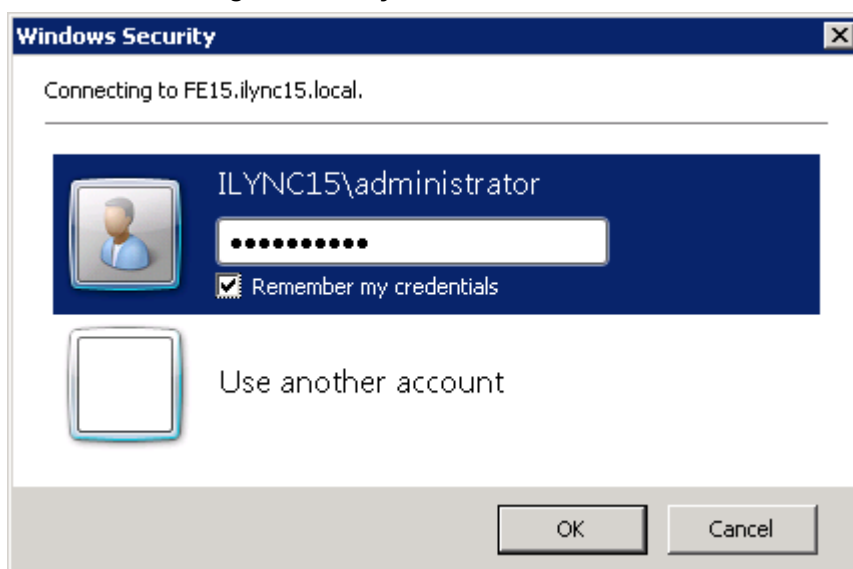
1. Start the Microsoft Lync Server 2013 Control Panel (**Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel**), as shown below:

Figure 3-14: Opening the Lync Server Control Panel



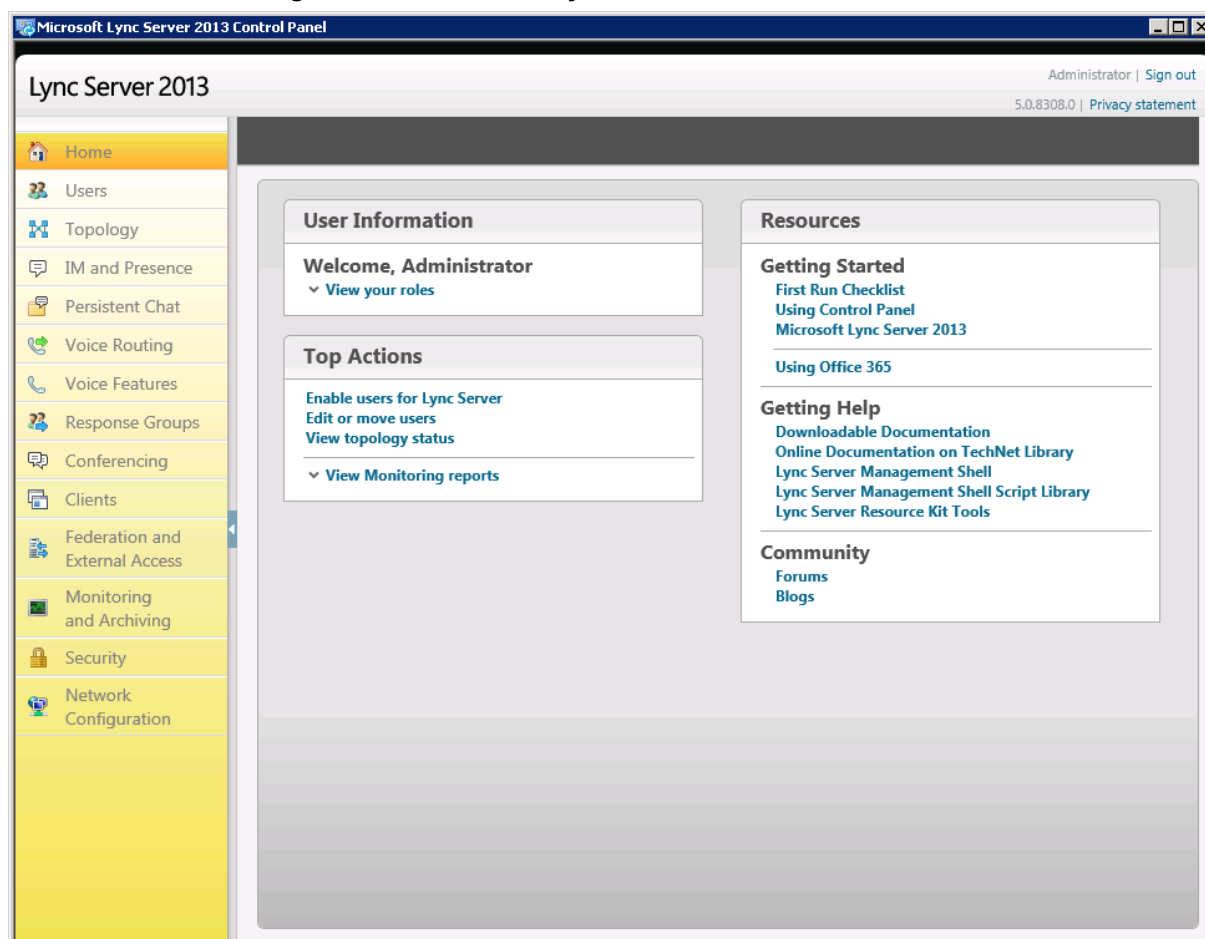
2. You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



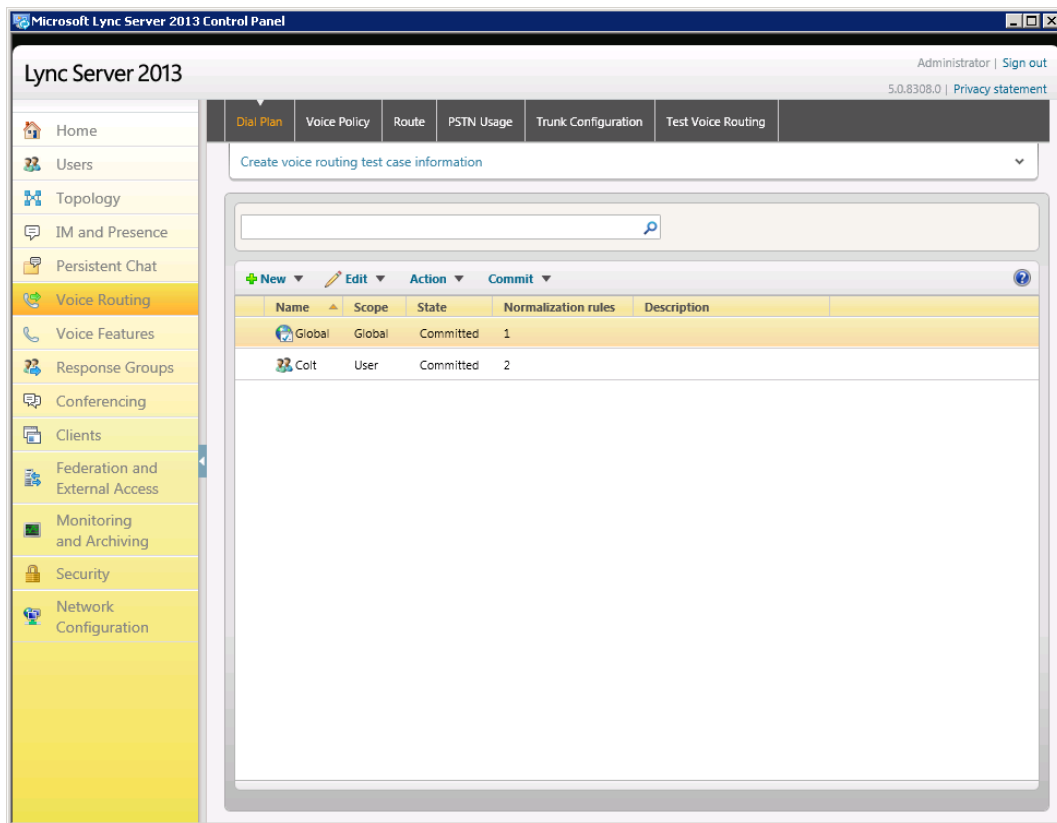
3. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



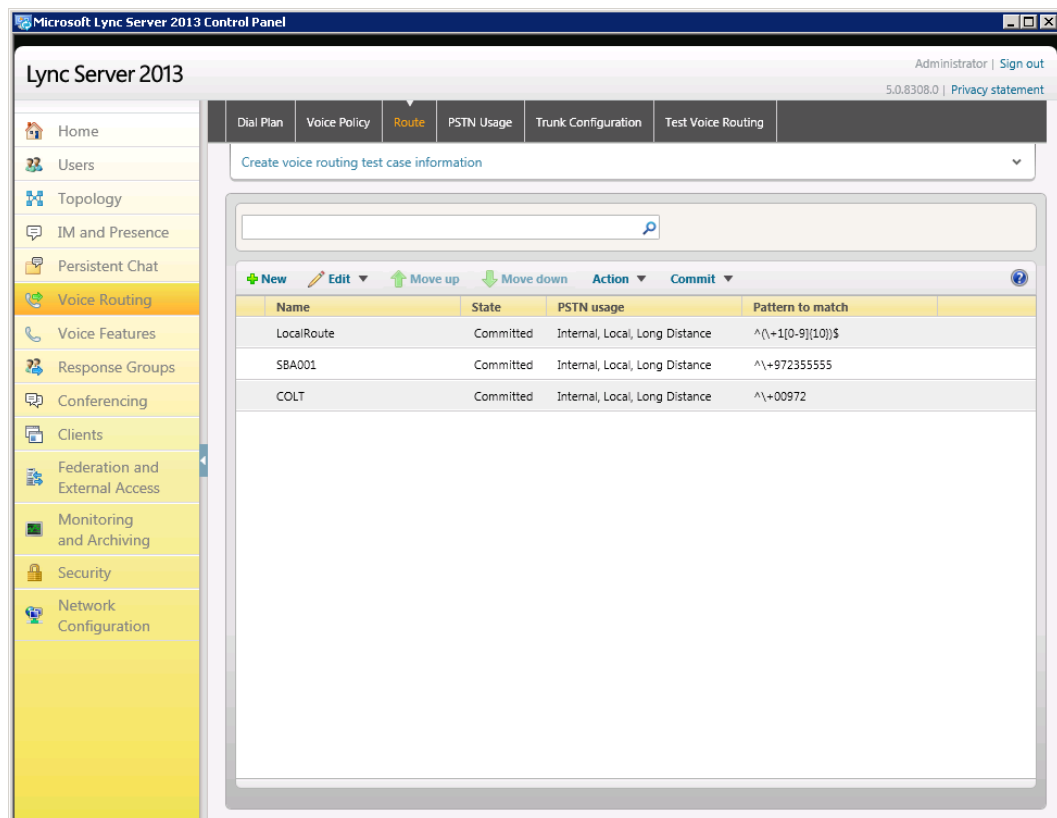
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



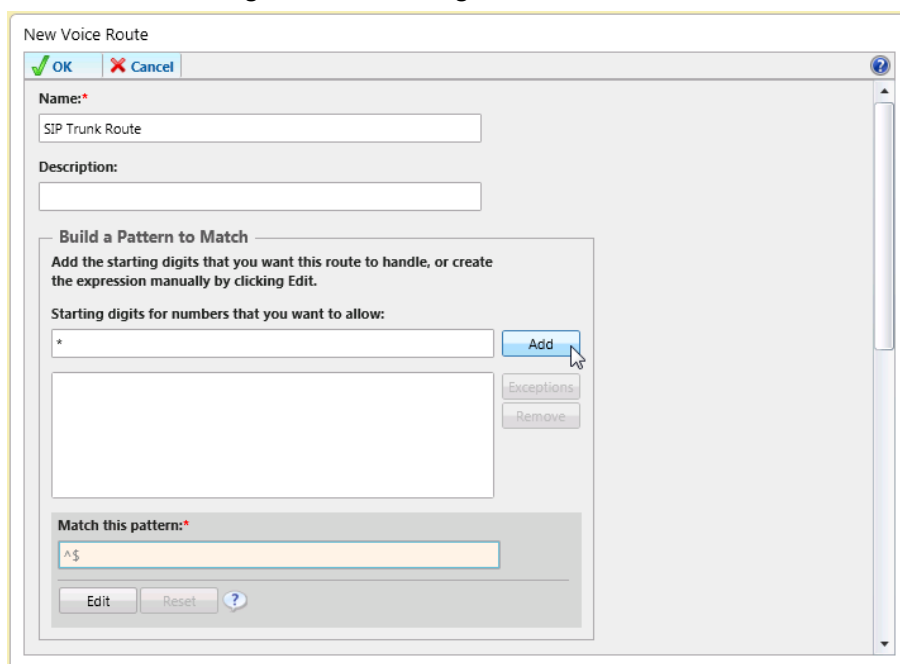
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



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

Figure 3-19: Adding New Voice Route



New Voice Route

OK Cancel

Name:*

SIP Trunk Route

Description:

Build a Pattern to Match

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

Starting digits for numbers that you want to allow:

* Add

Exceptions

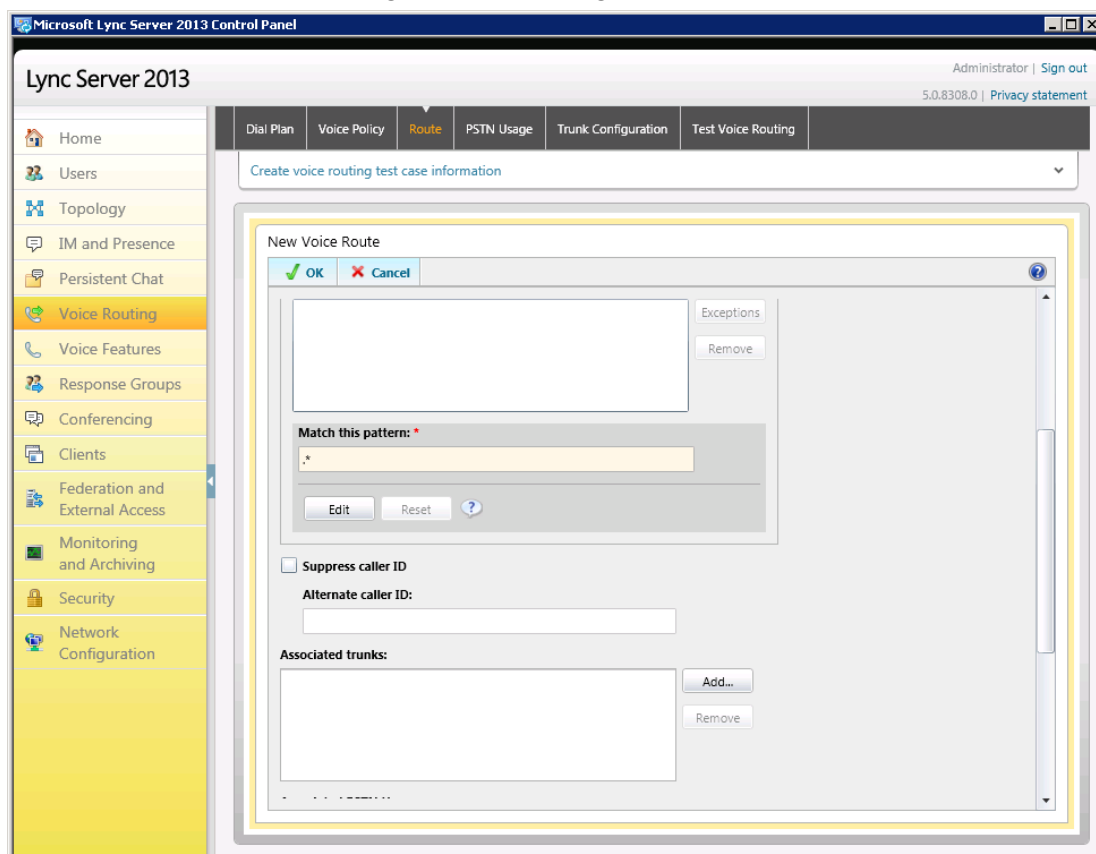
Remove

Match this pattern:*

^\$ Edit Reset ?

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

Figure 3-20: Adding New Trunk



Microsoft Lync Server 2013 Control Panel

Lync Server 2013

Administrator | Sign out

5.0.8308.0 | Privacy statement

Home

Users

Topology

IM and Presence

Persistent Chat

Voice Routing

Voice Features

Response Groups

Conferencing

Clients

Federation and External Access

Monitoring and Archiving

Security

Network Configuration

Dial Plan

Voice Policy

Route

PSTN Usage

Trunk Configuration

Test Voice Routing

Create voice routing test case information

New Voice Route

OK Cancel

Exceptions

Remove

Match this pattern: *

* Edit Reset ?

Suppress caller ID

Alternate caller ID:

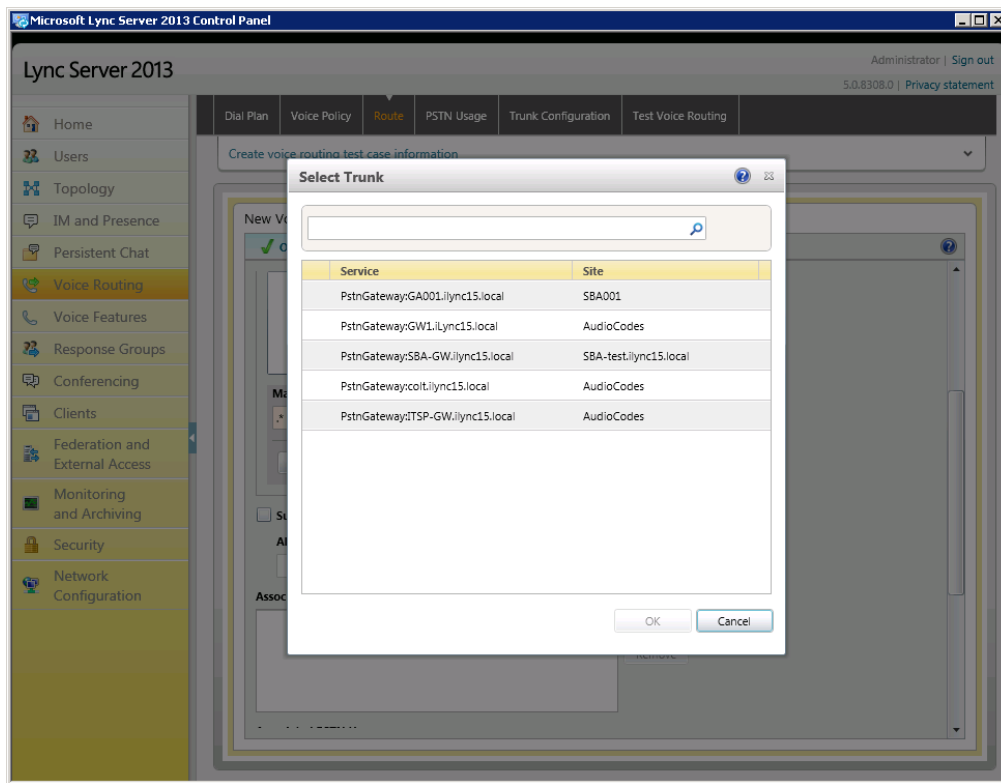
Associated trunks:

Add...

Remove

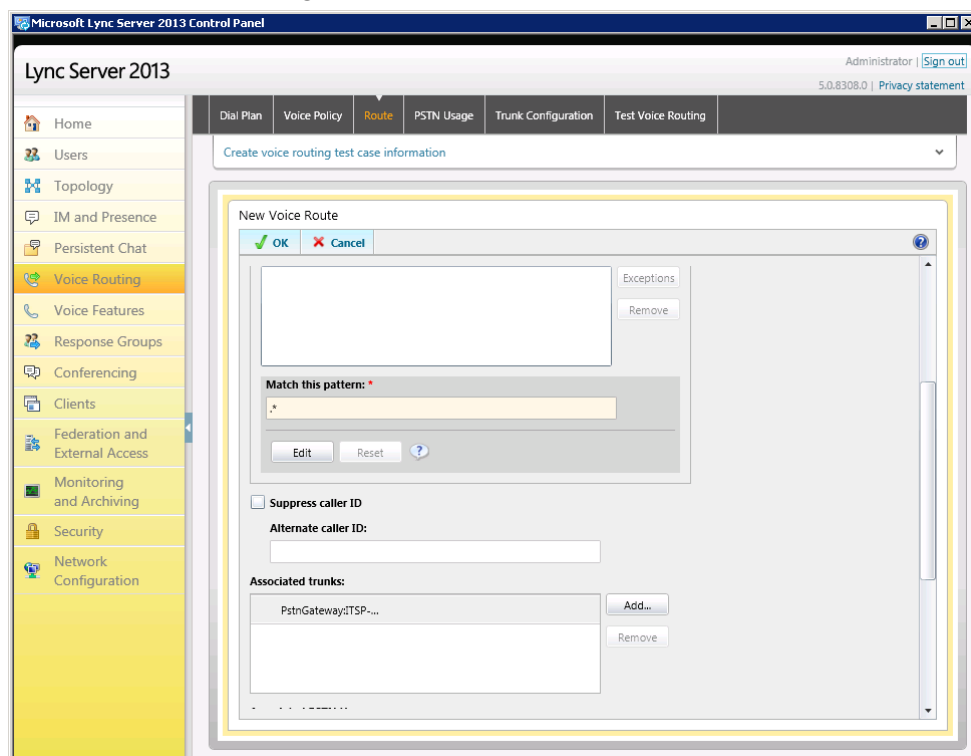
9. Associate the route with the E-SBC Trunk that you created:
 - a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



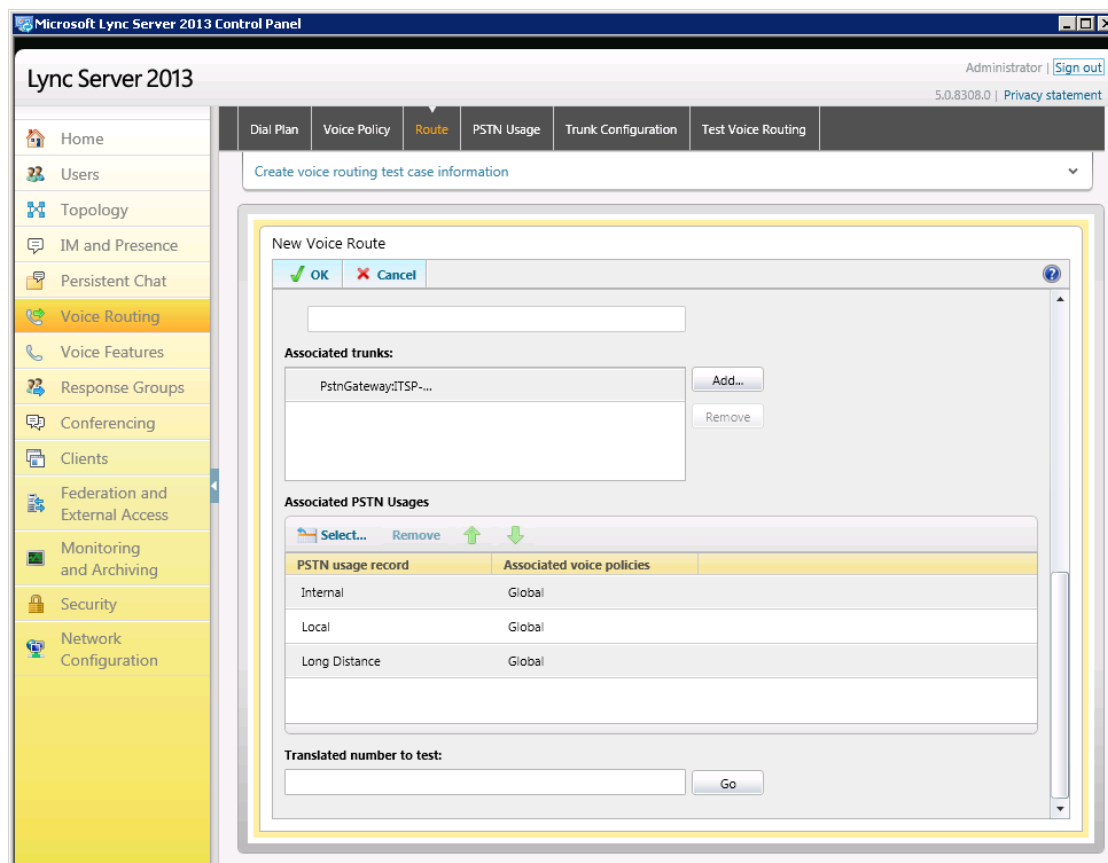
- b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



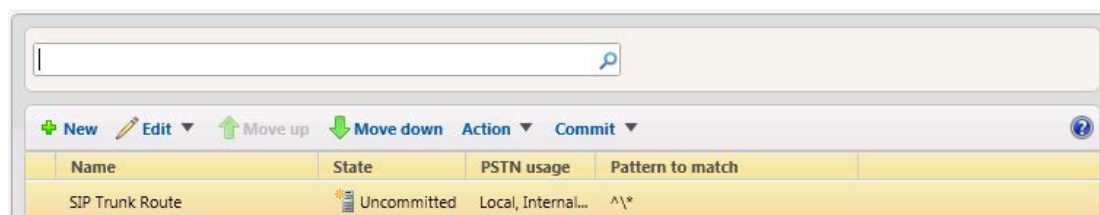
10. Associate a PSTN Usage to this route:
 - a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



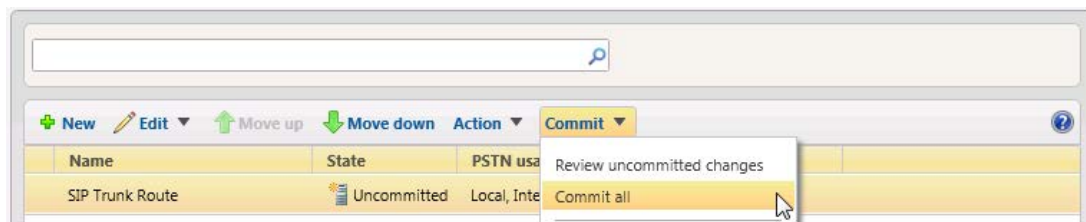
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



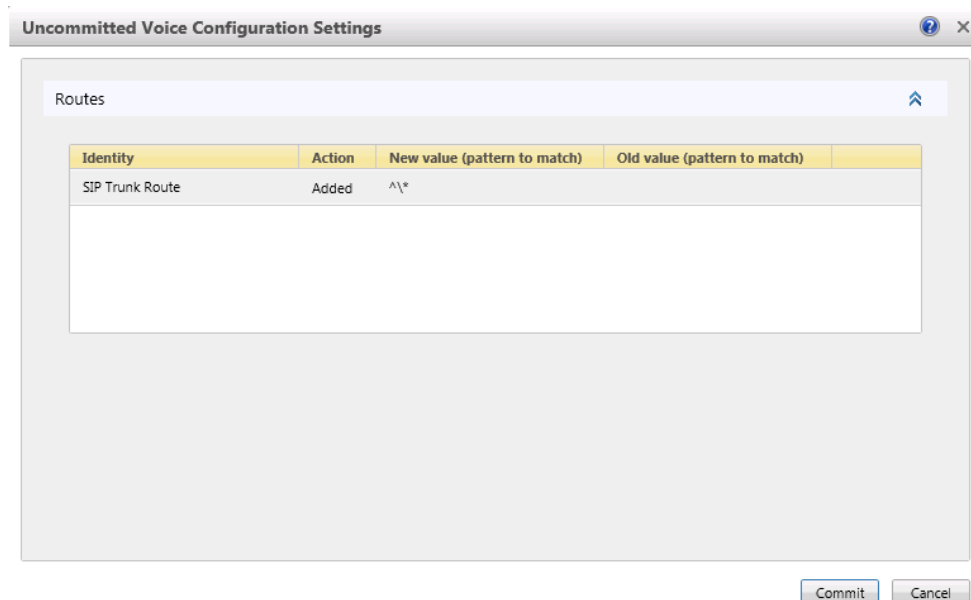
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



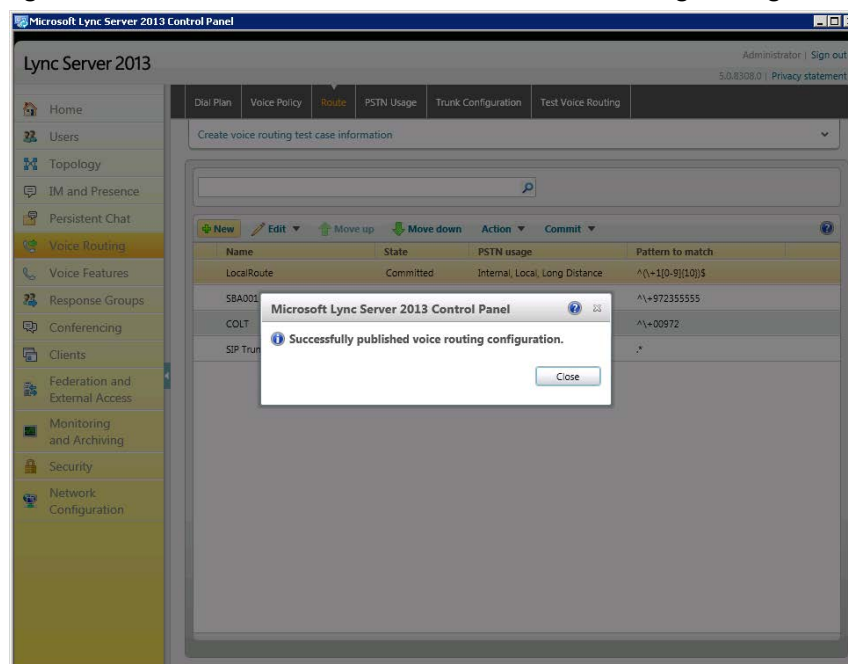
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



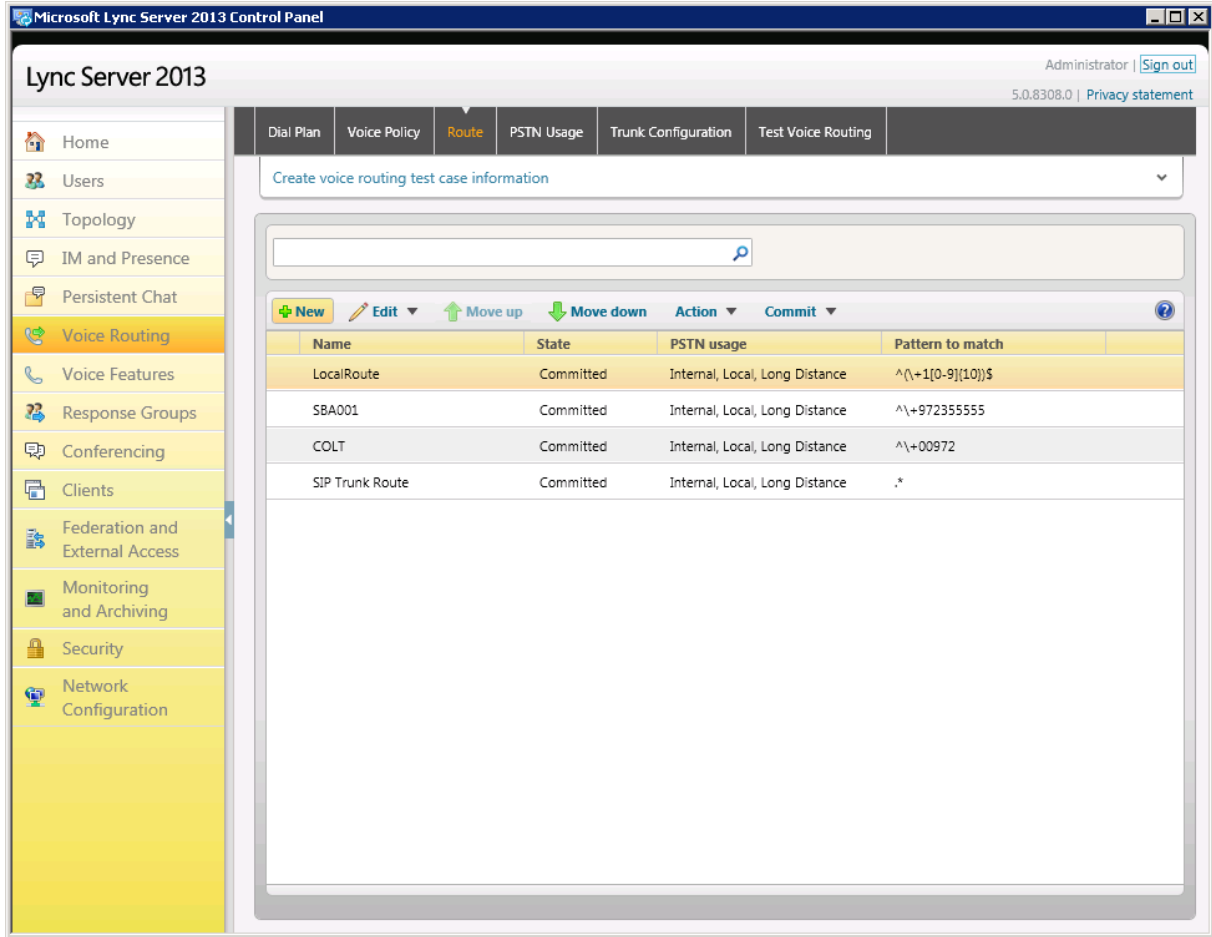
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirmation of Successful Voice Routing Configuration



14. Click **Close**; the new committed Route is displayed in the Voice Routing page, as shown below:

Figure 3-28: Voice Routing Screen Displaying Committed Routes



The screenshot shows the Microsoft Lync Server 2013 Control Panel. The left sidebar contains navigation links: Home, Users, Topology, IM and Presence, Persistent Chat, Voice Routing (selected), Voice Features, Response Groups, Conferencing, Clients, Federation and External Access, Monitoring and Archiving, Security, and Network Configuration. The main area shows the 'Route' tab under 'Voice Routing'. A search bar is at the top. Below it, a table lists committed routes:

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

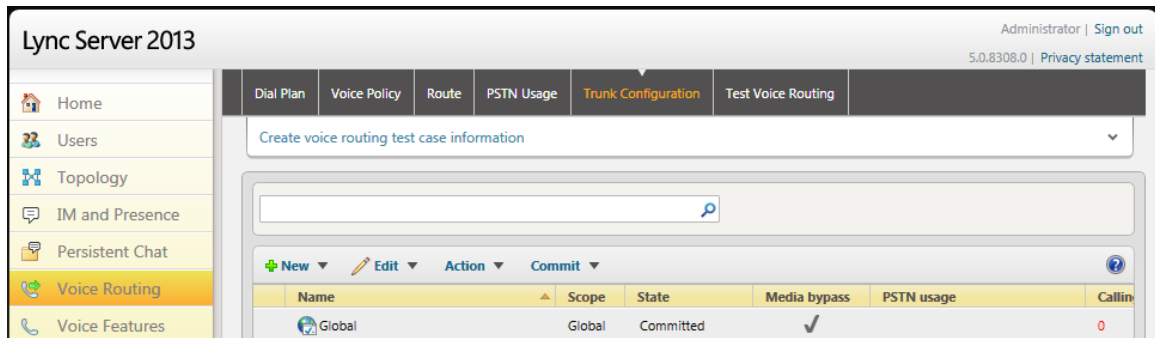
15. For ITSPs that implement a call identifier, continue with the following steps:



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 Virgin Media SIP Trunk in the P-Asserted-Identity header. Using IP Profile configuration (see Section 4.6 on page 50), 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



The screenshot shows the Microsoft Lync Server 2013 Control Panel with the 'Trunk Configuration' tab selected. The left sidebar is the same as in Figure 3-28. The main area shows the 'Trunk Configuration' tab. A search bar is at the top. Below it, a table lists trunk configurations:

Name	Scope	State	Media bypass	PSTN usage	Callin
Global	Global	Committed	✓		0

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

Edit Trunk Configuration - Global

OK Cancel

Scope: Global

Name: *

Global

Description:

Maximum early dialogs supported:

20

Encryption support level:

Required

Refer support:

Enable sending refer to the gateway

☒ Enable media bypass

☒ Centralized media processing

☐ Enable RTP latching

☒ Enable forward call history

☐ Enable forward P-Asserted-Identity data

☒ Enable outbound routing failover timer

^ Associated PSTN Usages

Select... Remove Up Down

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

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

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

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

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

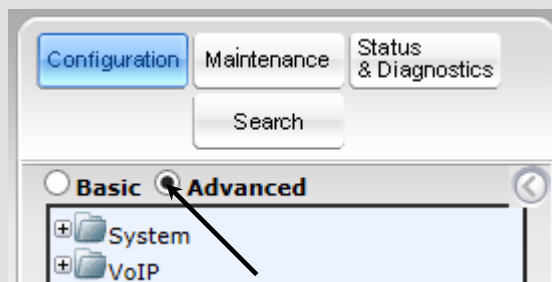
Notes:

- For implementing Microsoft Lync and Virgin Media SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:

- ✓ Microsoft
- ✓ SBC
- ✓ Security
- ✓ DSP
- ✓ RTP
- ✓ SIP

For more information about the Software License Key, contact your AudioCodes sales representative.

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



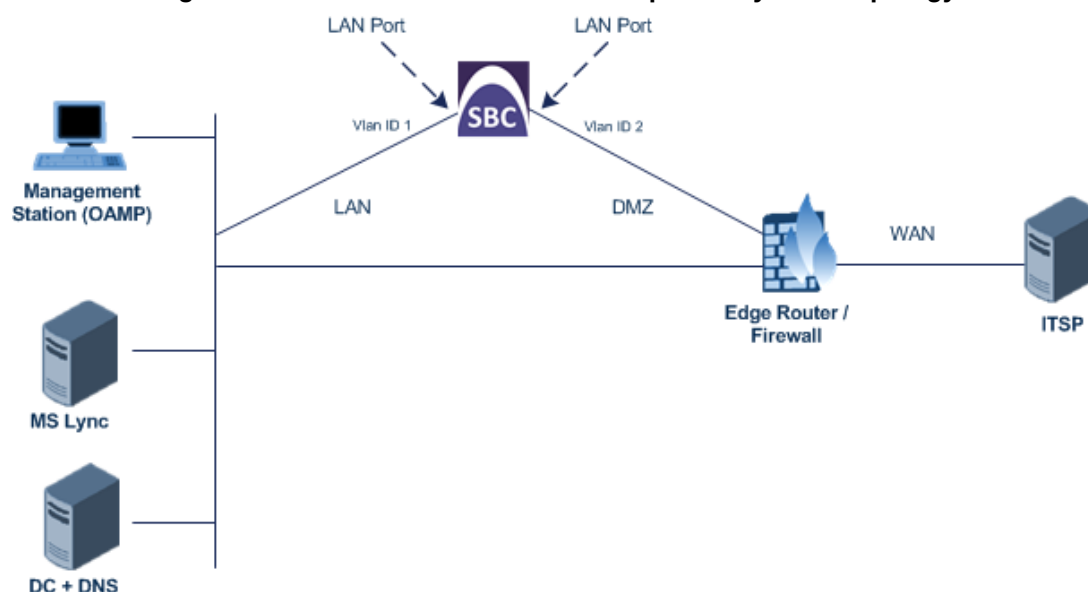
- When the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

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

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

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

➤ **To configure the VLANs:**

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

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

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

Ethernet Device Table			
Add +			
Index	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2
Page 1 of 1 Show 10 records per page View 1 - 2 of 2			

4.1.2 Step 1b: Configure Network Interfaces

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

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

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

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

Parameter	Value
IP Address	10.15.17.77 (IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Gateway	10.15.0.1
VLAN ID	1
Interface Name	Voice (arbitrary descriptive name)
Primary DNS Server IP Address	10.15.25.1
Underlying Device	vlan 1

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

Parameter	Value
Application Type	Media + Control
IP Address	195.189.192.158 (WAN IP address)
Prefix Length	25 (for 255.255.255.128)
Gateway	195.189.192.129 (router's IP address)
VLAN ID	2
Interface Name	WANSP
Primary DNS Server IP Address	80.179.52.100
Secondary DNS Server IP Address	80.179.55.100
Underlying Device	vlan 2

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

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

▼ Interface Table									
Add +									
Index ↕	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	Voice	10.15.25.1	0.0.0.0	vlan 1
1	Media + Control	IPv4 Manual	195.189.192.15	25	195.189.192.12	WANSP	80.179.52.100	80.179.55.100	vlan 2
Page 1 of 1 Show 10 records per page View 1 - 2 of 2									

4.1.3 Step 1c: Configure the Native VLAN ID

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

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

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

Figure 4-4: Configured Port Native VLAN

Physical Ports Settings							
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

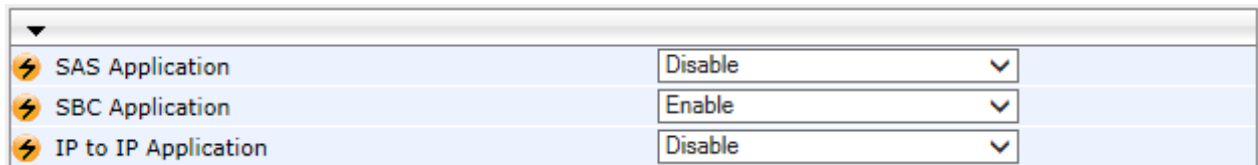
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

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

Figure 4-5: Enabling SBC Application



The screenshot shows a web interface with a table of applications. The table has three rows: 'SAS Application', 'SBC Application', and 'IP to IP Application'. Each row has a status dropdown menu. The 'SBC Application' dropdown is currently set to 'Enable'.

Application	Status
SAS Application	Disable
SBC Application	Enable
IP to IP Application	Disable

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 87).

4.3 Step 3: Signaling Routing Domains Configuration

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

The SRD is composed of the following:

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

4.3.1 Step 3a: Configure Media Realms

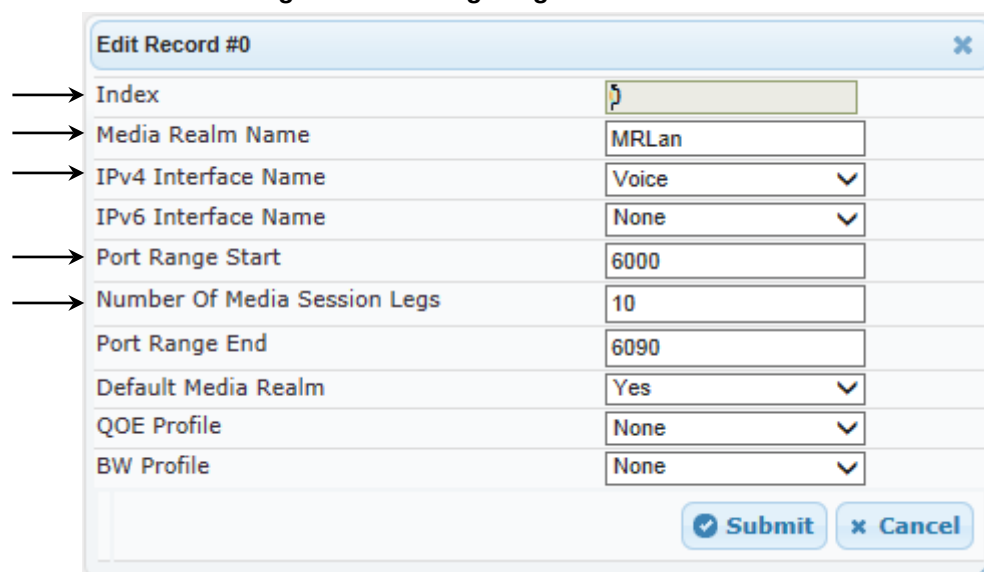
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ **To configure Media Realms:**

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

Parameter	Value
Index	0
Media Realm Name	MRLan (descriptive name)
IPv4 Interface Name	Voice
Port Range Start	6000 (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	10 (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for LAN



→ Index

→ Media Realm Name

→ IPv4 Interface Name

→ IPv6 Interface Name

→ Port Range Start

→ Number Of Media Session Legs

Port Range End

Default Media Realm

QOE Profile

BW Profile

Submit Cancel

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	WANSP
Port Range Start	7000 (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	10 (media sessions assigned with port range)

Figure 4-7: Configuring Media Realm for WAN

The configured Media Realms are shown in the figure below:

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

Media Realm Table			
Add +			
Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	MRLan	Voice	None
1	MRWan	WANSP	None
Page 1 of 1 Show 10 records per page View 1 - 2 of 2			

4.3.2 Step 3b: Configure SRDs

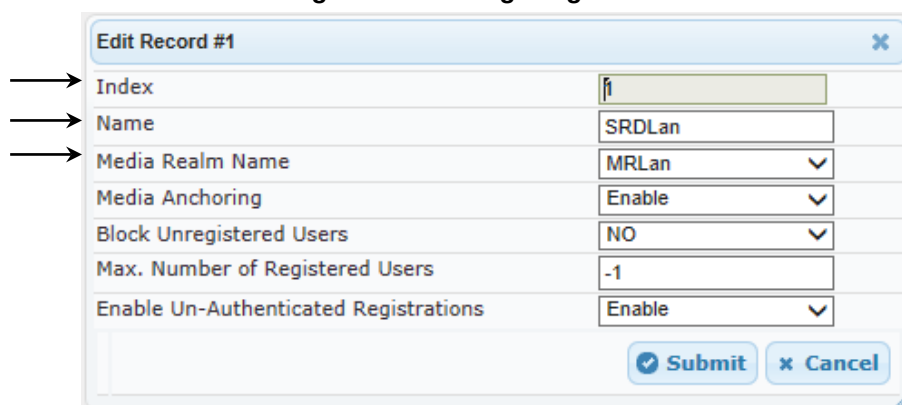
This step describes how to configure the SRDs.

➤ **To configure SRDs:**

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

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

Figure 4-9: Configuring LAN SRD



→ Index: 1

→ Name: SRDLan

→ Media Realm Name: MRLan

Media Anchoring: Enable

Block Unregistered Users: NO

Max. Number of Registered Users: -1

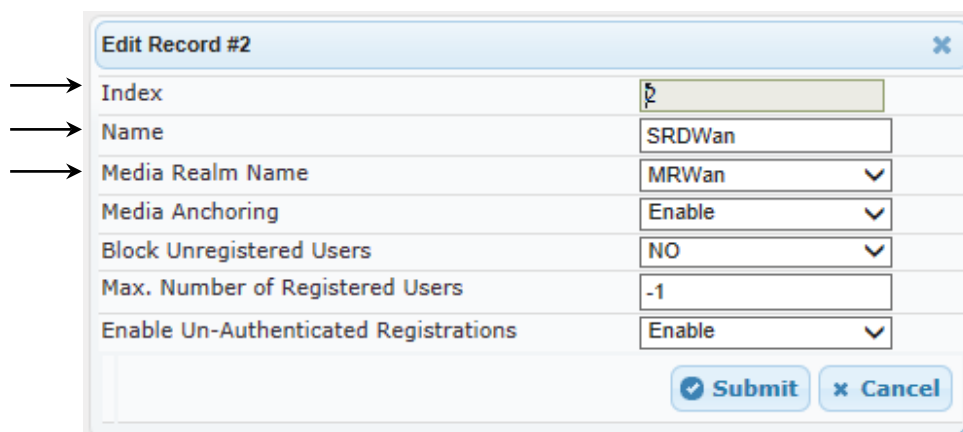
Enable Un-Authenticated Registrations: Enable

Submit Cancel

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

Parameter	Value
Index	2
Name	SRDWan
Media Realm	MRWan

Figure 4-10: Configuring 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

Submit Cancel

4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➤ **To configure SIP Interfaces:**

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

Parameter	Value
Index	1
Interface Name	Lync (arbitrary descriptive name)
Network Interface	Voice
Application Type	SBC
TLS Port	5067
TCP and UDP	0
SRD	1

3. Configure a SIP interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

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

The screenshot shows the 'SIP Interface Table' configuration page. At the top, there is a table with two rows of configured interfaces. Below this, there is a table with columns: Index, SIP Interface Name, Network Interface, Application Type, UDP Port, TCP Port, TLS Port, and SRD. The table contains two rows of data. At the bottom, there is a pagination bar showing 'Page 1 of 1', 'Show 10 records per page', and 'View 1 - 2 of 2'.

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

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

4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Lync Server 2013
- Virgin Media SIP Trunk A
- Virgin Media SIP Trunk B

These Proxy Sets will later be associated with IP Groups.

➤ To configure Proxy Sets:

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

Parameter	Value
Proxy Set ID	1
Proxy Address	FE15.ilync15.local:5067 (Lync Server 2013 IP address / FQDN and destination port)
Transport Type	TLS
Proxy Name	Lync (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	Yes
SRD Index	1

Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013

Proxy Set ID: 1

	Proxy Address	Transport Type
1	FE15.lync15.local:5067	TLS
2		
3		
4		
5		

Proxy Name: Lync

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Round Robin

Is Proxy Hot Swap: Yes

Proxy Redundancy Mode: Not Configured

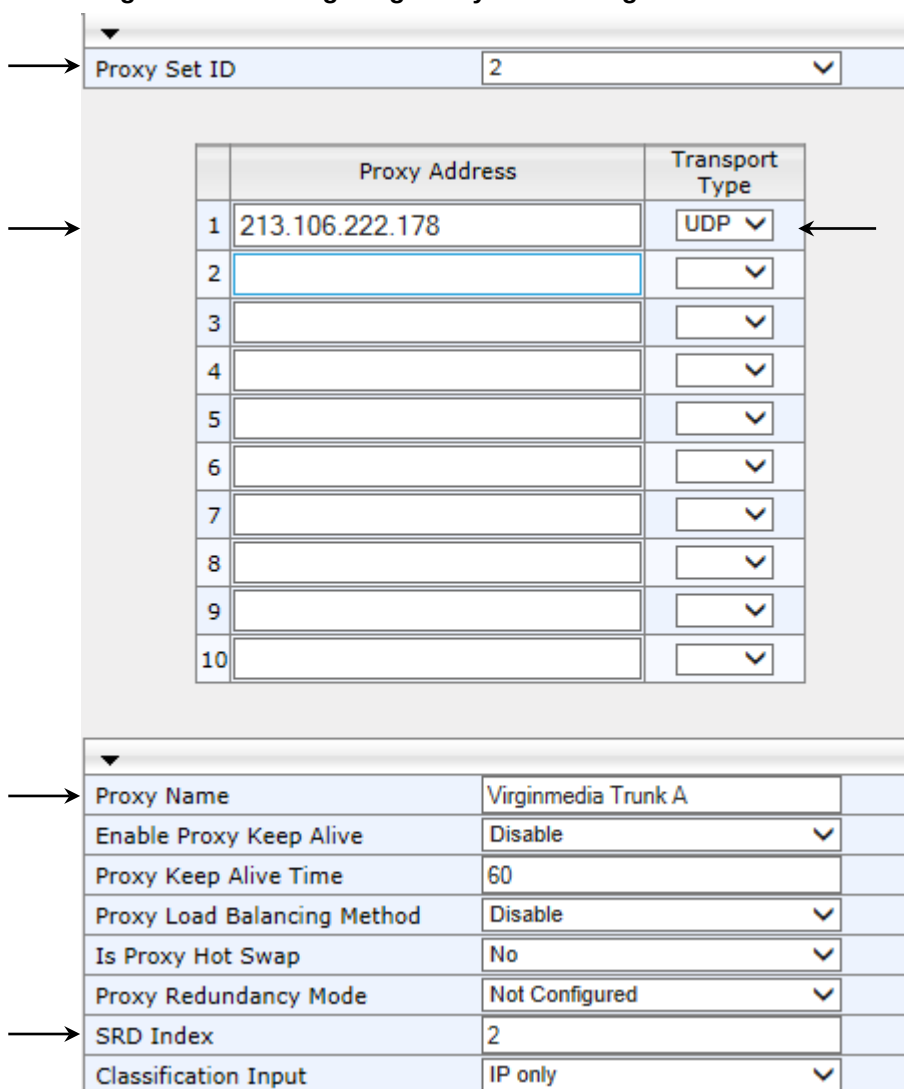
SRD Index: 1

Classification Input: IP only

3. Configure a Proxy Set for the Virgin Media SIP Trunk A:

Parameter	Value
Proxy Set ID	2
Proxy Address	213.106.222.178 (Virgin Media Trunk A IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	Virginmedia Trunk A (arbitrary descriptive name)
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to Virgin Media SIP Trunk)

Figure 4-13: Configuring Proxy Set for Virgin Media SIP Trunk A



The screenshot shows the configuration interface for a Proxy Set. It includes a table for Proxy Address and Transport Type, and a list of configuration parameters.

	Proxy Address	Transport Type
1	213.106.222.178	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Below the table, the following configuration parameters are shown:

- Proxy Set ID: 2
- Proxy Name: Virginmedia Trunk A
- Enable Proxy Keep Alive: Disable
- Proxy Keep Alive Time: 60
- Proxy Load Balancing Method: Disable
- Is Proxy Hot Swap: No
- Proxy Redundancy Mode: Not Configured
- SRD Index: 2
- Classification Input: IP only

4. Configure a Proxy Set for the Virgin Media SIP Trunk B:

Parameter	Value
Proxy Set ID	2
Proxy Address	82.14.171.226 (Virgin Media Trunk B IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	Virginmedia Trunk B (arbitrary descriptive name)
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to Virgin Media SIP Trunk)

Figure 4-14: Configuring Proxy Set for Virgin Media SIP Trunk B

Proxy Set ID: 3

	Proxy Address	Transport Type
1	82.14.171.226	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: Virginmedia Trunk B

Enable Proxy Keep Alive: Disable

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Not Configured

SRD Index: 2

Classification Input: IP only

5. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.15 on page 87).

4.5 Step 5: Configure IP Groups

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

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

- Lync Server 2013 (Mediation Server) located on the LAN
- Virgin Media SIP Trunks A and B located on the WAN

➤ To configure IP Groups:

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

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

3. Configure an IP Group for the Virgin Media SIP Trunk A.

Parameter	Value
Index	2
Type	Server
Description	Virginmedia Trunk A (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	213.106.222.178 (according to ITSP requirement)
SRD	2
Media Realm Name	MRWan
IP Profile ID	2

4. Configure an IP Group for the Virgin Media SIP Trunk B.

Parameter	Value
Index	3
Type	Server
Description	Virginmedia Trunk B (arbitrary descriptive name)
Proxy Set ID	3
SIP Group Name	82.14.171.226 (according to ITSP requirement)
SRD	2
Media Realm Name	MRWan
IP Profile ID	2

The configured IP Groups are shown in the figure below:

Figure 4-15: Configured IP Groups in IP Group Table

▼ IP Group Table								
Add +								
Index	Type	Description	Proxy Set ID	SIP Group Name :	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	Lync	1	213.106.222.178		Not Configured	No	1
2	Server	Virginmedia Trunk A	2	213.106.222.178		Not Configured	No	2
3	Server	Virginmedia Trunk B	3	82.14.171.226		Not Configured	No	2
<< << Page 1 of 1 >> >> Show 10 records per page View 1 - 3 of 3								

4.6 Step 6: Configure IP Profiles

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

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

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

Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 48).

➤ To configure IP Profiles:

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

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

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

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

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

Parameter	Value
Allowed Media Types	audio (required, as Lync Server 2013 does not support media type m=image, which sent by Virgin Media)
SBC Media Security Behavior	SRTP
Remote Update Support	Supported Only After Connect
Remote Re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally (required, as Lync Server 2013 does not support receipt of SIP REFER)
Remote 3xx Behavior	Handle Locally (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
Enforce MKI Size	Enforce
Remote Early Media RTP Behavior	Delayed (required, as Lync Server 2013 does not send RTP immediately to remote side when it sends a SIP 18x response)
Remote Hold Format	Inactive (required, as Lync Server 2013 does not support hold format a=inactive with IP 0.0.0.0, which sent by Virgin Media)
SDP Ptime Answer	Preferred Value
Preferred PTime	20 (required as Lync Server 2013 always sends PTime = 20)

Figure 4-17: Configuring IP Profile for Lync Server 2013 – SBC Tab

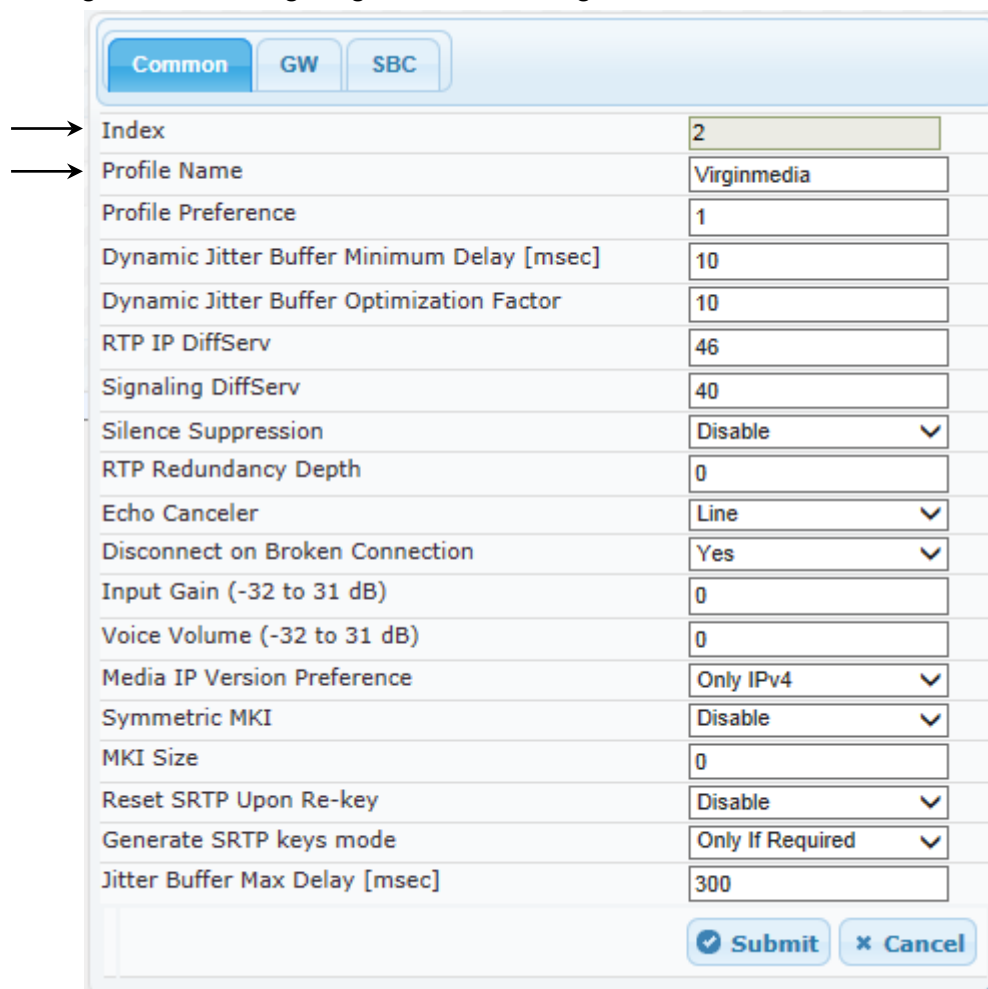
Parameter	Value
Index	1
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	audio
Allowed Coders Group ID	None
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
SBC Media Security Behavior	SRTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
Remote Update Support	Supported Only After
Remote re-INVITE	Supported only with ?
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally
Remote 3xx Behavior	Handle Locally
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
Enforce MKI Size	Enforce
Remote Early Media RTP Behavior	Delayed
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Inactive
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Preferred Value
Preferred PTime	20
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care

Submit Cancel

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

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

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



The screenshot shows the 'Common' tab of the IP Profile configuration window. The 'Index' field is set to 2, and the 'Profile Name' field is set to 'Virginmedia'. Other parameters include Profile Preference (1), Dynamic Jitter Buffer Minimum Delay (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), and Jitter Buffer Max Delay (300). The 'Submit' and 'Cancel' buttons are at the bottom right.

Parameter	Value
Index	2
Profile Name	Virginmedia
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

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

Parameter	Value
Profile ID	2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Restrict and Preference (Re-arranges the order of the coders in the SDP according to their order of appearance in the Allowed Coders Group list)
SBC Media Security Behavior	RTP
P-Asserted-Identity	Add (required for anonymous calls)
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Remote Hold Format	Send Only (required, as Virgin Media work in Send Only mode)
SDP Ptime Answer	Preferred Value
Preferred PTime	10 (required according Virgin Media request)

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

Common GW SBC	
Index	2
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	Coders Group 2
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction and Prefer
SBC Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	Add
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally
Remote 3xx Behavior	Transparent
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
Enforce MKI Size	Don't enforce
Remote Early Media RTP Behavior	Immediate
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Send Only
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Preferred Value
Preferred PTime	10
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care

Submit Cancel

4.7 Step 7: Configure Coders

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Virgin Media SIP Trunks uses only the G.711 coders, where G.711A-law is preferred (proposed first). Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Virgin Media SIP Trunks in the previous step (see Section 4.6 on page 50).

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

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

Parameter	Value
Allowed Coders Group ID	2
Coder Name	G.711A-law
Coder Name	G.711U-law

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

Allowed Audio Coders Group ID: 2

Coder Name
G.711A-law
G.711U-law

4.8 Step 8: SIP TLS Connection Configuration

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

4.8.1 Step 8a: Configure the NTP Server Address

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

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

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

Figure 4-21: Configuring NTP Server Address

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

3. Click **Submit**.

4.8.2 Step 8b: Configure a Certificate

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

The procedure involves the following main steps:

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

➤ **To configure a certificate:**

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

Figure 4-22: Certificates Page - Creating CSR

▼ Certificate Signing Request

Subject Name [CN]

Organizational Unit [OU] (optional)

Company name [O] (optional)

Locality or city name [L] (optional)

State [ST] (optional)

Country code [C] (optional)

Create CSR

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNFQlUdXLMlseW5jMTUubG9jYWwz8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCKxytgT2W1vz0NGUstpa7w2DKKkxr8xA9sGLXwy0ZCyB49U1pDF
DJV8IldUfT8qL9d9V64f3z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAAgADANBgkqhkiG9w0BAQQAFAAOBgQLqe880JGrmEzPu5Q1
pRGiOuEQ4Pr6PL+JKghii6UpLmHEwixTedayzNh7b2yQgFYxiVWmX2JwrvXaCp5Y
8z8hOCZXV/E4MrR2s8bYb6bqxeteAXs+VwxgKObb4pSFfGLc82+dZUcODAB0wZFv
nxSEcPACKnZittF/GgW+A4AoMQ==
-----END CERTIFICATE REQUEST-----
```

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

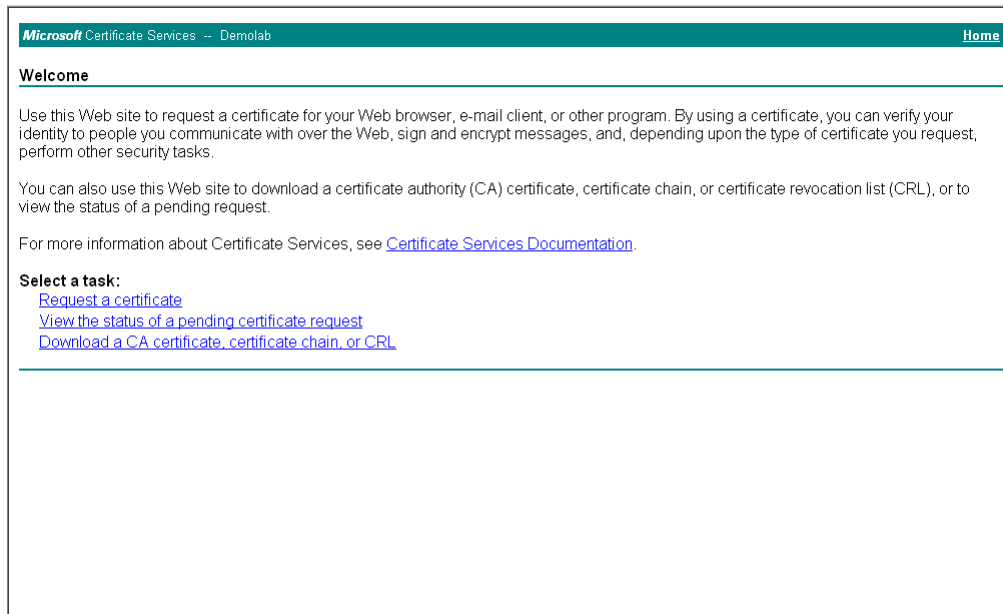


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 15).

- Click **Create CSR**; a certificate request is generated.
- Copy the CSR from the line "**-----BEGIN CERTIFICATE**" to "**END CERTIFICATE REQUEST-----**" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.

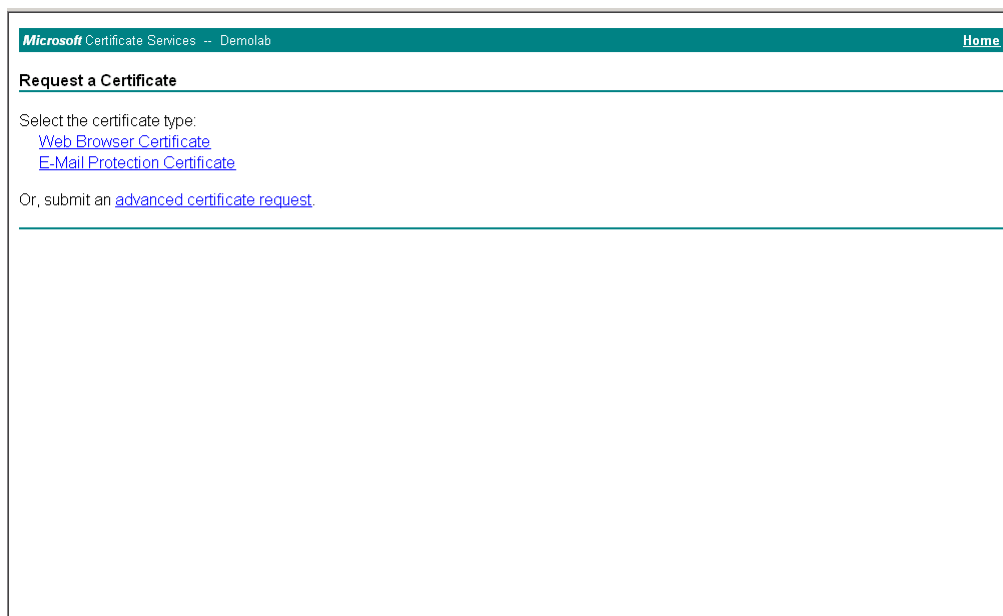
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-23: Microsoft Certificate Services Web Page



6. Click **Request a certificate**.

Figure 4-24: Request a Certificate Page



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

Figure 4-25: Advanced Certificate Request Page

The screenshot shows the 'Advanced Certificate Request' page. At the top, there is a breadcrumb trail: 'Microsoft Certificate Services -- Demolab' and a 'Home' link. The page title is 'Advanced Certificate Request'. Below the title, a message states: 'The policy of the CA determines the types of certificates you can request. Click one of the following options to:'. There are three links: 'Create and submit a request to this CA.', 'Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.', and a third link that is partially obscured. The page is mostly blank below the links.

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

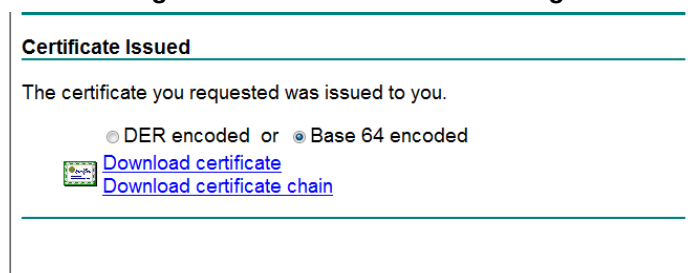
Figure 4-26: Submit a Certificate Request or Renewal Request Page

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page. At the top, there is a breadcrumb trail: 'Microsoft Active Directory Certificate Services -- Lync-DC-LYNC-CA' and a 'Home' link. The page title is 'Submit a Certificate Request or Renewal Request'. Below the title, a message states: 'To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.' There are three sections: 'Saved Request:' with a text area containing a base-64-encoded request; 'Certificate Template:' with a dropdown menu set to 'Web Server'; and 'Additional Attributes:' with a text area. At the bottom right, there is a 'Submit >' button.

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

11. Click **Submit**.

Figure 4-27: Certificate Issued Page



Certificate Issued

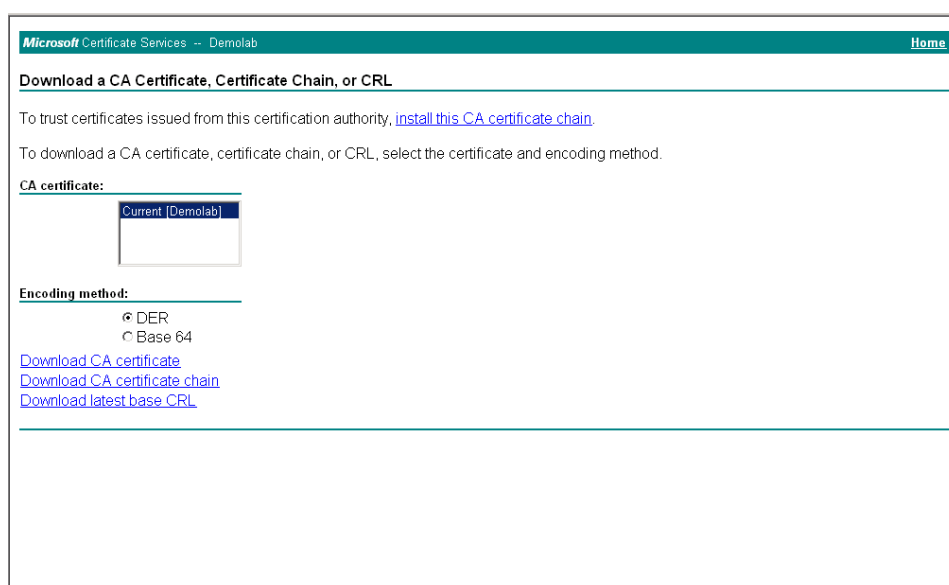
The certificate you requested was issued to you.

☐ DER encoded or
 ☒ Base 64 encoded


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

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

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



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

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Encoding method:

☒ DER
☐ Base 64

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

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

19. In the E-SBC's Web interface, return to the Certificates page and do the following:
 - a. In the 'Device Certificate' field, click **Browse** and select the *gateway.cer* certificate file that you saved on your computer in Step 13, and then click **Send File** to upload the certificate to the E-SBC.
 - b. In the 'Trusted Root Certificate Store' field, click **Browse** and select the *certroot.cer* certificate file that you saved on your computer in Step 18, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-29: Certificates Page (Uploading Certificate)

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

- Private key pass-phrase (optional):** A text input field with the value "audc".
- Send Private Key file from your computer to the device:** A message stating "The file must be in either PEM or PFX (PKCS#12) format." Below this is a text input field, a "Browse..." button, and a "Send File" button.
- Note:** A bold note stating "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:** A message stating "The file must be in textual PEM format." Below this is a text input field, a "Browse..." button, and a "Send File" button.
- Send "Trusted Root Certificate Store" file from your computer to the device:** A message stating "The file must be in textual PEM format." Below this is a text input field, a "Browse..." button, and a "Send File" button.

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 87).

4.9 Step 9: Configure SRTP

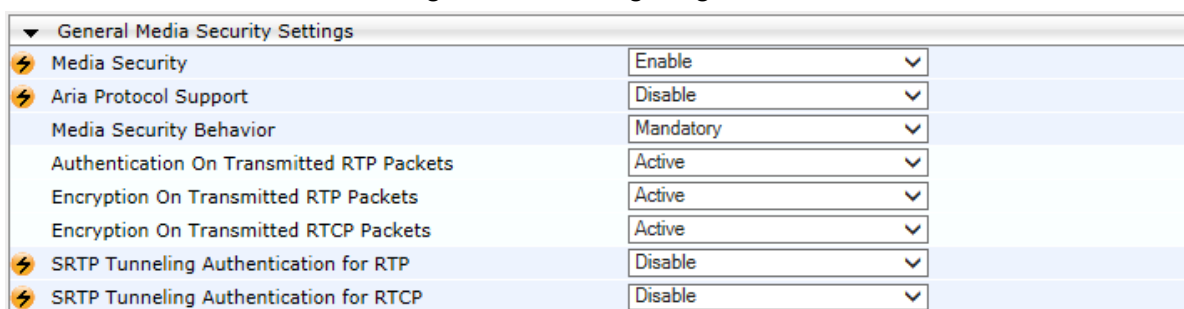
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 50).

➤ **To configure media security:**

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

Parameter	Value
Media Security	Enable

Figure 4-30: Configuring SRTP



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

3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 87).

4.10 Step 10: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 48, IP Group 1 represents Lync Server 2013, IP Group 2 represents Virgin Media SIP Trunk A and IP Group 3 represents Virgin Media SIP Trunk B.

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 Virgin Media SIP Trunk (WAN):

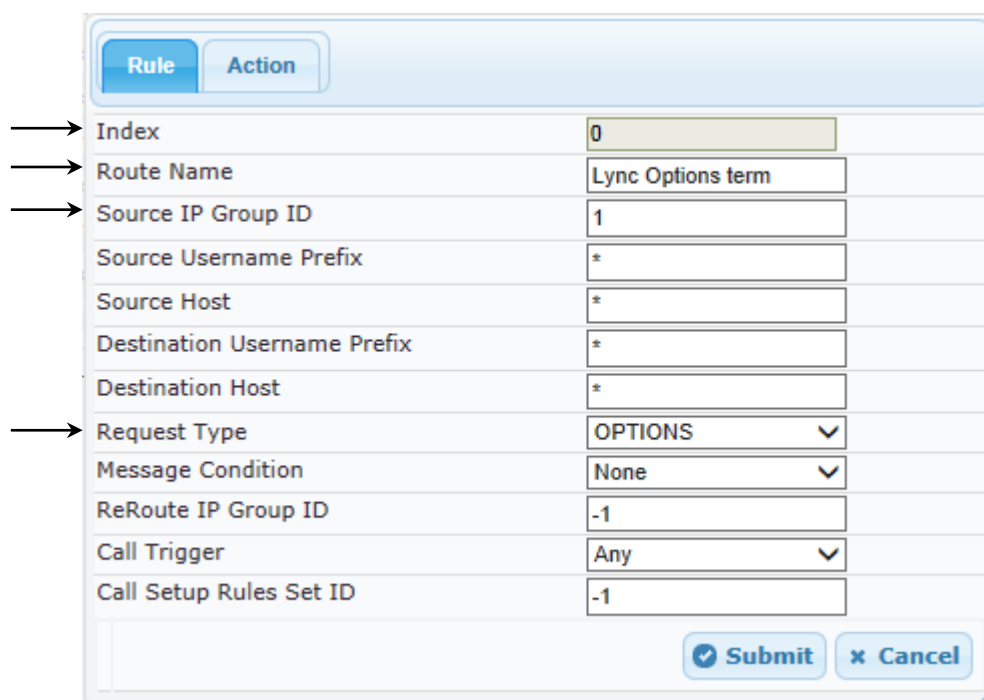
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Reroute SIP OPTIONS messages, received from Virgin Media SIP Trunk A back to SIP Trunk A
- Reroute SIP OPTIONS messages, received from Virgin Media SIP Trunk B back to SIP Trunk B
- Calls from Lync Server 2013 to Virgin Media SIP Trunk A
- Calls from Virgin Media SIP Trunk A to Lync Server 2013
- Calls from Lync Server 2013 to Virgin Media SIP Trunk B
- Calls from Virgin Media SIP Trunk B 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	Lync Options term (arbitrary descriptive name)
Source IP Group ID	1
Request Type	OPTIONS

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



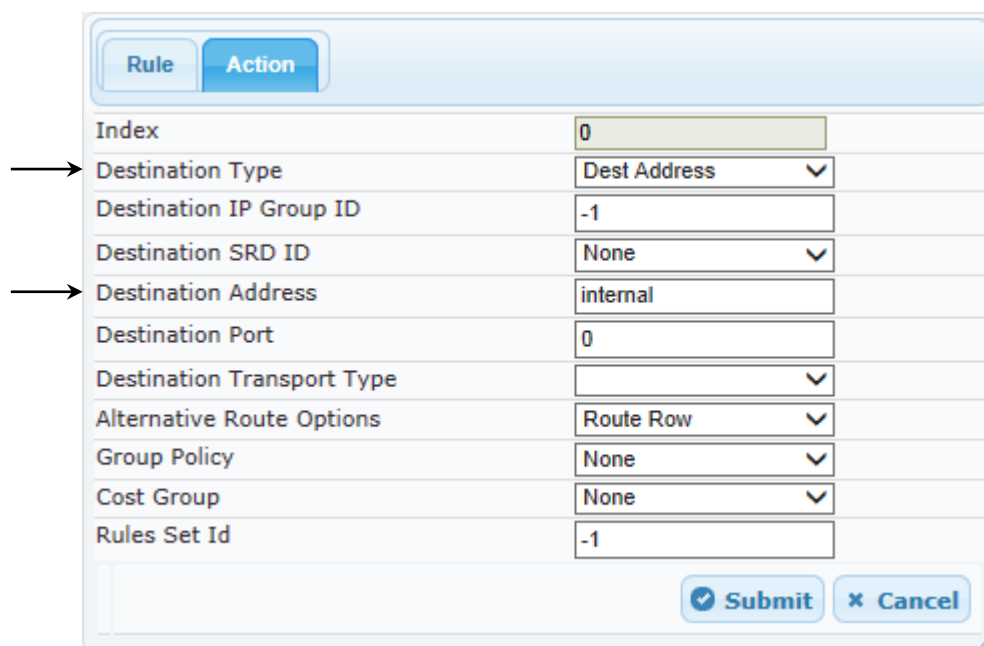
Rule	
Index	0
Route Name	Lync Options term
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

Submit Cancel

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-32: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



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

Submit Cancel

6. Configure a rule to reroute SIP OPTIONS messages, received from Virgin Media SIP Trunk A back to SIP Trunk A:
7. Click **Add**.
8. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	Trunk A Options term (arbitrary descriptive name)
Source IP Group ID	2
Request Type	OPTIONS

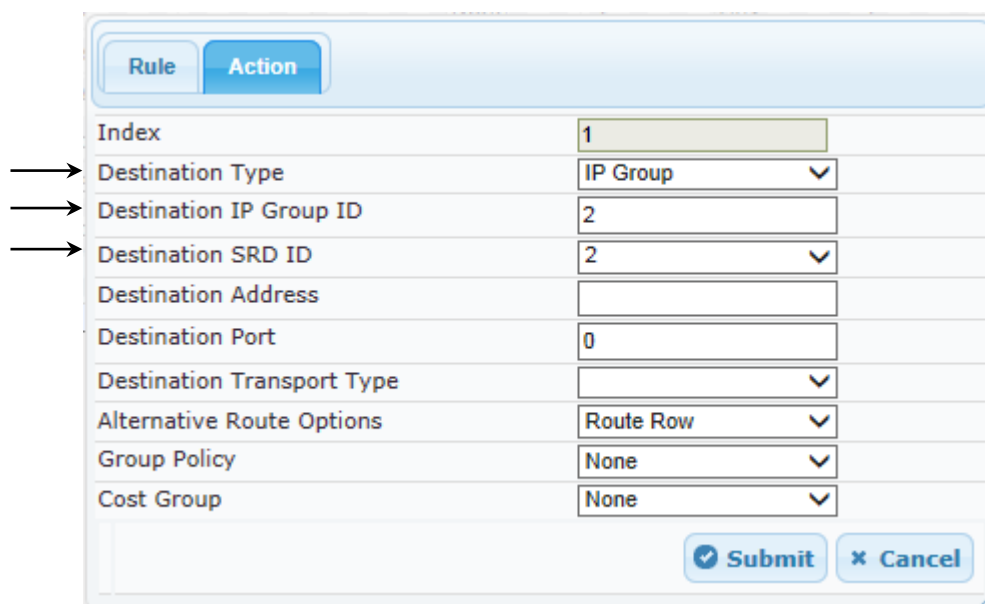
Figure 4-33: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk A – Rule Tab

Rule	
Index	1
Route Name	Trunk A Options term
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

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 4-34: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk A – Action Tab



Parameter	Value
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

Submit Cancel

10. Configure a rule to reroute SIP OPTIONS messages, received from Virgin Media SIP Trunk B back to SIP Trunk A:
11. Click **Add**.
12. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	Trunk B Options term (arbitrary descriptive name)
Source IP Group ID	3
Request Type	OPTIONS

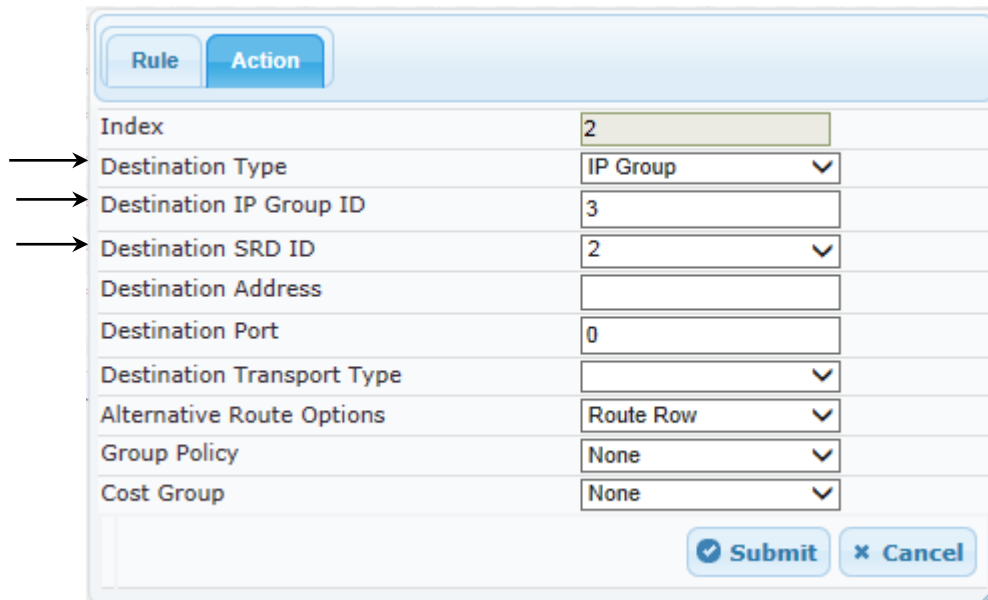
Figure 4-35: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk B – Rule Tab

	Rule	Action
→	Index	2
→	Route Name	Trunk B Options term
→	Source IP Group ID	3
	Source Username Prefix	*
	Source Host	*
	Destination Username Prefix	*
	Destination Host	*
→	Request Type	OPTIONS
	Message Condition	None
	ReRoute IP Group ID	-1
	Call Trigger	Any
	Call Setup Rules Set ID	-1
	☒ Submit ☐ Cancel	

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	3
Destination SRD ID	3

Figure 4-36: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from Virgin Media Trunk B – Action Tab



Rule Action

Index 2

Destination Type IP Group

Destination IP Group ID 3

Destination SRD ID 2

Destination Address

Destination Port 0

Destination Transport Type

Alternative Route Options Route Row

Group Policy None

Cost Group None

Submit Cancel

14. Configure a rule to route calls from Lync Server 2013 to Virgin Media SIP Trunk A:
15. Click **Add**.
16. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	3
Route Name	Lync to Trunk A (arbitrary descriptive name)
Source IP Group ID	1

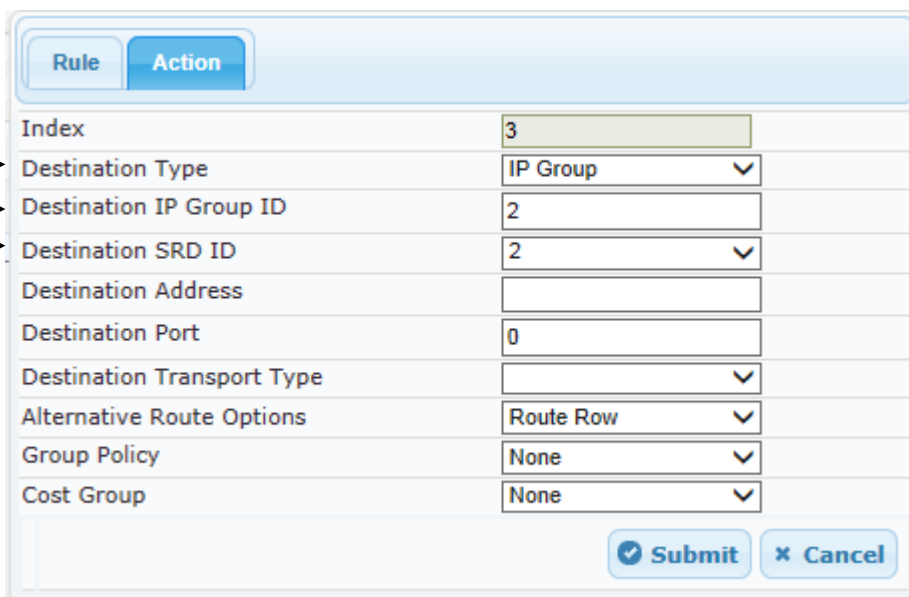
Figure 4-37: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk A – Rule tab

Rule	
Index	3
Route Name	Lync to Trunk A
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
Call Setup Rules Set ID	-1

17. 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 4-38: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk A – Action tab



Rule Action

Index 3

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

Submit Cancel

18. Configure a rule to route calls from Virgin Media SIP Trunk A to Lync Server 2013:
19. Click **Add**.

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

Parameter	Value
Index	4
Route Name	Trunk A to Lync (arbitrary descriptive name)
Source IP Group ID	2

Figure 4-39: Configuring IP-to-IP Routing Rule for Virgin Media Trunk A to Lync – Rule tab

The screenshot shows the 'Rule' tab of the configuration interface. The 'Rule' tab is selected, and the 'Action' tab is also visible. The form contains the following fields and values:

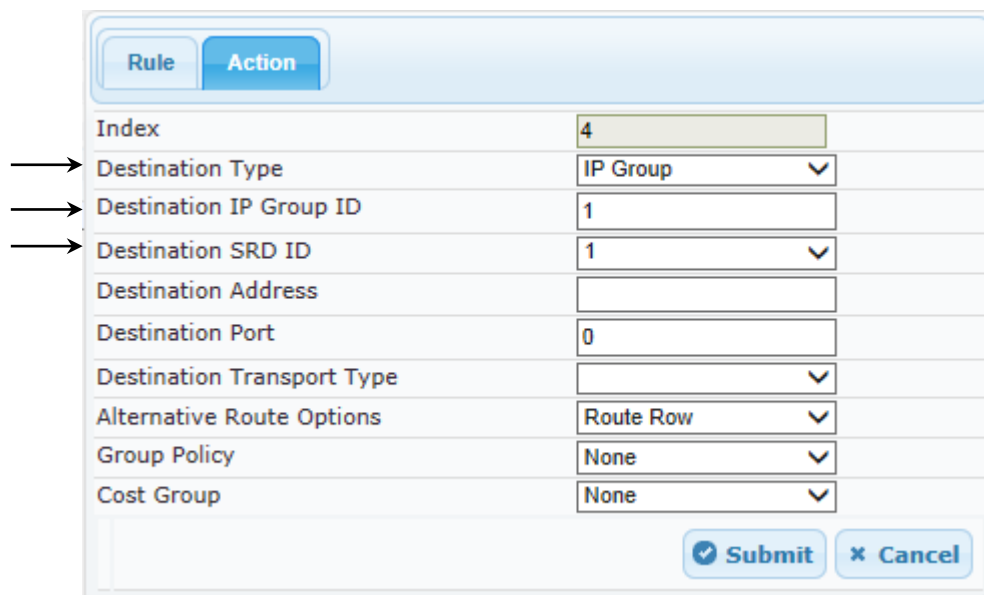
Index	4
Route Name	Trunk A to Lync
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

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

21. 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 4-40: Configuring IP-to-IP Routing Rule for Virgin Media Trunk A to Lync – Action tab



Rule	
Action	
Index	4
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

Submit Cancel

22. Configure a rule to route calls from Lync Server 2013 to Virgin Media SIP Trunk B:
23. Click **Add**.

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

Parameter	Value
Index	5
Route Name	Lync to Trunk B (arbitrary descriptive name)
Source IP Group ID	1

Figure 4-41: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk B – Rule tab

The screenshot shows a configuration window with two tabs: 'Rule' (selected) and 'Action'. The 'Rule' tab contains a list of parameters and their values. Three arrows on the left point to the 'Index', 'Route Name', and 'Source IP Group ID' fields. The 'Submit' button is highlighted with a checkmark icon.

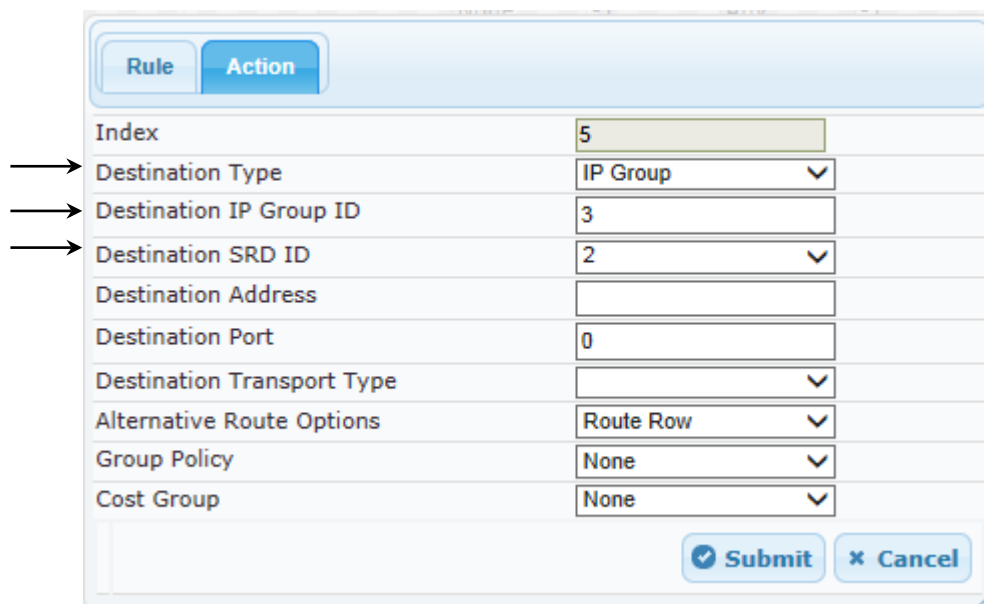
Parameter	Value
Index	5
Route Name	Lync to Trunk B
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

Submit Cancel

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	3
Destination SRD ID	2

Figure 4-42: Configuring IP-to-IP Routing Rule for Lync to Virgin Media Trunk B – Action tab



Parameter	Value
Index	5
Destination Type	IP Group
Destination IP Group ID	3
Destination SRD ID	2
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None

26. Configure a rule to route calls from Virgin Media SIP Trunk B to Lync Server 2013:
 27. Click **Add**.

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

Parameter	Value
Index	6
Route Name	Trunk B to Lync (arbitrary descriptive name)
Source IP Group ID	3

Figure 4-43: Configuring IP-to-IP Routing Rule for Virgin Media Trunk B to Lync – Rule tab

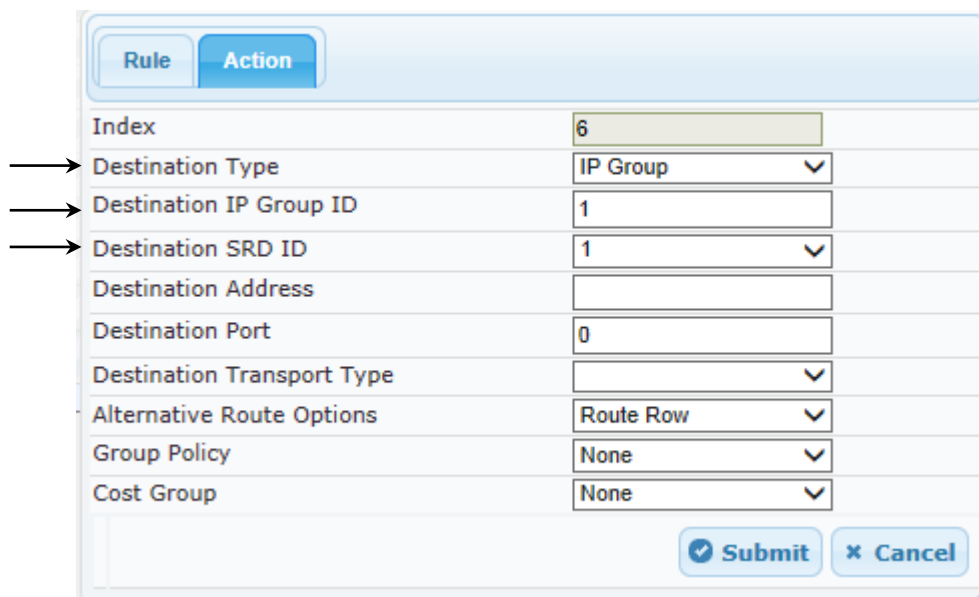
The screenshot shows the 'Rule' tab of the configuration interface. It contains a table of parameters and their values. Four arrows point to the 'Route Name', 'Source IP Group ID', 'Source Username Prefix', and 'Destination Username Prefix' fields. The 'Submit' button is highlighted with a checkmark.

Rule	
Index	6
Route Name	Trunk B to Lync
Source IP Group ID	3
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

29. 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 4-44: Configuring IP-to-IP Routing Rule for Virgin Media Trunk B to Lync – Action tab



The configured routing rules are shown in the figure below:

Figure 4-45: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table										
Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination SRD ID
0	Lync Options ter	*	*	*	None	-1	Any	-1	Dest Address	None
1	Trunk A Options	*	*	*	None	-1	Any	-1	IP Group	2
2	Trunk B Options	*	*	*	None	-1	Any	-1	IP Group	2
3	Lync to Trunk A	*	*	*	None	-1	Any	-1	IP Group	2
4	Trunk A to Lync	*	*	*	None	-1	Any	-1	IP Group	1
5	Lync to Trunk B	*	*	*	None	-1	Any	-1	IP Group	2
6	Trunk B to Lync	*	*	*	None	-1	Any	-1	IP Group	1



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

4.11 Step 11: 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 48, IP Group 1 represents Lync Server 2013, IP Group 2 represents Virgin Media SIP Trunk A and IP Group 3 represents Virgin Media SIP Trunk B.



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 (Virgin Media SIP Trunk A) or IP Group 3 (Virgin Media SIP Trunk B) 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 4-46: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

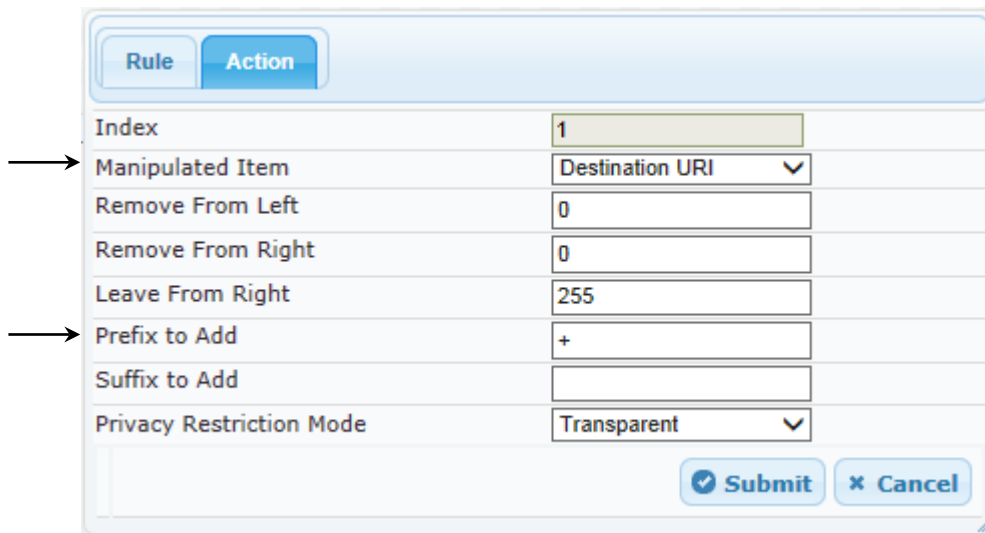
Rule	
Index	1
Manipulation Name	
Additional Manipulation	No
Source IP Group ID	2
Destination IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Calling Name Prefix	*
Message Condition	None
Request Type	All
ReRoute IP Group ID	-1
Call Trigger	Any

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 4-47: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

Figure 4-48: 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 URI	+	
2		No	1	2	+	*	*	*	All	Source URI		
3		No	3	1	*	*	*	*	All	Destination URI	+	
4		No	1	3	+	*	*	*	All	Source URI		

Page 1 of 1 Show 10 records per page View 1 - 4 of 4

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

4.12 Step 12: Configure Message Manipulation Rules

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

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

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for Virgin Media SIP Trunk A. This rule is applied to response messages sent to the Virgin Media SIP Trunk A (IP Group 2) or Trunk B (IP Group 3) and consist method type '410 Gone'. This replaces the method type '410' with the value '480', according to Virgin Media request.

Parameter	Value
Index	0
Manipulation Set ID	4
Message Type	any.response
Condition	header.request-uri.methodtype=='410'
Action Subject	header.request-uri.methodtype
Action Type	Modify
Action Value	'480'
Row Role	Use Current Condition

Figure 4-49: Configuring SIP Message Manipulation Rule 1 (for Virgin Media SIP Trunk A)

→ Index: 0

Manipulation Name:

→ Manipulation Set ID: 4

→ Message Type: any.response

→ Condition: header.request-uri.methoc

→ Action Subject: header.request-uri.methoc

→ Action Type: Modify

→ Action Value: '480'

→ Row Role: Use Current Condior

Submit Cancel

Figure 4-50: Example of Configured SIP Message Manipulation Rule

Message Manipulations							
Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0		4	any.response	header.request-uri.meth	header.request-uri.m	Modify	'480'

The table displayed below includes SIP message manipulation rule which is bound together by commonality via the Manipulation Set ID 4 which is executed for messages sent to and from the Virgin Media SIP Trunks (IP Groups 2 and 3). This rule is specifically required to enable proper interworking between Virgin Media SIP Trunk and Lync Server 2013. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule is applied to response messages sent to the Virgin Media SIP Trunk A (IP Group 2) or Trunk B (IP Group 3) and consist method type '410 Gone'. This replaces the method type '410' with the value '480'.	Virgin Media request to change '410' method type to '480'.

3. Assign Manipulation Set ID 4 to IP Group 2:
 - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
 - b. Select the row of IP Group 2, and then click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Outbound Message Manipulation Set' field to 4.

Figure 4-51: Assigning Manipulation Set to IP Group 2

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

- e. Click **Submit**.

4. Assign Manipulation Set ID 4 to IP Group 3:
 - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
 - b. Select the row of IP Group 3, and then click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-52: Assigning Manipulation Set 4 to IP Group 3

The screenshot shows the 'SBC' configuration tab for IP Group 3. The 'Index' field is set to 3. The 'Classify By Proxy Set' dropdown is set to 'Enable'. The 'Max. Number of Registered Users' field is set to -1. The 'Inbound Message Manipulation Set' field is set to -1. The 'Outbound Message Manipulation Set' field is set to 4. The 'Registration Mode' dropdown is set to 'User Initiates Registrat'. The 'Authentication Mode' dropdown is set to 'User Authenticates'. The 'Authentication Method List' field is empty. The 'SBC Client Forking Mode' dropdown is set to 'Sequential'. The 'Source URI Input' dropdown is set to 'Not Configured'. The 'Destination URI Input' dropdown is set to 'Not Configured'. The 'Username' and 'Password' fields are empty. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Common	GW	SBC
Index	3	
Classify By Proxy Set	Enable	
Max. Number of Registered Users	-1	
Inbound Message Manipulation Set	-1	
Outbound Message Manipulation Set	4	
Registration Mode	User Initiates Registrat	
Authentication Mode	User Authenticates	
Authentication Method List		
SBC Client Forking Mode	Sequential	
Source URI Input	Not Configured	
Destination URI Input	Not Configured	
Username		
Password		
		Submit Cancel

- e. Click **Submit**.

4.13 Step 13: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the Virgin Media SIP Trunk on behalf of Lync Server 2013. The Virgin Media SIP Trunk doesn't require registration but does require authentication to provide service.

In the interoperability test topology, the Served IP Group is Lync Server 2013 (IP Group 1) and the Serving IP Groups are Virgin Media SIP Trunk A (IP Group 2) and Virgin Media SIP Trunk B (IP Group 3).

➤ **To configure a registration accounts:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Enter an index number ("0" for Virgin Media Trunk A), and then click **Add**.
3. Configure the account according to the provided information from Virgin Media, for example:

Parameter	Value
Served IP Group	1 (Lync Server 2013)
Serving IP Group	2 (Virgin Media SIP Trunk A)
Username	As provided by Virgin Media
Password	As provided by Virgin Media
Register	No
Application Type	SBC

4. Click **Apply**.
5. Repeat for Virgin Media Trunk B:

Parameter	Value
Served IP Group	1 (Lync Server 2013)
Serving IP Group	3 (Virgin Media SIP Trunk B)
Username	As provided by Virgin Media
Password	As provided by Virgin Media
Register	No
Application Type	SBC

6. Click **Apply**; the following screen appears:

Figure 4-53: Configuring SIP Registration Accounts

Account Table									
Add +									
Index	Served Trunk Group	Served IP Group	Serving IP Group	User Name	Password	Host Name	Register	Contact User	Application Type
0	-1	1	2	virginpbx01_*			No		SBC
1	-1	1	3	virginpbx01_*			No		SBC

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

7. Confirm that the 'Cnonce' field contains the default value of **Default_Cnonce**, by opening the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).

Figure 4-54: Proxy & Registration

Proxy & Registration	
Use Default Proxy	No
Proxy Name	
Redundancy Mode	Parking
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Always Use Proxy	Disable
Redundant Routing Mode	Routing Table
SIP ReRouting Mode	Standard Mode
Gateway Name	
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Subscription Mode	Per Endpoint
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd
Cnonce	Default_Cnonce

4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

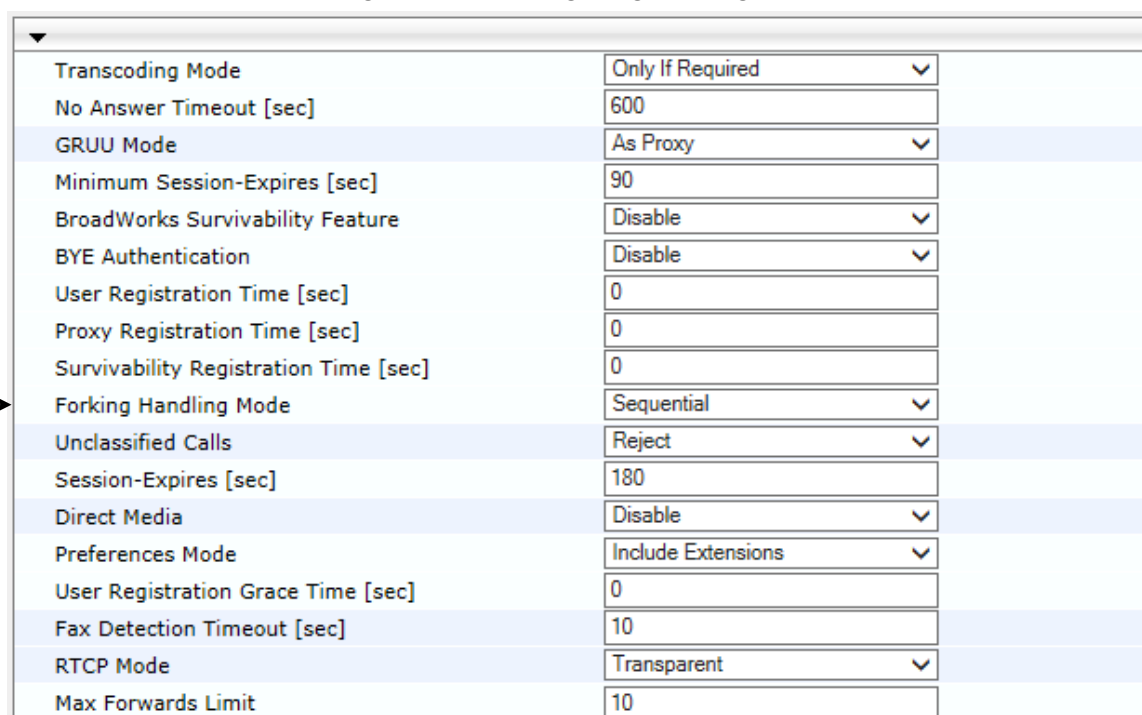
4.14.1 Step 14a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if 180 response without SDP is received. It's mandatory to set this field for the Lync Server 2013 environment.

➤ **To configure call forking:**

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

Figure 4-55: Configuring Forking Mode



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

3. Click **Submit**.

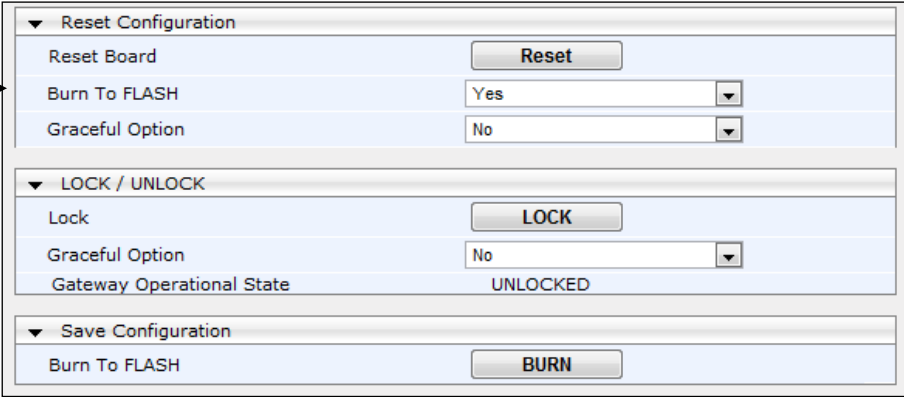
4.15 Step 15: Reset the E-SBC

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

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

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

Figure 4-56: Resetting the E-SBC



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

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

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

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 33, is shown below:



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

```

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 2265355
;Slot Number: 1
;Software Version: 6.80A.009.005
;DSP Software Version: 5014AE3_R => 680.22
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M  Flash size: 64M  Core speed: 300Mhz
;Num of DSP Cores: 3  Num DSP Channels: 62
;Num of physical LAN ports: 12
;Profile: NONE
;Key features;;Board Type: 72 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;System features: POE-
AF ;DSP Voice features: Ipmdetector RTCP-XR AMRPolicyManagement ;Coders:
G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B
AMR-WB G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB
;QOE features: VoiceQualityMonitoring MediaEnhancement ;Channel Type: RTP
DspCh=62 IPMediaDspCh=62 ;PSTN FALLBACK Supported ;E1Trunks=2 ;T1Trunks=2
;FXSPorts=4 ;FXOPorts=4 ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;Control Protocols: MGCP MEGACO H323 SIP TPNC
SASurvivability SBC=60 MSFT CLI TRANSCODING=60 FEU=60 TestCall=60
SIPRec=60 CODER-TRANSCODING=60 EMS SBC-SIGNALING=60 SBC-MEDIA=60 ;Default
features;;Coders: G711 G726;

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

[SYSTEM Params]

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

```

```
NTPServerIP = '10.15.25.1'
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
```

[BSP Params]

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

[Analog Params]

```
FarEndDisconnectType = 7
```

[ControlProtocols Params]

```
AdminStateLockControl = 0
```

[MGCP Params]

[MEGACO Params]

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

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

```
BrokenConnectionEventTimeout = 100000
ENABLEMEDIASEcurity = 1
CallProgressTonesFilename = 'usa_tones_13.dat'
```

[WEB Params]

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

[SIP Params]

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

```
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SCTP Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 1, 4, "User Port #11", "GROUP_6",
"Redundant";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 2, "FE_5_1", "FE_5_2";
EtherGroupTable 3 = "GROUP_4", 2, "FE_5_3", "FE_5_4";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
```

```
[ \EtherGroupTable ]

[ DeviceTable ]

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

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

;
; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 10, 6090, 1, "", "";
CpMediaRealm 1 = "MRWan", "WANSP", "", 7000, 10, 7090, 0, "", "";

[ \CpMediaRealm ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
```

```
SRD 1 = "SRDLan", "MRLan", 0, 0, -1, 1;
SRD 2 = "SRDWan", "MRWan", 0, 0, -1, 1;

[ \SRD ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 1 = "213.106.222.178", 0, 2;
ProxyIp 2 = "82.14.171.226", 0, 3;

[ \ProxyIp ]

[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOffersSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPptimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;
```

```

IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "audio", -1, -1, 0,
1, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1, 0, 3, 2, 1,
0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 3, 0, 2, 20, 0, 0, 0,
0, 0, 0, 300;

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

[ \IpProfile ]

[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode,
ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, -1, -1, "";
ProxySet 1 = "Lync", 1, 60, 1, 1, 1, 0, 1, -1, "";
ProxySet 2 = "Virginmedia Trunk A", 0, 60, 0, 0, 2, 0, -1, -1, "";
ProxySet 3 = "Virginmedia Trunk B", 0, 60, 0, 0, 2, 0, -1, -1, "";

[ \ProxySet ]

[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "Lync", 1, "213.106.222.178", "", 0, -1, -1, 0, -1, 1,
"MRlan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "",
"", "", 0, "", "";
IPGroup 2 = 0, "Virginmedia Trunk A", 2, "213.106.222.178", "", 0, -1, -
1, 0, -1, 2, "MRwan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", "", 0, "", "";
IPGroup 3 = 0, "Virginmedia Trunk B", 3, "82.14.171.226", "", 0, -1, -1,
0, -1, 2, "MRwan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", "", 0, "", "";

[ \IPGroup ]

[ Account ]

```

```

FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup,
Account_ServingIPGroup, Account_Username, Account_Password,
Account_HostName, Account_Register, Account_ContactUser,
Account_ApplicationType;
Account 0 = -1, 1, 2, "virginpbx01_01183374130",
"$1$IxcXFBMeHhAfbhRvHRd2dXF3AHFz", "", 0, "", 2;
Account 1 = -1, 1, 3, "virginpbx01_01183374130",
"$1$IxcXFBMeHhAfbhRvHRd2dXF3AHFz", "", 0, "", 2;

[ \Account ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "Lync Options term", 1, "", "", "", "", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "Trunk A Options term", 2, "", "", "", "", 6, "", -
1, 0, -1, 0, 2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "Trunk B Options term", 3, "", "", "", "", 6, "", -
1, 0, -1, 0, 3, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 3 = "Lync to Trunk A", 1, "", "", "", "", 0, "", -1, 0,
-1, 0, 2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 4 = "Trunk A to Lync", 2, "", "", "", "", 0, "", -1, 0,
-1, 0, 1, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 5 = "Lync to Trunk B", 1, "", "", "", "", 0, "", -1, 0,
-1, 0, 3, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 6 = "Trunk B to Lync", 3, "", "", "", "", 0, "", -1, 0,
-1, 0, 1, "1", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ SIPInterface ]

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

[ \SIPInterface ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,

```

```

IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 1 = "", 0, 2, 1, "*", "*", "*", "*", "*", "", 0, -
1, 0, 1, 0, 0, 255, "+", "", 0;
IPOutboundManipulation 2 = "", 0, 1, 2, "+", "*", "*", "*", "*", "", 0, -
1, 0, 0, 1, 0, 255, "", "", 0;
IPOutboundManipulation 3 = "", 0, 3, 1, "*", "*", "*", "*", "*", "", 0, -
1, 0, 1, 0, 0, 255, "+", "", 0;
IPOutboundManipulation 4 = "", 0, 1, 3, "+", "*", "*", "*", "*", "", 0, -
1, 0, 0, 1, 0, 255, "", "", 0;

[ \IPOutboundManipulation ]

[ AllowedCodersGroup2 ]

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

[ \AllowedCodersGroup2 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "", 4, "any.response", "header.request-
uri.methodtype=='410'", "header.request-uri.methodtype", 2, "'480'", 0;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]

[ ResourcePriorityNetworkDomains ]

```

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



Configuration Note