

Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

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



Microsoft Partner
Gold Communications



July 2014

Document #: LTRT-31906

Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	Verizon SIP Trunking Version.....	9
2.3	Microsoft Lync Server 2013 Version	9
2.4	AudioCodes Gateway Version	10
2.5	Interoperability Test Topology	10
2.5.1	Environment Setup	11
2.5.2	Known Limitations.....	11
3	Configuring Lync Server 2013	13
3.1	Configuring the E-SBC as an IP / PSTN Gateway	13
3.2	Configuring the "Route" on Lync Server 2013.....	21
4	Configuring AudioCodes E-SBC.....	31
4.1	Step 1: Configure IP Network Interfaces	32
4.1.1	Step 1a: Configure VLANs.....	33
4.1.2	Step 1b: Configure Network Interfaces.....	33
4.1.3	Step 1c: Configure the Native VLAN ID.....	35
4.2	Step 2: Enable the SBC Application	36
4.3	Step 3: Configure SRDs	37
4.3.1	Step 3a: Configure Media Realms.....	37
4.3.2	Step 3b: Configure SRDs	39
4.3.3	Step 3c: Configure SIP Signaling Interfaces	40
4.4	Step 4: Configure Proxy Sets	41
4.5	Step 5: Configure IP Groups.....	43
4.6	Step 6: Configure IP Profiles	45
4.7	Step 7: Configure Coders	53
4.8	Step 8: Configure a SIP TLS Connection.....	56
4.8.1	Step 8a: Configure the NTP Server Address.....	56
4.8.2	Step 8b: Configure a Certificate	57
4.9	Step 9: Configure SRTP	62
4.10	Step 10: Configure Maximum IP Media Channels	63
4.11	Step 11: Configure IP-to-IP Call Routing Rules	64
4.12	Step 12: Configure IP-to-IP Manipulation Rules.....	74
4.13	Step 13: Configure Message Manipulation Rules	82
4.14	Step 14: Configure Miscellaneous E-SBC Settings.....	97
4.14.1	Step 14a: Configure Call Forking Mode	97
4.15	Step 15: Reset the E-SBC	98
A	AudioCodes <i>ini</i> File.....	99
B	Configuring Analog Devices (ATAs) for Fax Support.....	107
B.1	Step 1: Configure the Endpoint Phone Number Table	107
B.2	Step 2: Configure the Tel to IP Routing Table.....	108

B.3	Step 3: Configure the Coders Table	109
B.4	Step 4: Configure SIP UDP Transport Type and Fax Signaling Method.....	110
B.5	Step 5: Configure FAX Settings.....	110

Notice

This document describes how to connect the Microsoft Lync Server 2013 and Verizon SIP Trunk using AudioCodes Mediant E-SBC product series.

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

© Copyright 2014 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: July-18-2014

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, 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.

Documentation Feedback

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

Reader's Notes

1 Introduction

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

1.1 Intended Audience

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

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none"> ▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 E-SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (Server Edition and Virtual Edition)
Software Version	SIP_6.80A.018.005
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the Verizon SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	<p>Fax is supported by analog devices (ATAs). FXS ports on devices that support FXS ports can also be used.</p> <p>Mediant 9000 SBC and Mediant Software SBC can be utilized if no transcoding is required for the deployment.</p>

2.2 Verizon SIP Trunking Version

Table 2-2: Verizon Version

Vendor/Service Provider	Verizon
SSW Model/Service	-
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 AudioCodes Gateway Version

Table 2-4: AudioCodes Gateway Version

Gateway Vendor	AudioCodes
Model	AudioCodes MP-11x series.
Software Version	SIP_6.60A.270.010
Interface Type	SIP/IP
VoIP Protocol	SIP
Additional Notes	Fax is supported by analog devices (ATAs). FXS ports on devices that support FXS ports can also be used. CNG detection enabled to support interwork with Verizon SIP Trunking network.

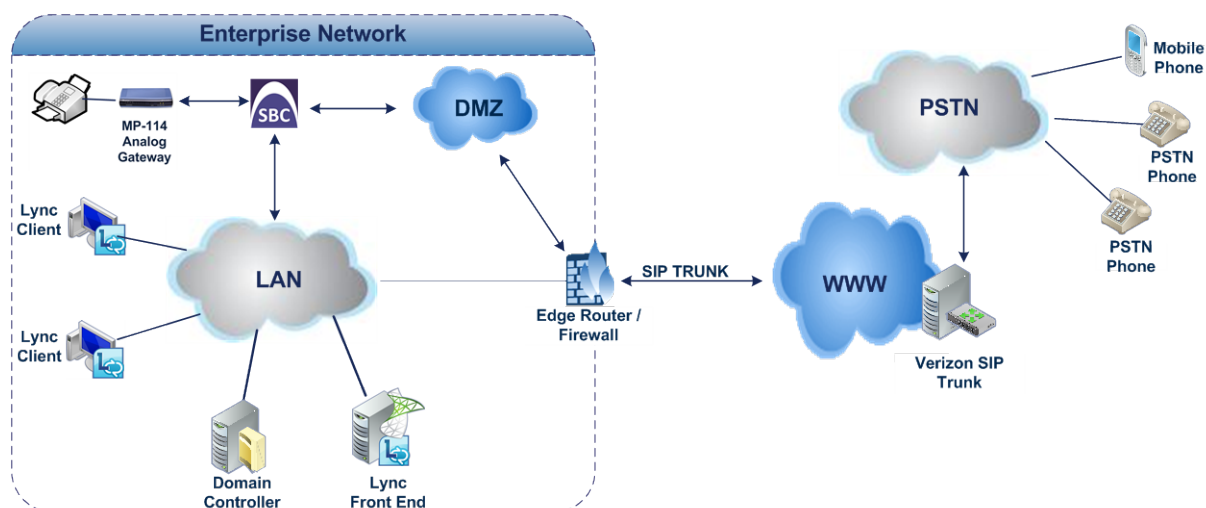
2.5 Interoperability Test Topology

Interoperability testing between AudioCodes E-SBC and Verizon SIP Trunk with Lync 2013 was performed using the following topology setup:

- The enterprise deployed Microsoft Lync Server 2013 in its private network for enhanced communication within the enterprise.
- The enterprise wants to offer its employees enterprise-voice capabilities and to connect the enterprise to the PSTN network using Verizon'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 IP-based Session Initiation Protocol (SIP).
 - Border: IP-to-IP network border between Lync Server 2013 network in the enterprise LAN and Verizon's SIP Trunk located in the public network.
 - Microsoft Lync Server 2013 works with TLS transport type while Verizon SIP trunk works on the SIP over UDP transport type.
- Transcoding support: Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders, while the Verizon SIP Trunk also supports the G.729 coder type.
- ATA - Fax support via analog media gateway. Alternatively to the ATA, FXS ports on devices that support FXS ports can be used. Verizon Network cannot initiate T.38 FAX relay reliably through all network devices. Because of this, CNG detection and activation of T.38 relay is enabled.

Figure 2-1 illustrates this interoperability test topology.

Figure 2-1: Test Topology: Interoperability between Microsoft Lync and Verizon SIP Trunk using E-SBC



2.5.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-5: Environment Setup

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

2.5.2 Known Limitations

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

Reader's Notes

3 Configuring Lync Server 2013

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



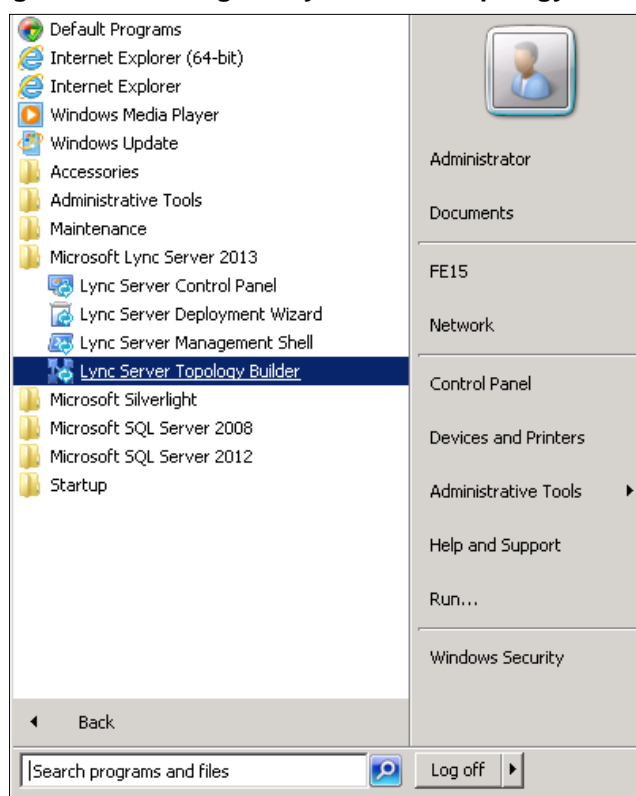
Note: Dial plans, voice policies, and PSTN uses are also necessary for enterprise voice deployment but are beyond the scope of this document.

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.

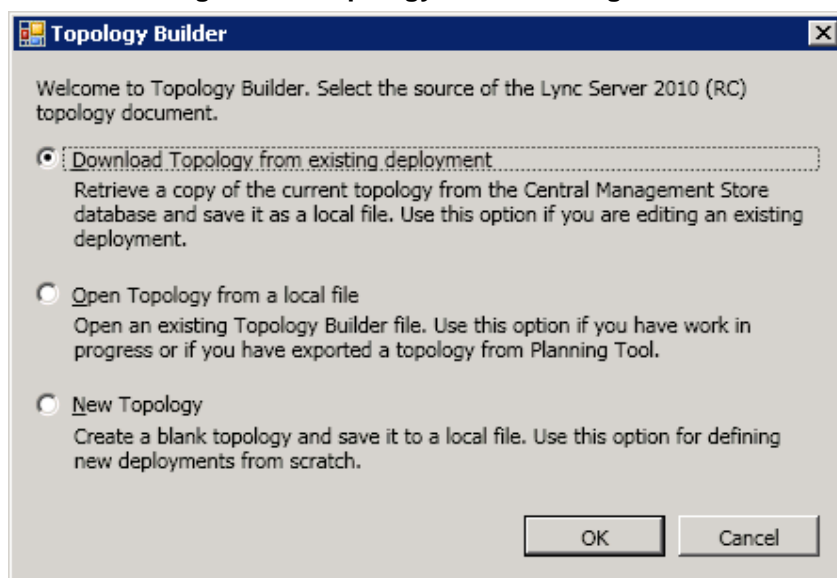
- **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**
- 1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



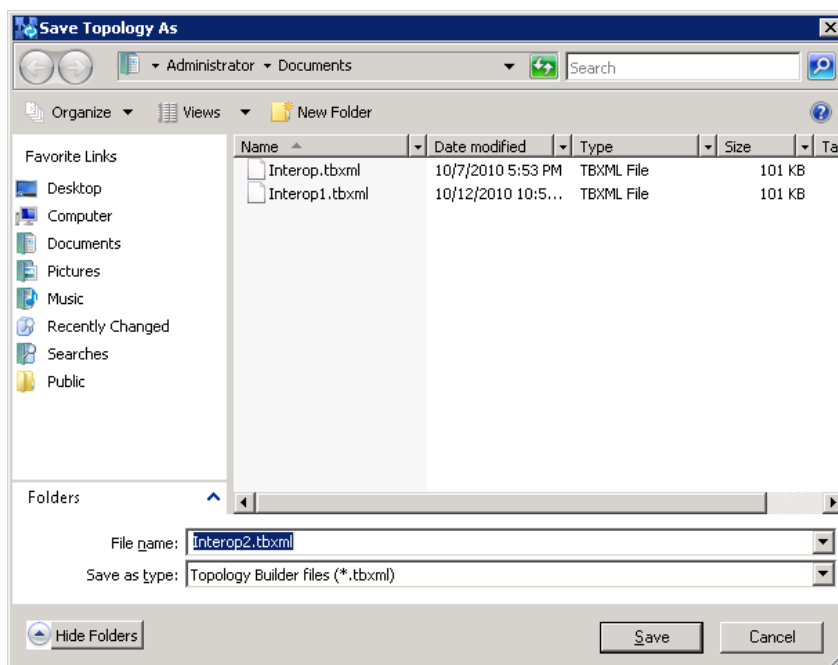
The following is displayed:

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:

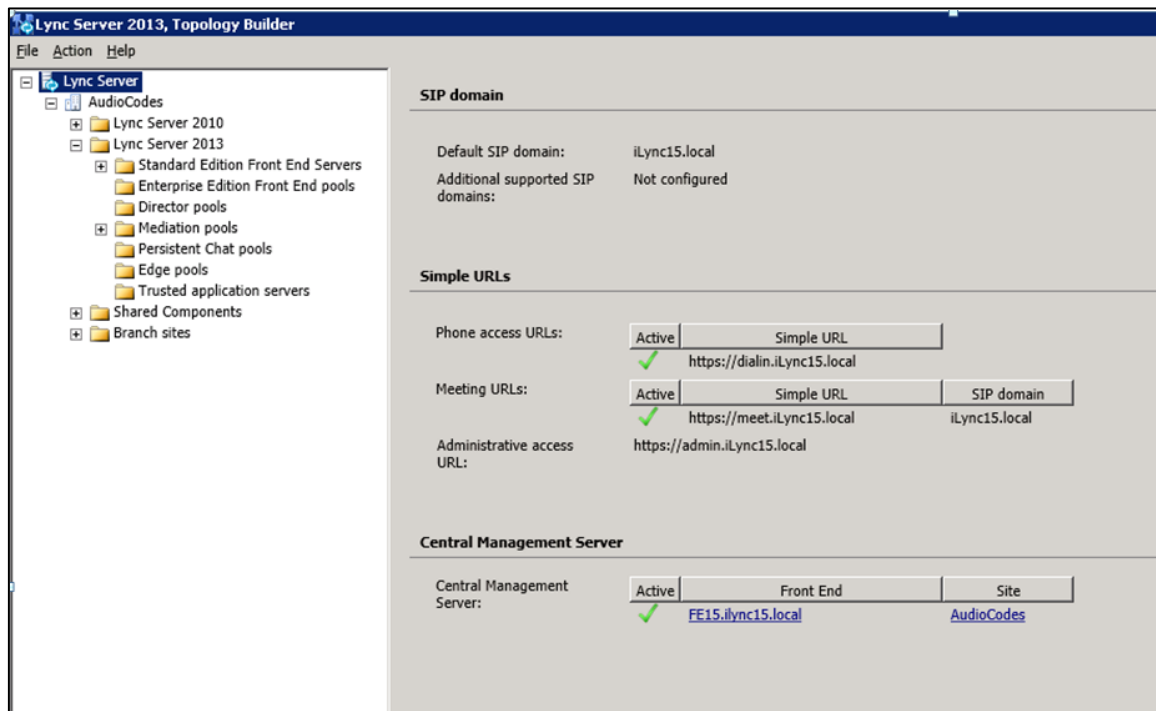
Figure 3-3: Save Topology Dialog Box



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.

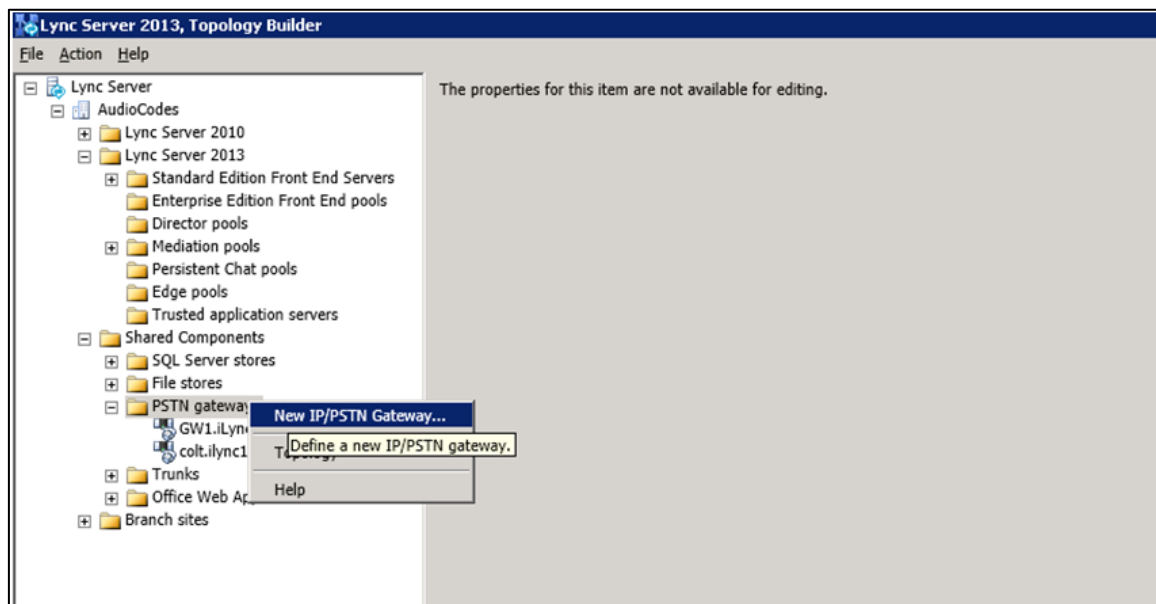
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



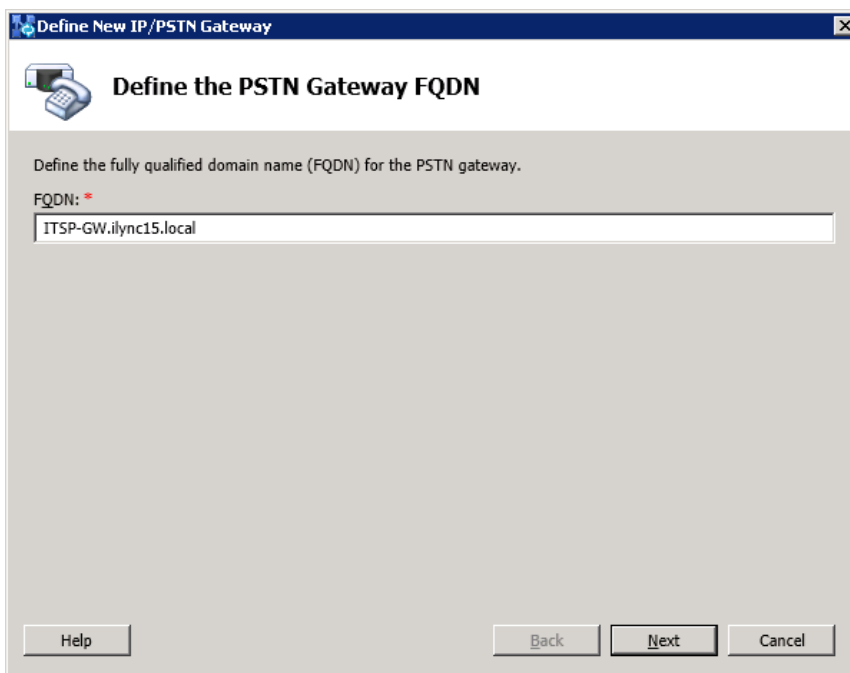
- Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



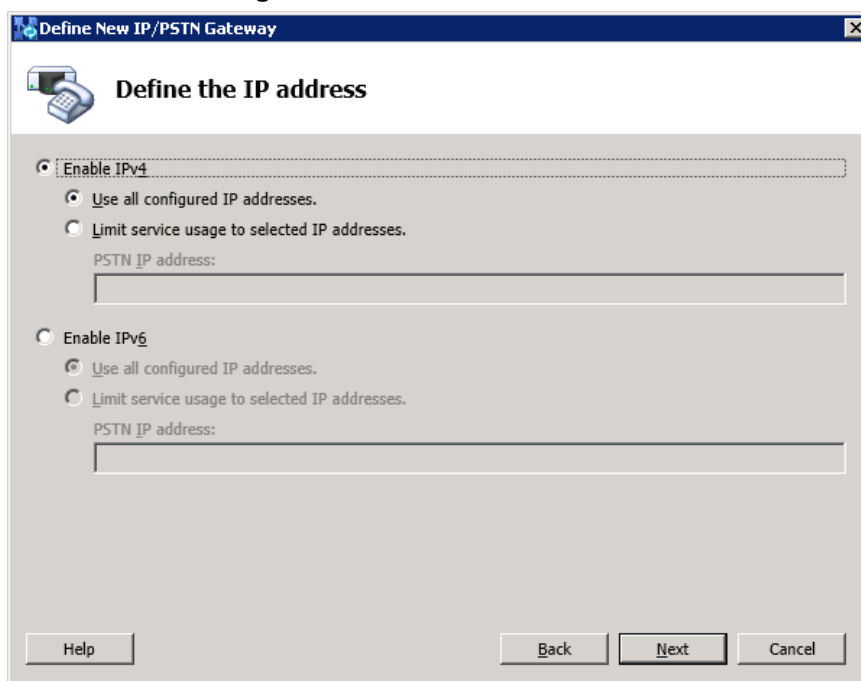
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



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



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.

**Note:**

- 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

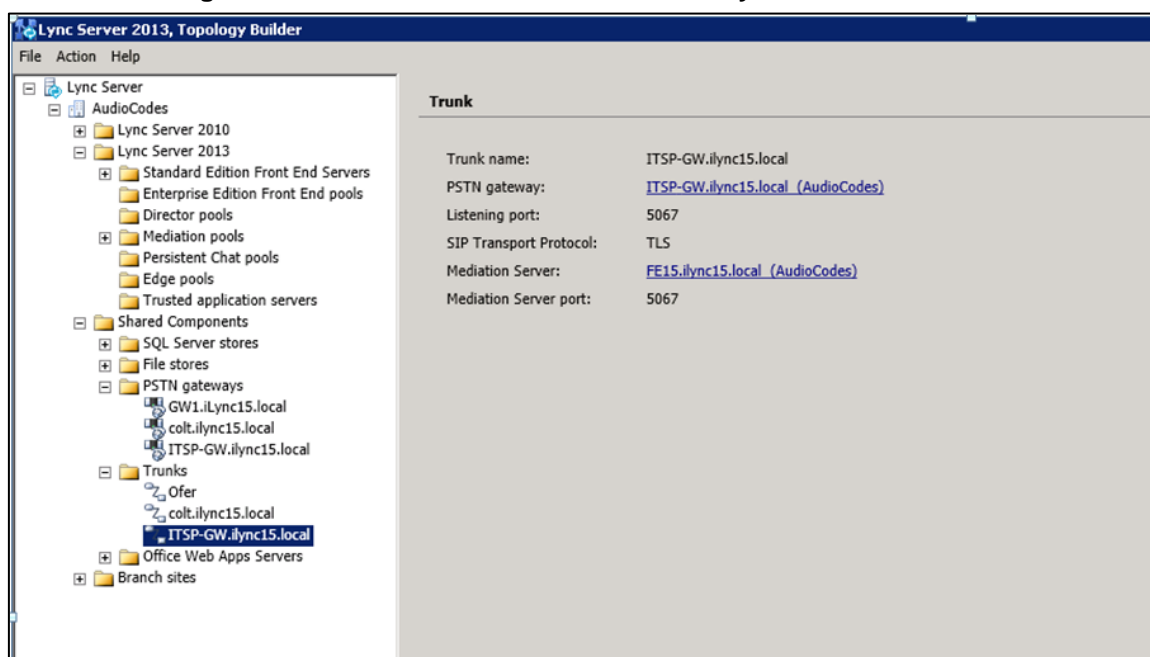
Associated Mediation Server port: *
5067

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**.

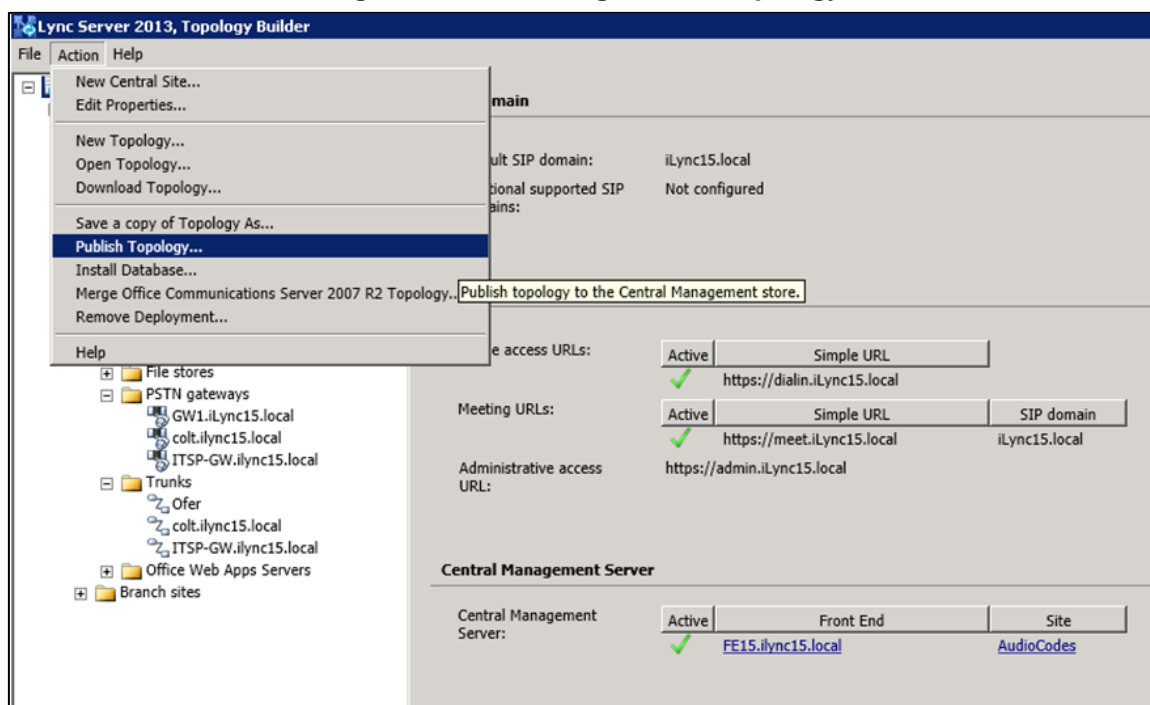
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



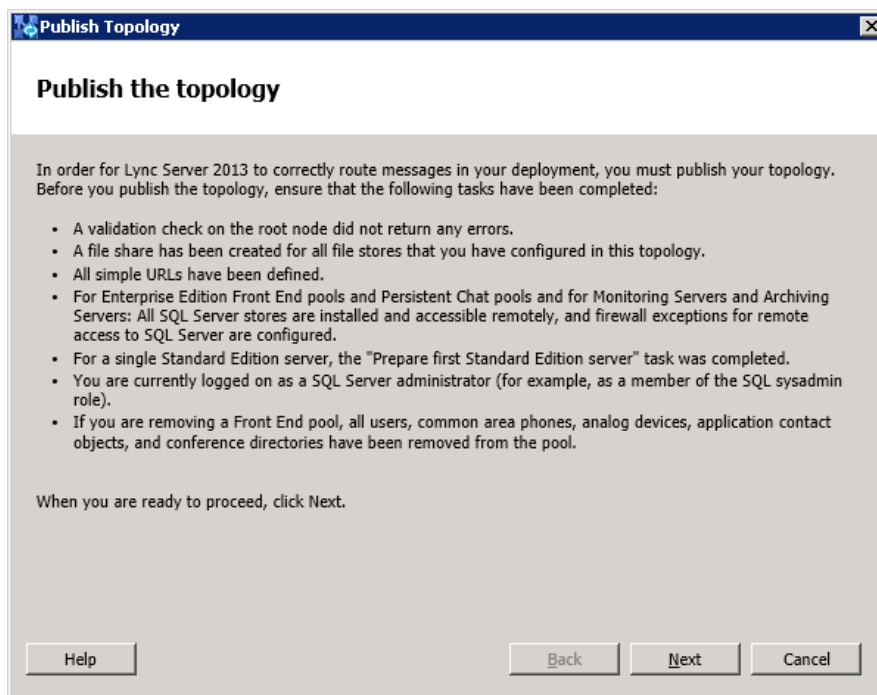
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



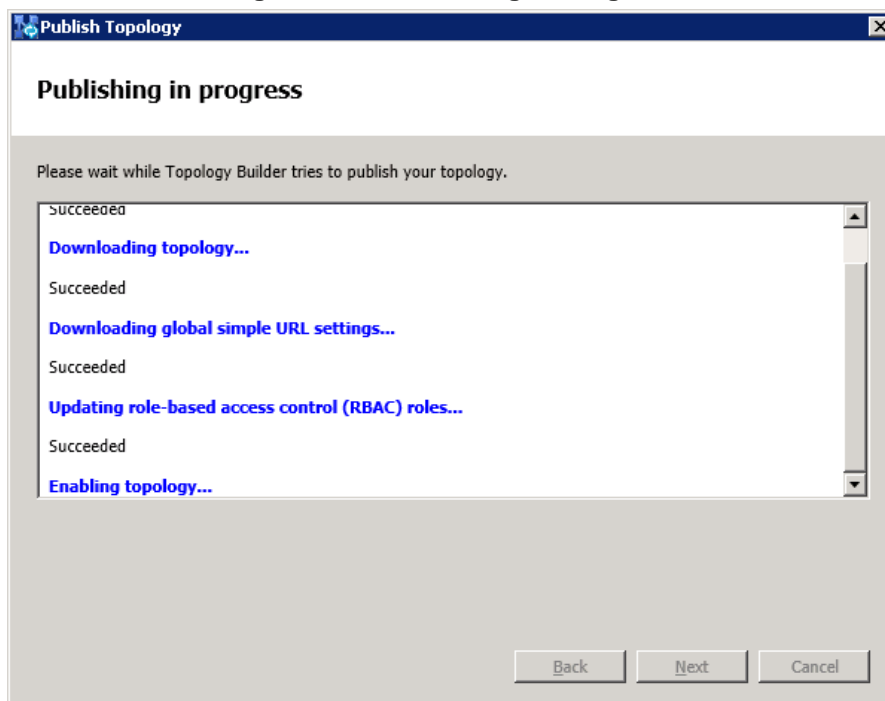
The following is displayed:

Figure 3-11: Publish the Topology



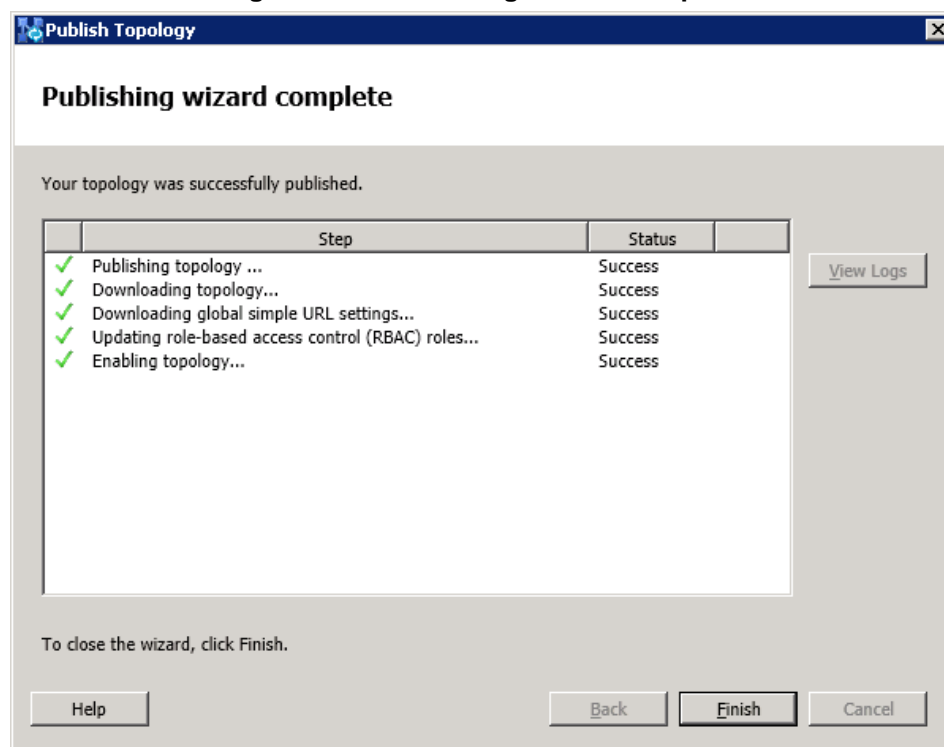
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

This section shows how to configure a "Route" on the Lync Server 2013, and to associate it with the E-SBC PSTN gateway.

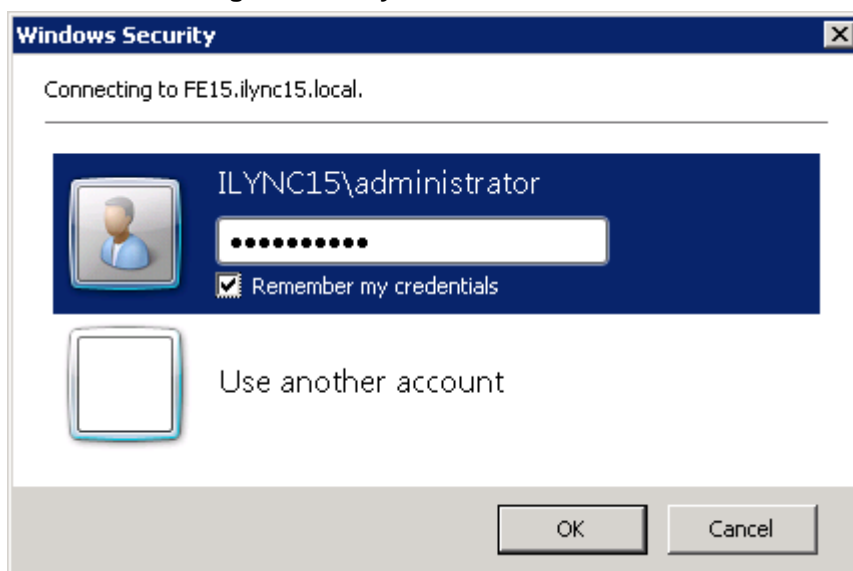
➤ **To configure the "route" on Lync Server 2013:**

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

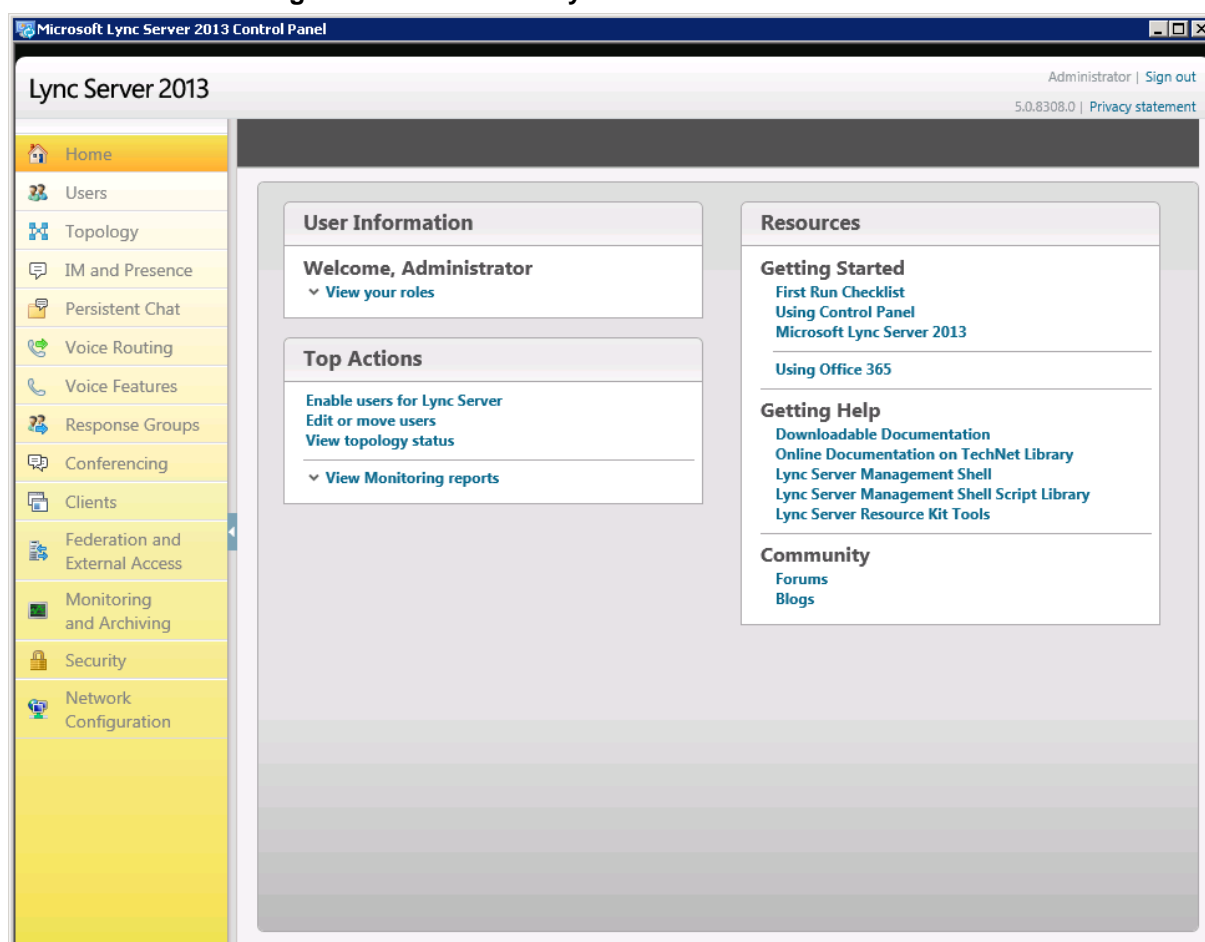
Figure 3-14: Opening the Lync Server Control Panel



You're prompted to enter your login credentials:

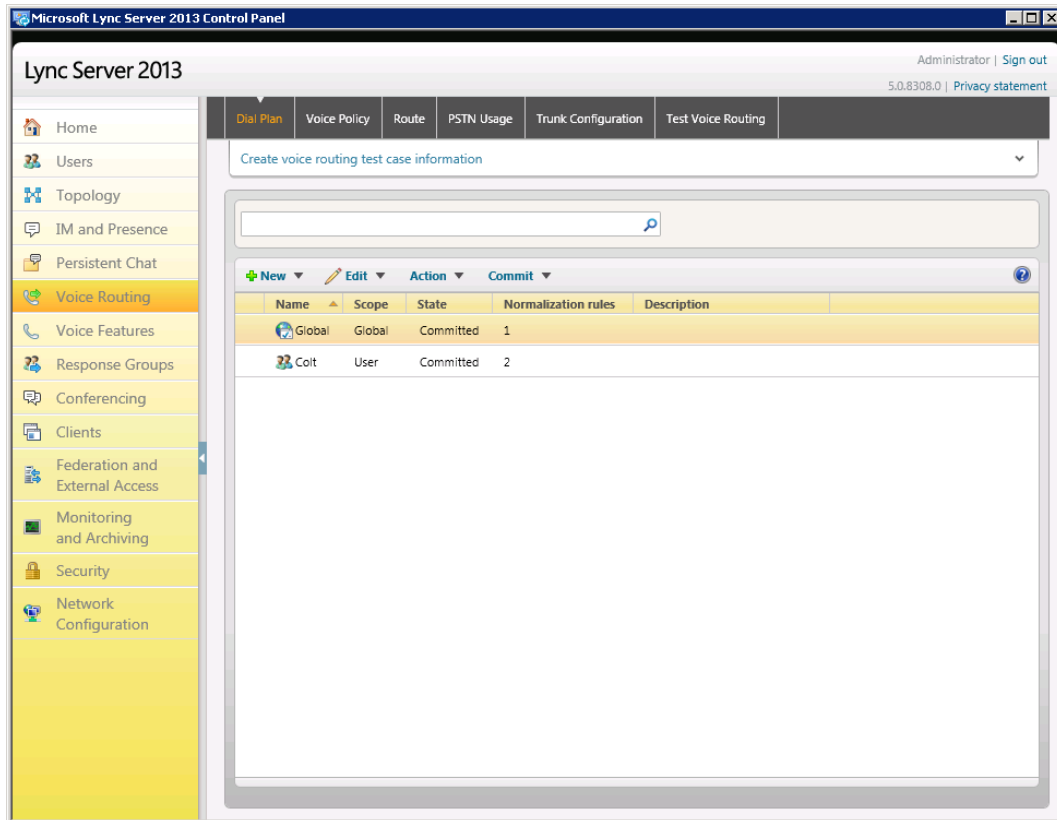
Figure 3-15: Lync Server Credentials


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

Figure 3-16: Microsoft Lync Server 2013 Control Panel


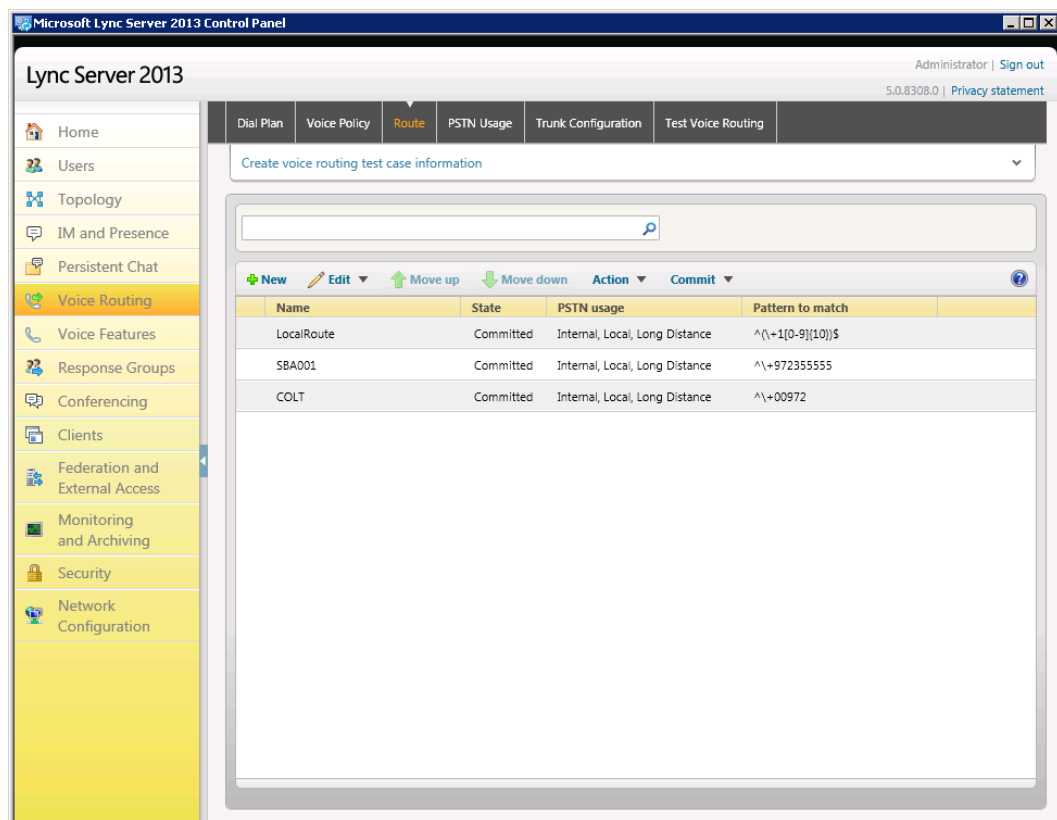
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



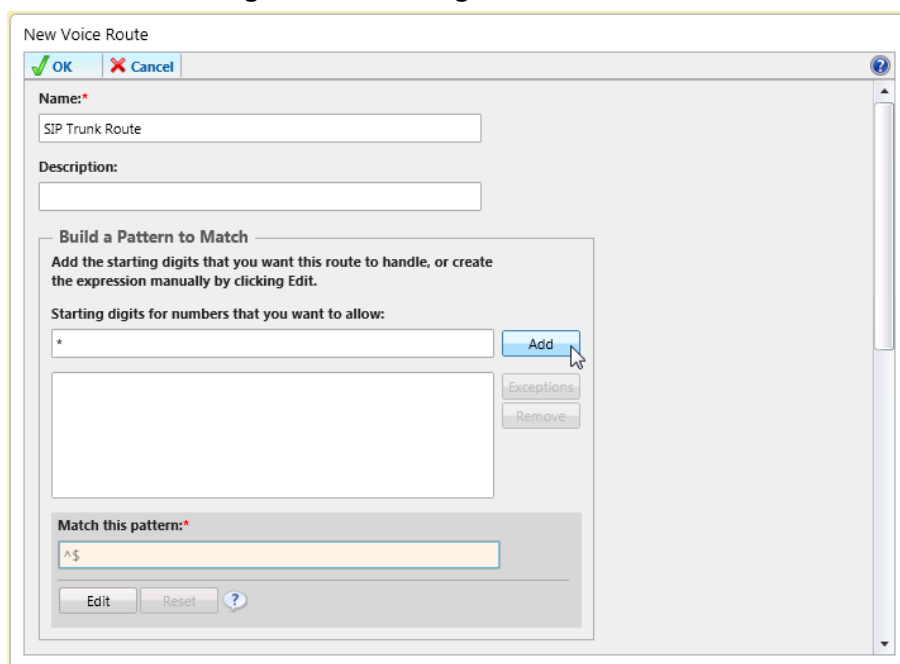
4. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



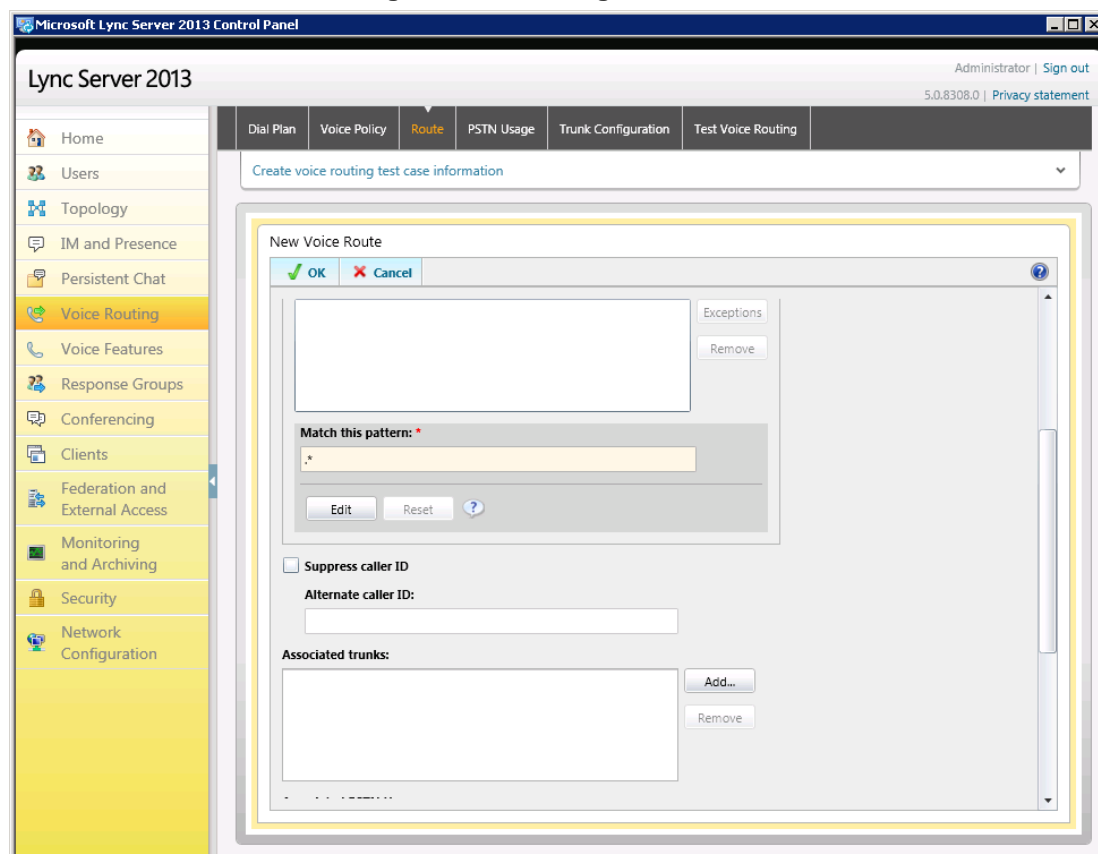
5. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



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

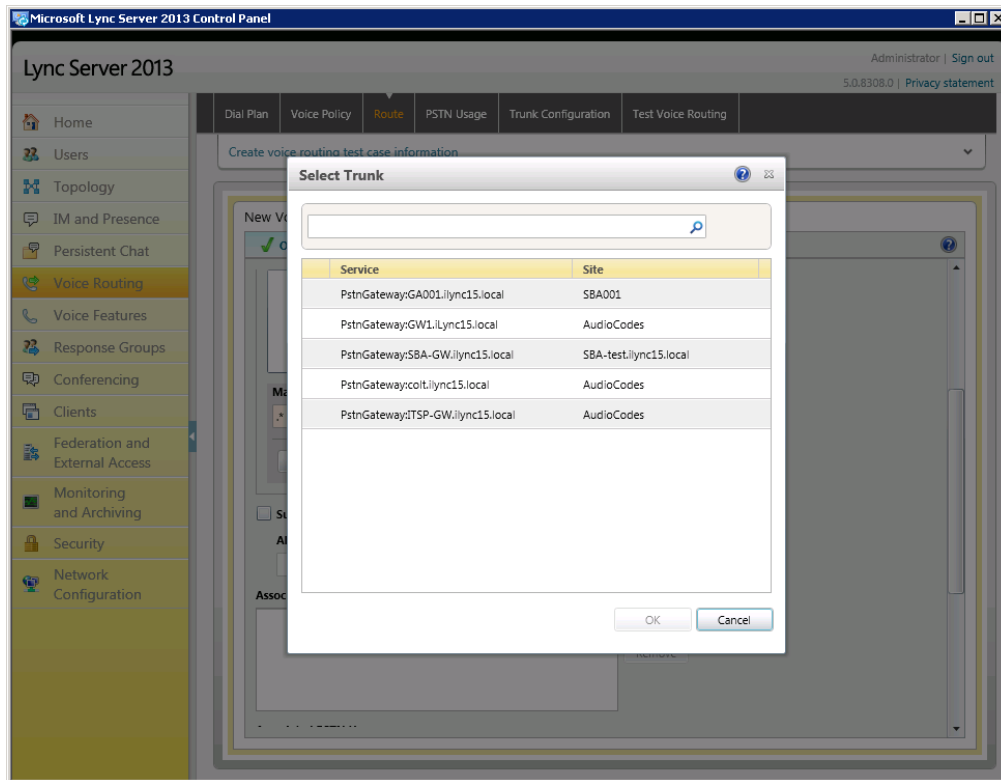
Figure 3-20: Adding New Trunk



8. Associate the route with the E-SBC Trunk that you created:

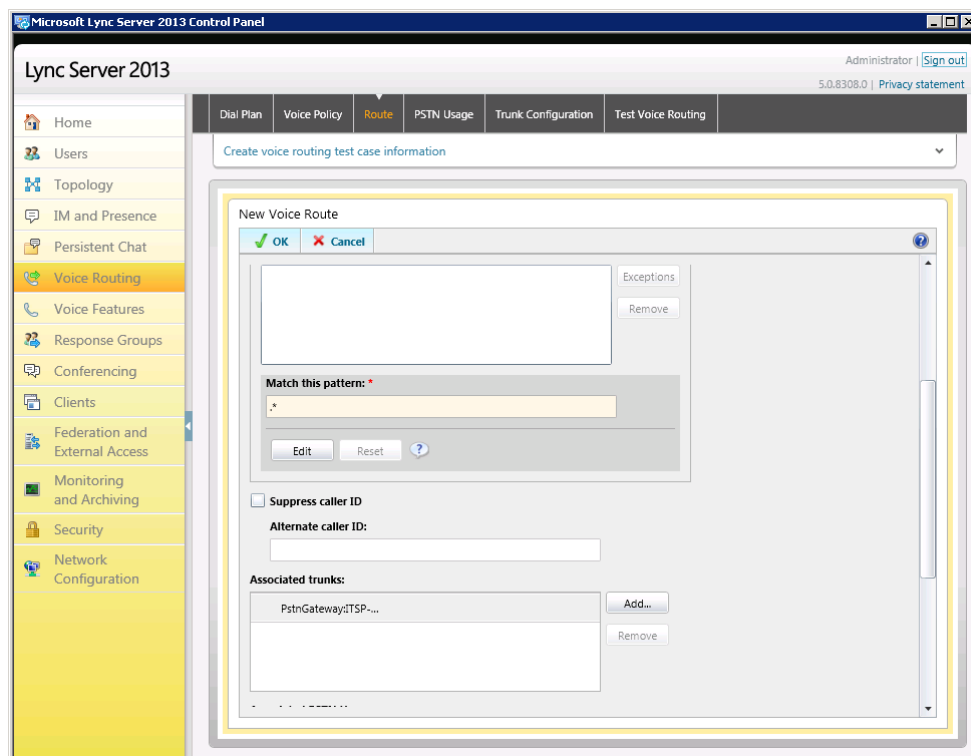
- a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



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

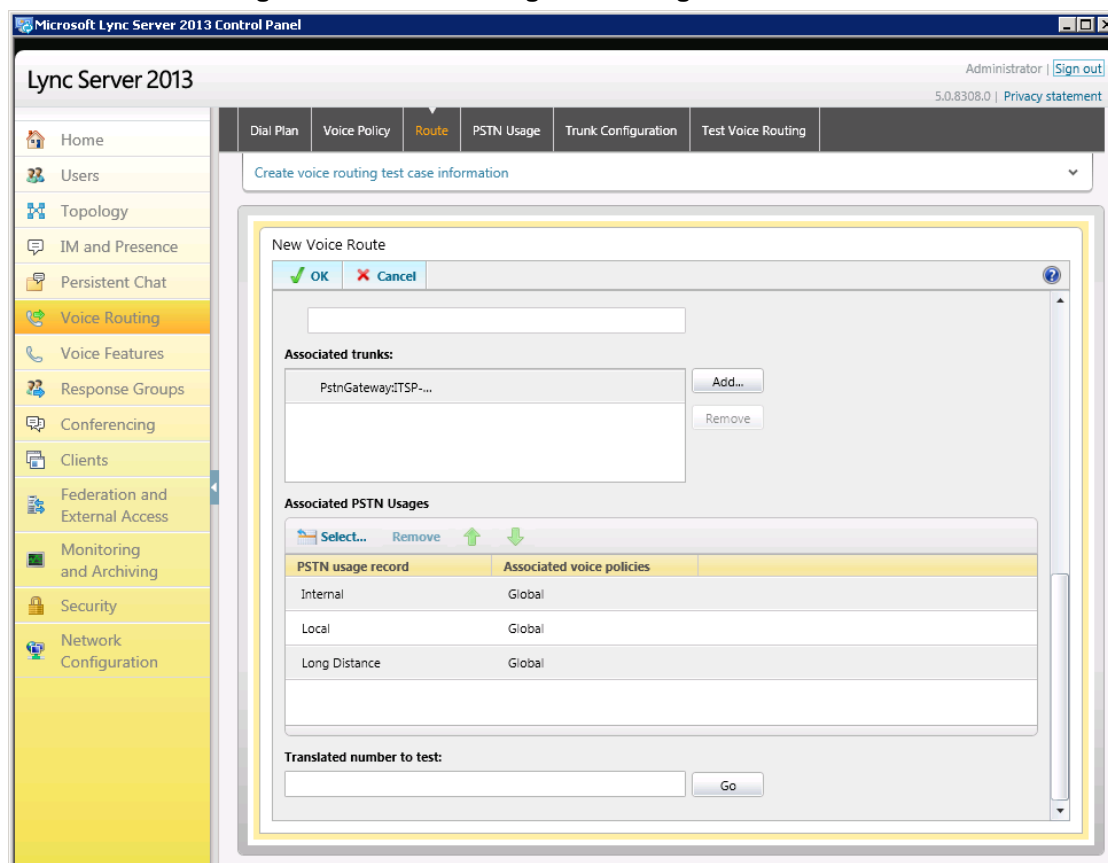
Figure 3-22: Selected E-SBC Trunk



9. Associate a PSTN Usage with this route:

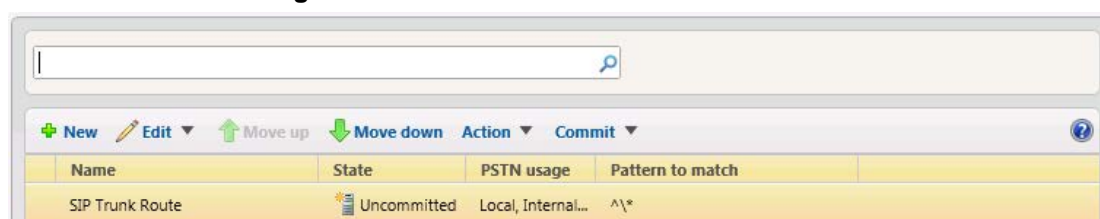
- a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage with the Route



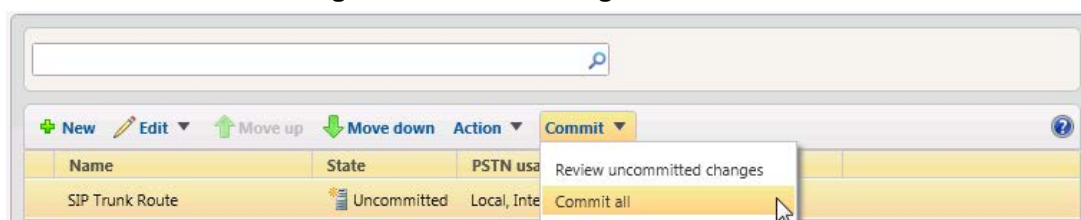
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



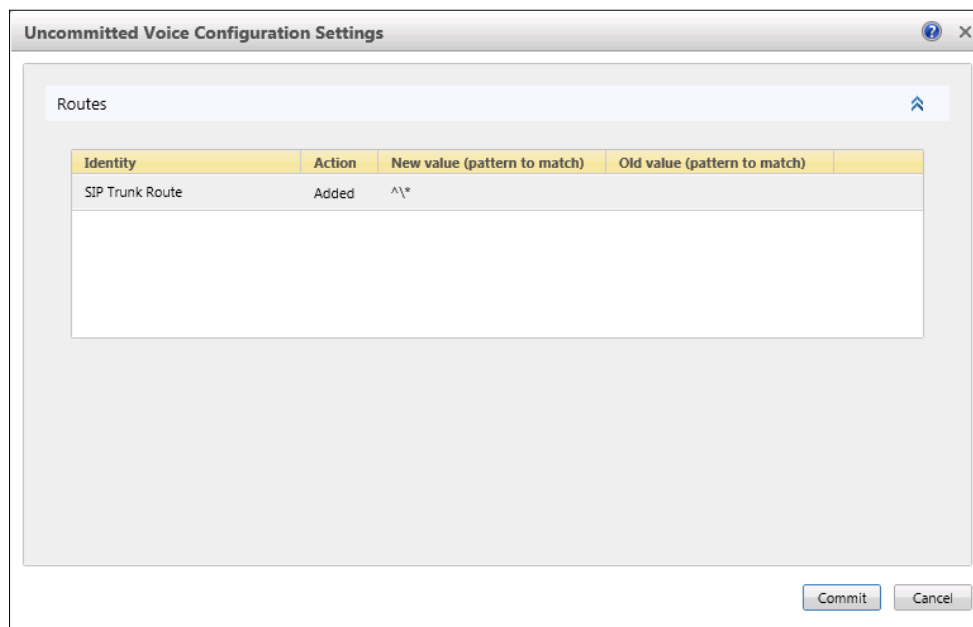
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



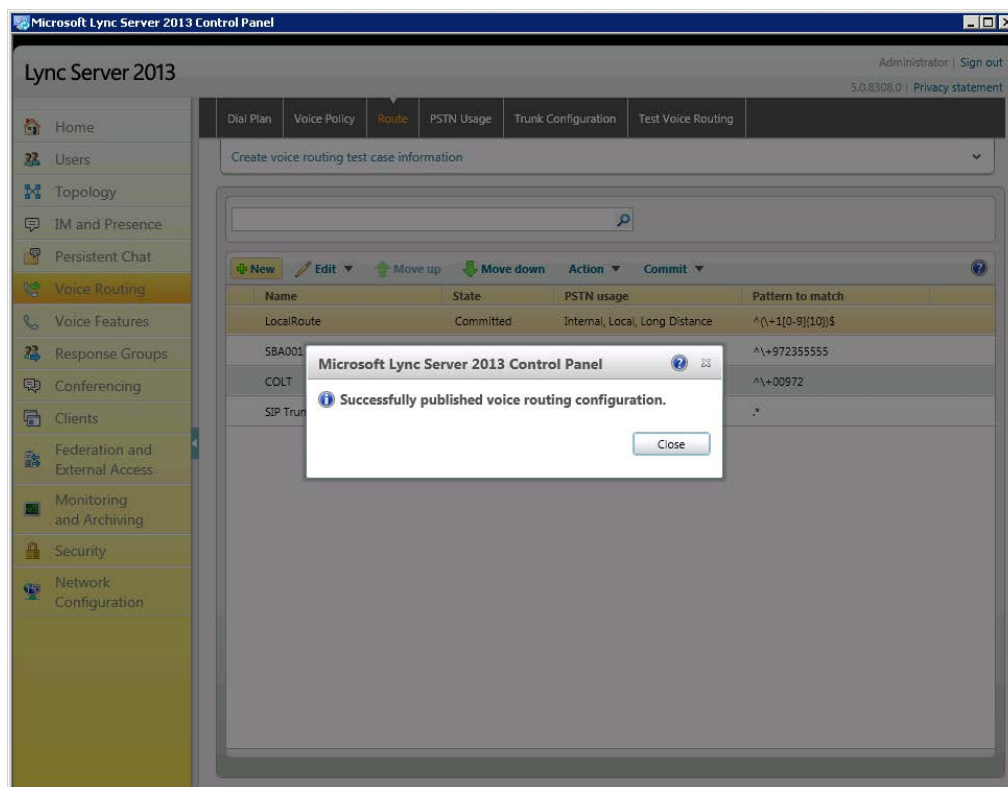
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



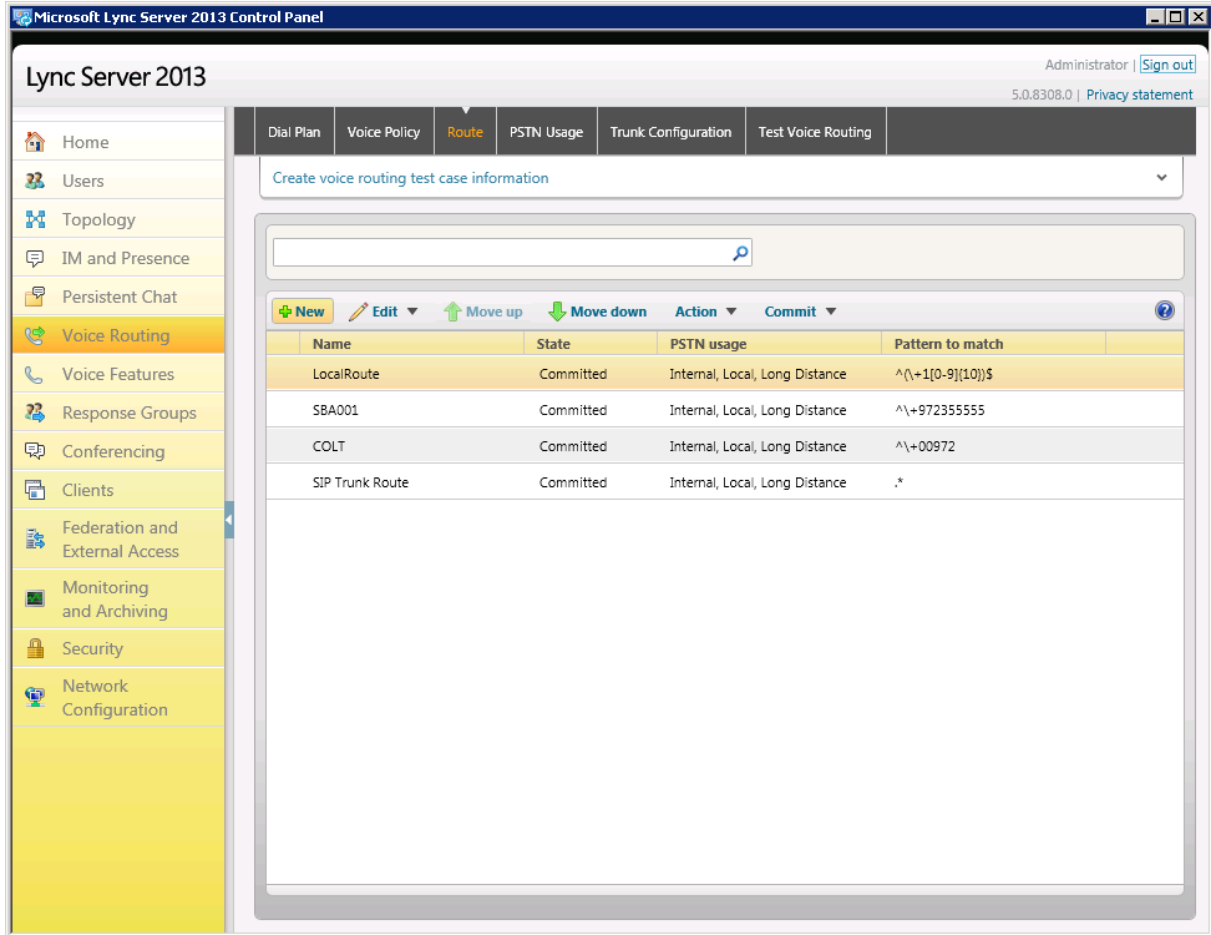
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirmation of Successful Voice Routing Configuration



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

Figure 3-28: Voice Routing Screen Displaying Committed Routes



The screenshot shows the Microsoft Lync Server 2013 Control Panel interface. The left sidebar contains navigation links: Home, Users, Topology, IM and Presence, Persistent Chat, Voice Routing (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, there are buttons for 'New', 'Edit', 'Move up', 'Move down', 'Action', and 'Commit'. A table displays the following data:

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

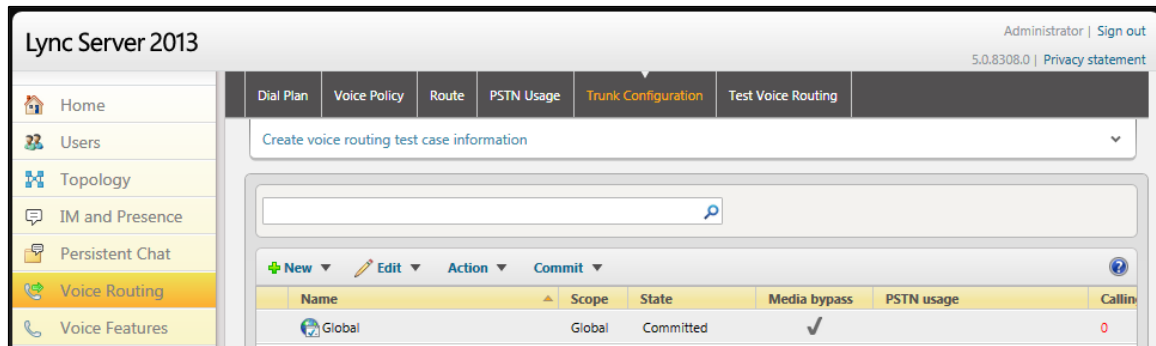
14. For ITSPs that implement a call identifier, continue with the steps below.



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 Verizon SIP Trunk in the Diversion header. Using the IP Profile settings assigned to the Verizon SIP Trunk (see Section 4.13 on page 82), the device adds this ID to an added Diversion header in the sent INVITE message while removing the History-Info header on the Verizon side of the call session.

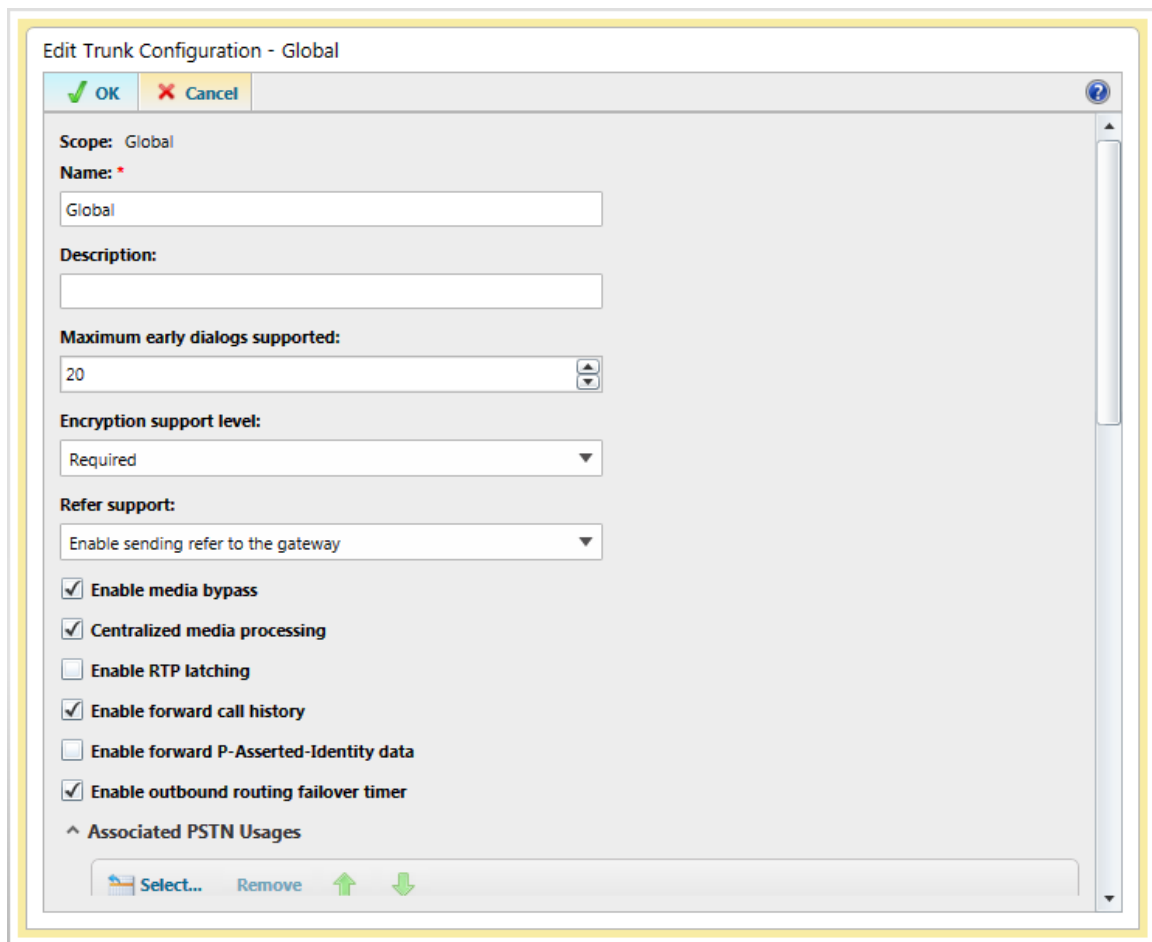
- a. In the Voice Routing page, select the **Trunk Configuration** tab. Note that you can add and modify trunk configuration by site or by pool.

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



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

Figure 3-30: Edit Trunk Configuration



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

Reader's Notes

4 Configuring AudioCodes E-SBC

This section shows how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the Verizon SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.5 on page 10, and includes the following main areas:

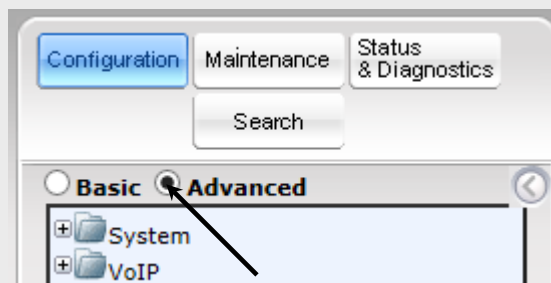
- E-SBC WAN interface - Verizon SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

Configuration is performed using the E-SBC's embedded Web server (referred to in this document as *Web interface*).

Notes:

- To implement Microsoft Lync and Verizon 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 **Advanced** display mode. To do this, select the **Advanced** option, as shown below:



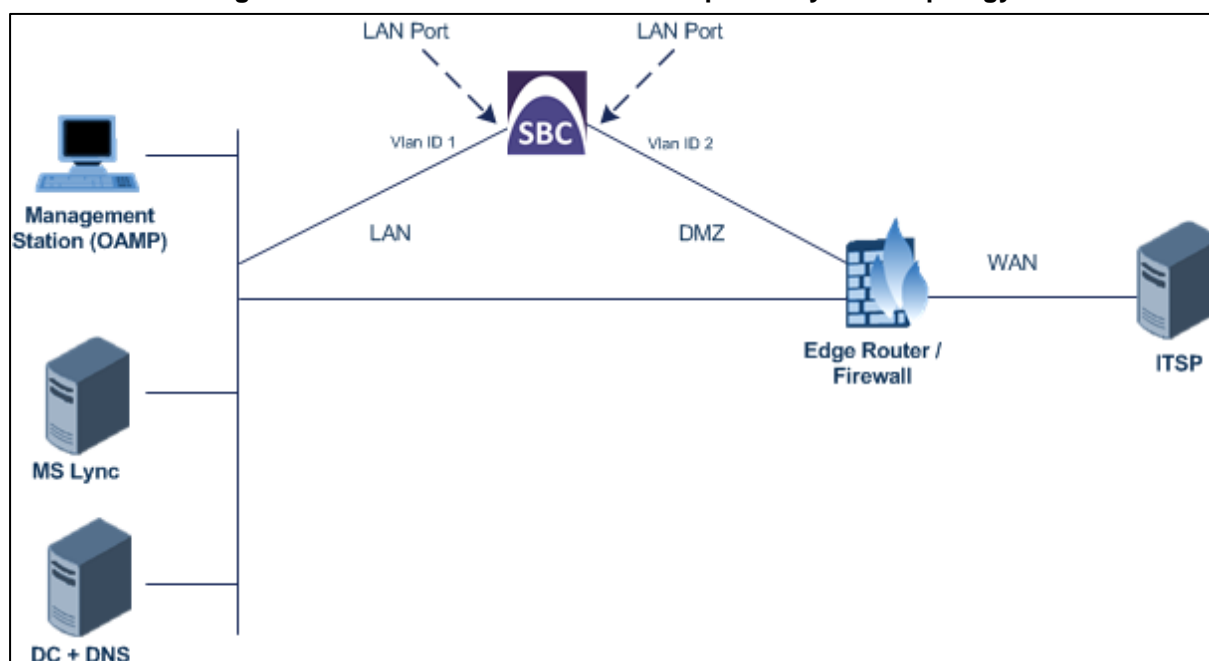
Note that when the E-SBC is reset, the navigation tree reverts to **Basic** menu display.

4.1 Step 1: Configure IP Network Interfaces

This step shows how to configure the E-SBC's IP network interfaces. There are several methods of deploying the E-SBC; this interoperability test topology employs the following deployment method:

- E-SBC interfaces with the following IP entities:
 - Lync servers, located on the LAN
 - Verizon 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 shows how to define VLANs for each of the following interfaces:

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

➤ **To configure the VLANs:**

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

There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.

2. 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 shows how to configure the IP network interfaces for each of the following interfaces:

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

➤ **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	10.133.4.43 (IP address of E-SBC)
Prefix Length	16 (subnet mask in bits for 255.255.0.0)
Gateway	10.133.4.1
Interface Name	Voice (arbitrary descriptive name)
Primary DNS Server IP Address	10.133.4.40
Underlying Device	vlan 1

3. Add a network interface for the WAN side:

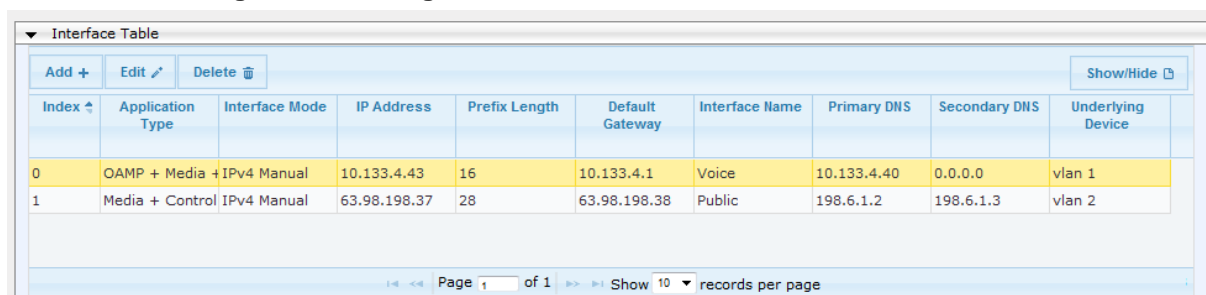
- Enter **1**, and then click **Add Index**.
- Configure the interface as follows:

Parameter	Value
Application Type	Media + Control
IP Address	63.98.198.37 (WAN IP address)
Prefix Length	28 (for 255.255.255.240)
Gateway	63.98.198.38 (router's IP address)
Interface Name	Public
Primary DNS Server IP Address	192.6.1.2
Secondary DNS Server IP Address	192.6.1.3
Underlying Device	vlan 2

4. Click **Apply**, and then **Done**.

The configured IP network interfaces are shown in the figure below:

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



Interface Table									
Add + Edit Delete			Show/Hide						
Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media +	IPv4 Manual	10.133.4.43	16	10.133.4.1	Voice	10.133.4.40	0.0.0.0	vlan 1
1	Media + Control	IPv4 Manual	63.98.198.37	28	63.98.198.38	Public	192.6.1.2	192.6.1.3	vlan 2



4.1.3 Step 1c: Configure the Native VLAN ID

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

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

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

Figure 4-4: Configured Port Native VLAN

Physical Ports Settings							
Edit 							Show/Hide 
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_0_1	Enable	1	Auto Negotiation	LAN Port#1	GROUP_1	Active
1	GE_0_2	Enable	1	Auto Negotiation	LAN Port#2	GROUP_1	Redundant
2	GE_7_1	Enable	2	Auto Negotiation	WAN Port#1	GROUP_2	Active
3	GE_7_2	Enable	2	Auto Negotiation	WAN Port#2	GROUP_2	Redundant
4	GE_7_3	Enable	3	Auto Negotiation	User Port #4	GROUP_3	Active
5	GE_7_4	Enable	3	Auto Negotiation	User Port #5	GROUP_3	Redundant

Page 1 of 1 Show 10 records per page View 1 - 6 of 6

4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

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

Figure 4-5: Enabling SBC Application

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

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 98).

4.3 Step 3: Configure SRDs

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

The SRD comprises:

- 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 shows 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	1
Media Realm Name	MRLan (descriptive name)
IPv4 Interface Name	Voice
Port Range Start	21010 (represents lowest UDP port number used for media on LAN.)
Number of Media Session Legs	10 (media sessions assigned with port range)

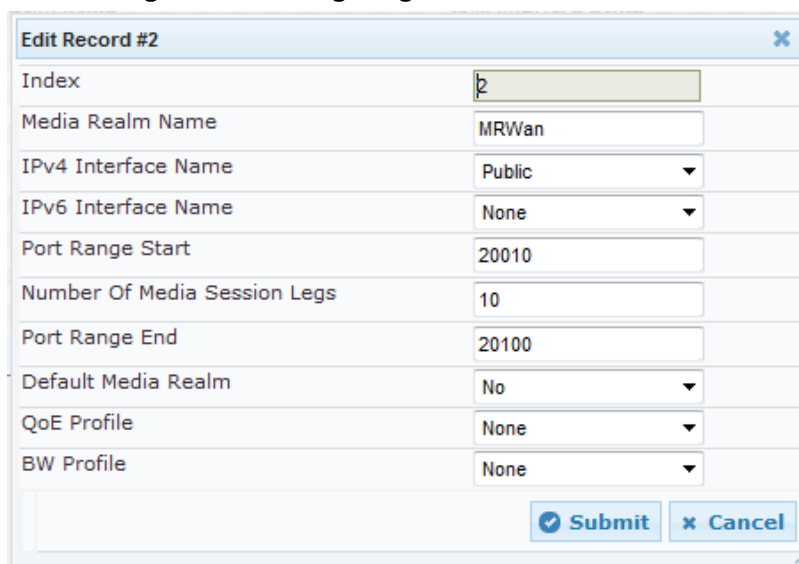
Figure 4-6: Configuring Media Realm for LAN

Edit Record #1	
Index	1
Media Realm Name	MRLan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	21010
Number Of Media Session Legs	10
Port Range End	21100
Default Media Realm	Yes
QoS Profile	None
BW Profile	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	2
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	Public
Port Range Start	20010 (represents the lowest UDP port number used for media on WAN. This was a requirement of certification testing)
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



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

4.3.2 Step 3b: Configure SRDs

This step shows how to configure the SRDs.

➤ **To configure SRDs:**

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

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

Figure 4-9: Configuring LAN SRD

Edit Record #1	
Index	1
Name	LanSRD
Media Realm Name	MRLan
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Parameter	Value
SRD Index	2
SRD Name	WanSRD
Media Realm	MRWan

Figure 4-10: Configuring WAN SRD

Edit Record #2	
Index	2
Name	WanSRD
Media Realm Name	MRWan
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

4.3.3 Step 3c: Configure SIP Signaling Interfaces

This step shows 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:

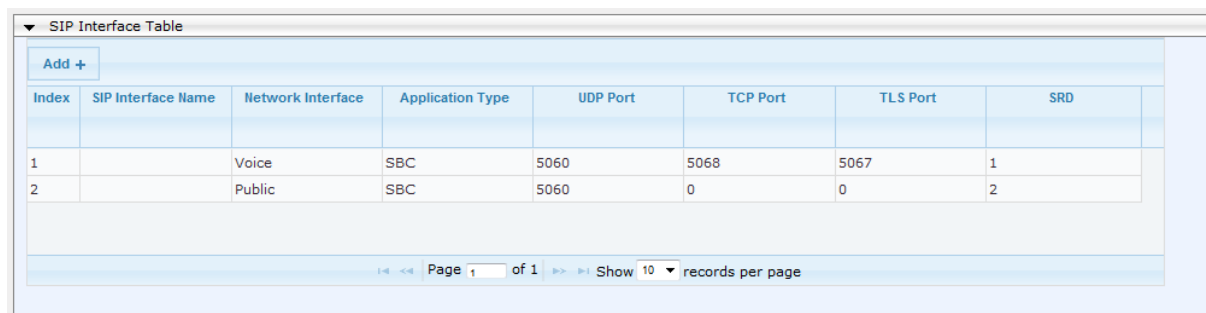
Parameter	Value
Index	1
Interface Name	Arbitrary descriptive name
Network Interface	Voice
Application Type	SBC
TLS Port	5067 (recommended)
TCP Port	5068 (if TCP is used)
UDP Port	5060
SRD	1

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	2
Interface Name	Arbitrary descriptive name
Network Interface	Public
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



Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1		Voice	SBC	5060	5068	5067	1
2		Public	SBC	5060	0	0	2

4.4 Step 4: Configure Proxy Sets

This step shows 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 must be configured for the following IP entities:

- Microsoft Lync Server 2013
- Verizon SIP Trunk

These Proxy Sets will later be associated with IP Groups.

➤ To configure Proxy Sets:

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

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

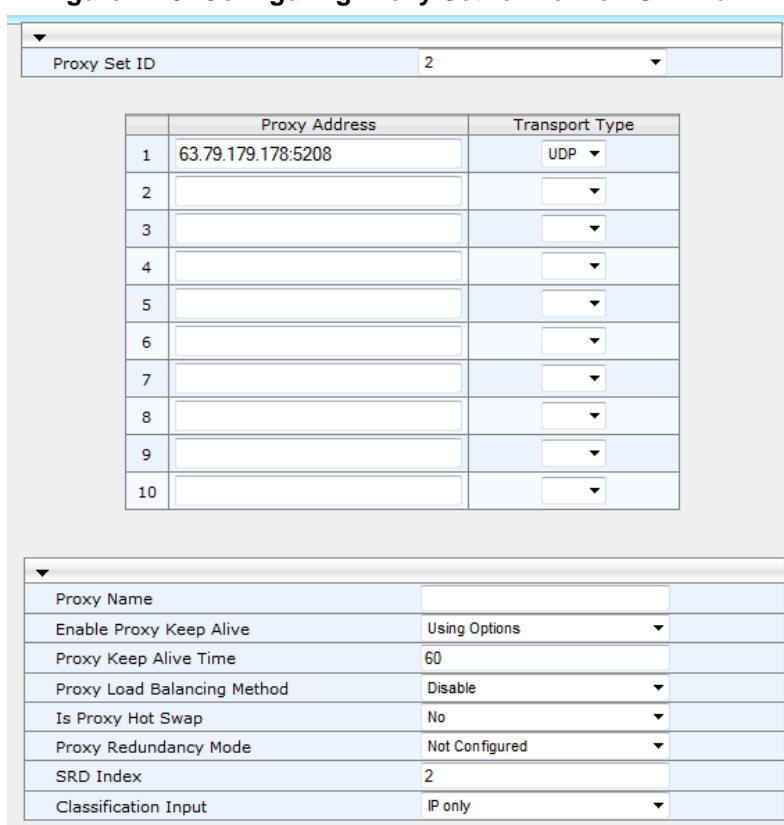
Figure 4-12: Configuring Proxy Set for Microsoft Lync Server 2013

The screenshot shows the configuration interface for Proxy Sets. At the top, there is a dropdown menu for 'Proxy Set ID' with the value '1'. Below this is a table with two columns: 'Proxy Address' and 'Transport Type'. The table has 10 rows, with the first row containing the values 'FE15.ilync15.local:5067' and 'TLS'. Below the table is a form with several fields: 'Proxy Name', 'Enable Proxy Keep Alive' (set to 'Using Options'), 'Proxy Keep Alive Time' (set to '30'), 'Proxy Load Balancing Method' (set to 'Disable'), 'Is Proxy Hot Swap' (set to 'Yes'), 'Proxy Redundancy Mode' (set to 'Not Configured'), 'SRD Index' (set to '1'), and 'Classification Input' (set to 'IP only').

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

Parameter	Value
Proxy Set ID	2
Proxy Address	63.79.179.178:5208 (Verizon IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	Arbitrary descriptive name
Enable Proxy Keep Alive	Using Options
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to Verizon SIP Trunk)

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



Proxy Set ID: 2

	Proxy Address	Transport Type
1	63.79.179.178:5208	UDP
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name:

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Not Configured

SRD Index: 2

Classification Input: IP only

4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.15 on page 98).

4.5 Step 5: Configure IP Groups

This step shows 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. After IP Groups are configured, they're 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
- Verizon SIP Trunk 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	Microsoft Lync (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	63.98.198.37 (according to ITSP requirement)
SRD	1
Media Realm Name	MRLan
IP Profile ID	1

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

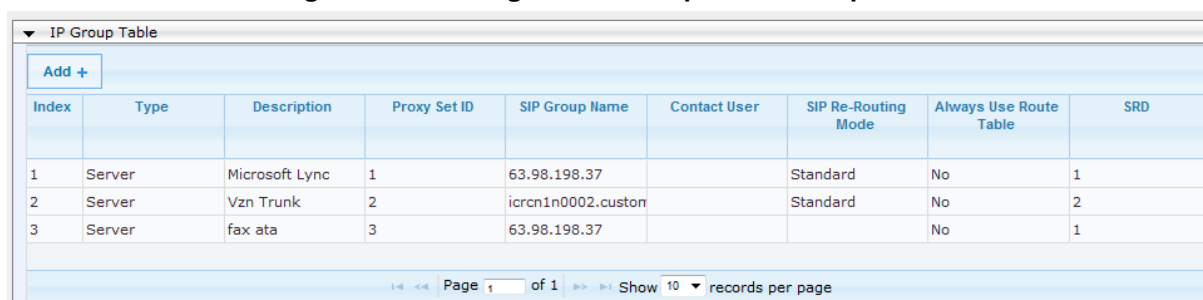
Parameter	Value
Index	2
Type	Server
Description	Vzn Trunk (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	icrcn1n0002.customer08.tsengr.com (according to ITSP requirement)
SRD	2
Media Realm Name	MRWan
IP Profile ID	2

4. Configure an IP Group for the Fax supporting ATA:

Parameter	Value
Index	3
Type	Server
Description	fax ata (arbitrary descriptive name)
Proxy Set ID	3
SIP Group Name	63.97.198.37 (according to ITSP requirement)
SRD	1
Media Realm Name	MRLan
IP Profile ID	3

The configured IP Groups are shown in the figure below:

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



IP Group Table								
Add +								
Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	Microsoft Lync	1	63.98.198.37		Standard	No	1
2	Server	Vzn Trunk	2	icrcn1n0002.custom		Standard	No	2
3	Server	fax ata	3	63.98.198.37			No	1

Page 1 of 1 Show 10 records per page

4.6 Step 6: Configure IP Profiles

This step shows 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 must be configured for the following IP entities:

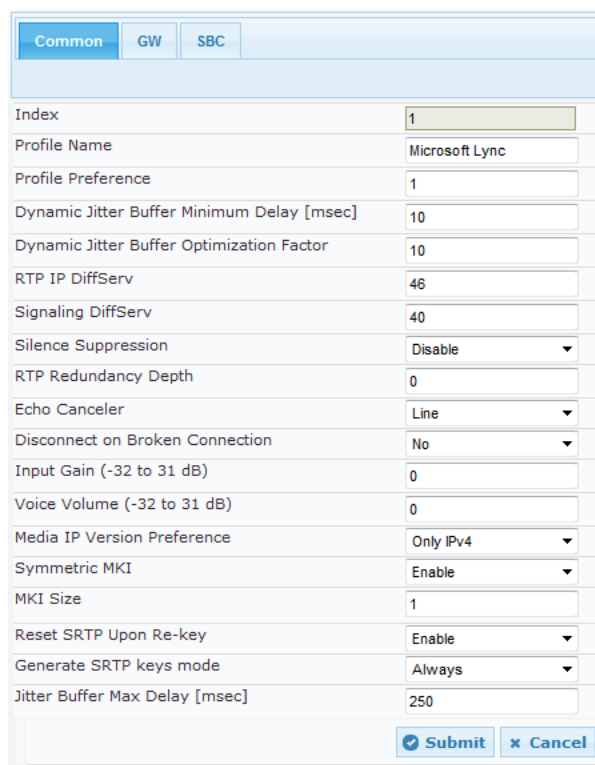
- Microsoft Lync Server 2013 - to operate in secure mode using SRTP and TLS
- Verizon SIP trunk - to operate in non-secure mode using RTP and UDP
- Fax supporting ATA

Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 43).

➤ **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	Microsoft Lync (arbitrary descriptive name)
Symmetric MKI	Enable
MKI Size	1
Reset SRTP State Upon Re-key	Enable
Generate SRTP keys mode:	Always

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


Parameter	Value
Index	1
Profile Name	Microsoft Lync
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceled	Line
Disconnect on Broken Connection	No
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Enable
MKI Size	1
Reset SRTP Upon Re-key	Enable
Generate SRTP keys mode	Always
Jitter Buffer Max Delay [msec]	250

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

Parameter	Value
Extension Coders Group ID	Coders Group 1
Transcoding Mode	Force
Allowed Coders Group ID	Coders Group 1
Allowed Coders Mode	Restriction and Preference
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 because Lync Server 2013 does not support receipt of SIP REFER)
Remote 3xx Behavior	Handle Locally (required because Lync Server 2013 does not support receipt of SIP 3xx responses)
Enforce MKI Size	Enforce
Remote Early Media RTP Behavior	Delayed (required because Lync Server 2013 does not send RTP immediately to the remote side when it sends a SIP 18x response)

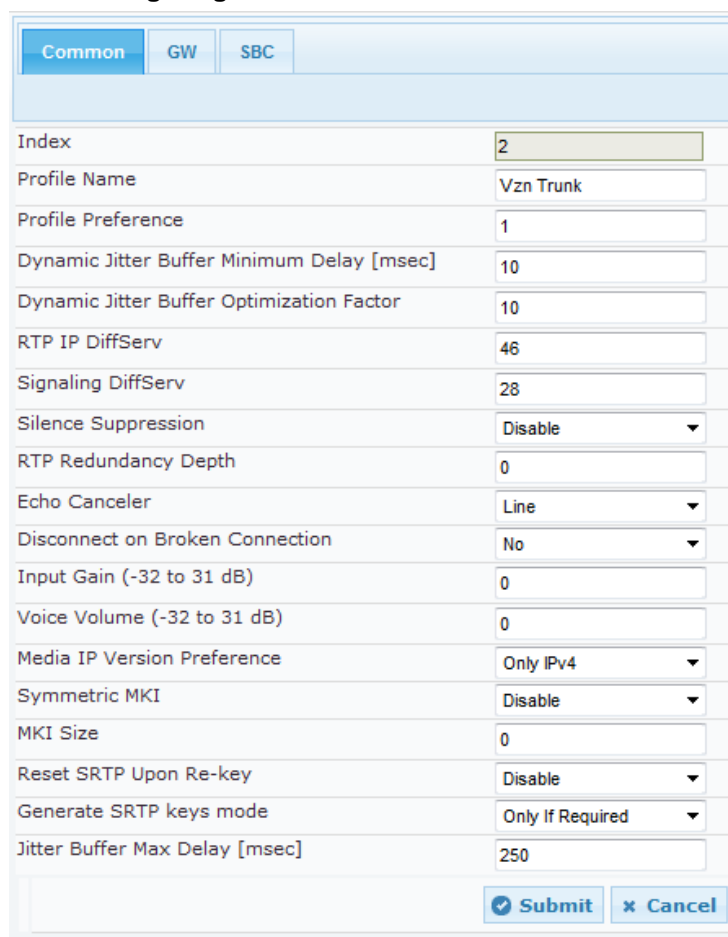
Figure 4-16: Configuring IP Profile for Lync Server 2013 – SBC Tab

Common GW SBC	
Index	1
Extension Coders Group ID	Coders Group 1
Transcoding Mode	Force
Allowed Media Types	
Allowed Coders Group ID	Coders Group 1
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction and Prefer
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 S
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally
Remote 3xx Behavior	Handle Locally
Remote Multiple 18x	Supported
Remote Early Media Response Type	183
Remote Early Media	Supported
Enforce MKI Size	Enforce
Remote Early Media RTP Behavior	Delayed
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Transparent
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

5. Configure an IP Profile for the Verizon SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Profile Name	Vzn Trunk (arbitrary descriptive name)
RTP IP DiffServ	46
Signaling Diffserv	28

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



Parameter	Value
Index	2
Profile Name	Vzn Trunk
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	28
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceler	Line
Disconnect on Broken Connection	No
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	250

Submit Cancel

6. Verizon requires the SIP Signaling and RTP packets to be treated independently and marked with the proper settings to be delivered to the Verizon SIP Trunking network.

Table 4-1: DiffServ Service Classes

Service Class Name	DSCP Name	DSCP Value	Example Apps	AudioCodes Value
Telephony	EF	101110	RTP/IP Telephony bearer	46
Signaling	CS5	101000	RTP/SIP/IP Telephony signaling	40
Multimedia Streaming	AF31	011010	SIP/Streaming video and audio on demand	26
	AF32	011100		28
	AF33	011110		30
Broadcast Video	CS3	011000	SIP/Broadcast TV & live events	24
Standard	DF (CS0)	000000	Undifferentiated applications	0
Low-priority data	CS1	001000	Any flow that has no BW assurance	8

Source: RFC 4594. Configuration Guidelines for DiffServ Service Classes.

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

Parameter	Value
Profile ID	2
Extension Coders Group ID	Coders Group 2
Allowed Coders Group ID	Coders Group 2
Allowed Coders Mode	Restriction and Preference (lists Allowed Coders first and then original coders in received SDP offer)
Media Security Behavior	RTP
P-Asserted-Identity	Add (required for anonymous calls)
Diversion Mode	Add
History-Info Mode	Remove
Fax Coders Group ID	Coder Group 4
Fax Behavior	Handle on re-INVITE
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Remote Multiple 18x	Not Supported
Remote Can Play Ringback	No (required because Lync Server 2013 does not provide a ringback tone for incoming calls)
Remote Hold Format	Send Only

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

Common GW SBC	
Index	2
Extension Coders Group ID	Coders Group 2
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	Coders Group 2
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction and Prefer
SBC Media Security Behavior	RTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	Add
Diversion Mode	Add
History-Info Mode	Remove
Fax Coders Group ID	Coders Group 4
Fax Behavior	Handle on re-INVITE
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	Not Supported
Remote Early Media Response Type	183
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	No
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Send Only
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

8. Configure an IP Profile for the Fax supporting ATA:
 - a. Click **Add**.
 - b. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	3
Profile Name	FAX ATA (arbitrary descriptive name)

Figure 4-19: Configuring IP Profile for FAX supporting ATA – Common Tab

Parameter	Value
Index	3
Profile Name	FAX ATA
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceled	Line
Disconnect on Broken Connection	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	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	250

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

Parameter	Value
Profile ID	3
Allowed Coders Mode	Restriction (lists Allowed Coders first and then original coders in received SDP offer)
Fax Coders Group ID	Coders Group 4
FAX Behavior	Handle on re-INVITE

Figure 4-20: Configuring IP Profile for Fax supporting ATA – SBC Tab

Common GW SBC	
Index	3
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	None
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
SBC Media Security Behavior	As Is
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	Coders Group 4
Fax Behavior	Handle on re-INVITE
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported
Remote REFER Behavior	Regular
Remote 3xx Behavior	Transparent
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
Enforce MKI Size	Don't enforce
Remote Early Media RTP Behavior	Immediate
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Transparent
Remote Replaces Behavior	Transparent
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Don't Care
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

4.7 Step 7: Configure Coders

This step shows how to configure coders (termed *Coder Group*). As Lync Server 2013 supports the G.711 coder while the network connection to Verizon SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the Verizon SIP Trunk.

Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 45).

➤ **To configure coders:**

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

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

Figure 4-21: Configuring Coder Group for Lync Server 2013

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

3. Configure a Coder Group for Verizon SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	G.729 G.711 U-law G.711 A-law

Figure 4-22: Configuring Coder Group for Verizon SIP Trunk

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729	20	8	18	Disabled
G.711U-law	20	64	0	Disabled
G.711A-law	20	64	8	Disabled

4. Configure a Coder Group for the FAX supporting ATA:

Parameter	Value
Coder Group ID	4
Coder Name	T.38

Figure 4-23: Configuring Coder Group for the FAX Supporting ATA



Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
T.38	N/A	N/A	N/A	N/A

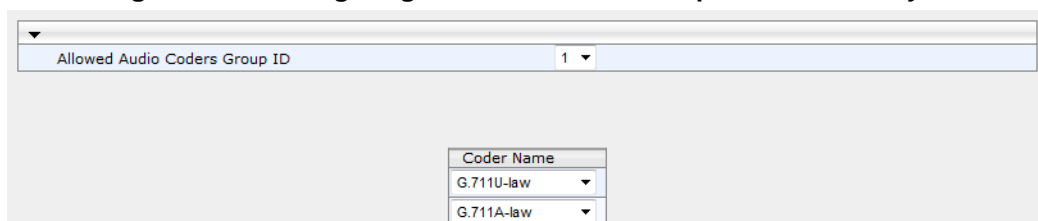
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Verizon SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Verizon SIP Trunk in the previous step (see Section 4.6 on page 45).

- **To set a preferred coder for Microsoft Lync:**

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

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

Figure 4-24: Configuring Allowed Coders Group for Microsoft Lync



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

3. Configure an Allowed Coder as follows:

Parameter	Value
Allowed Coders Group ID	2
Coder Name	G.729 G.711 U-law G.711 A-law

Figure 4-25: Configuring Allowed Coders Group for Verizon SIP Trunk

Allowed Audio Coders Group ID
2

Coder Name
G.729
G.711U-law
G.711A-law

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

Figure 4-26: SBC Preferences Mode

Transcoding Mode	Only If Required
No Answer Timeout [sec]	600
GRUU Mode	As Proxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
BYE Authentication	Disable
User Registration Time [sec]	0
Proxy Registration Time [sec]	0
Survivability Registration Time [sec]	0
Forking Handling Mode	Sequential
Unclassified Calls	Reject
Session-Expires [sec]	180
Direct Media	Disable
Preferences Mode	Include Extensions
User Registration Grace Time [sec]	0
Fax Detection Timeout [sec]	10
Max Forwards Limit	70
SBC Enable Subscribe Trying	Disable
RTCP Mode	Transparent

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

4.8 Step 8: Configure a SIP TLS Connection

This section shows 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.

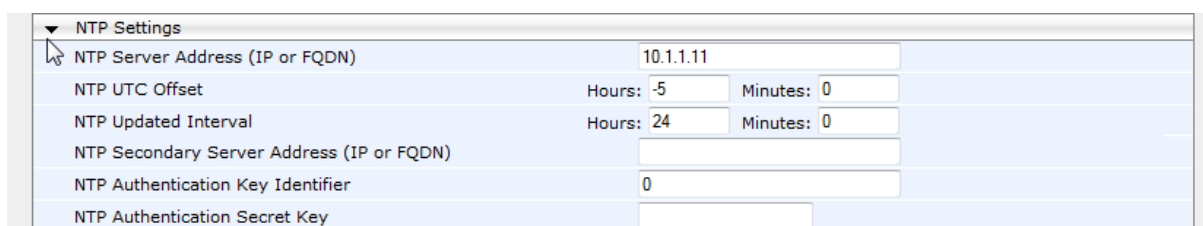
4.8.1 Step 8a: Configure the NTP Server Address

This step shows 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., **10.1.1.11**).

Figure 4-27: Configuring NTP Server Address



NTP Settings		
NTP Server Address (IP or FQDN)	10.1.1.11	
NTP UTC Offset	Hours: -5	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 shows 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.

Follow these main steps:

- Generate a Certificate Signing Request (CSR).
- Request a Device Certificate from CA.
- Obtain a Trusted Root Certificate from CA.
- Deploy Device and Trusted Root Certificates on the E-SBC.

➤ **To configure a certificate:**

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

Figure 4-28: 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-----
MIIBXzCBYQIBADAgMR4wHAYDVQQDExVJVFNQLUdXLmlseW5jMTUubG9jYWwWZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKkobC9QmE0XA0vaTrkioon0LVrwNsC1
3TMgncMVxdp9/BCXyygT2W1vz0NGUstypa7w2DKKkxr8x8A9sGLXwy0ZCyB49U1pDF
DJV8IldUfT8qL9d9V64f3z004I1hweZSn4hHdAfGy0S6e91JhFw/USUD6/bNygQz
5Z203jtjXKmdAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBqBLqe880JGrmEzPu5Q1
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**).

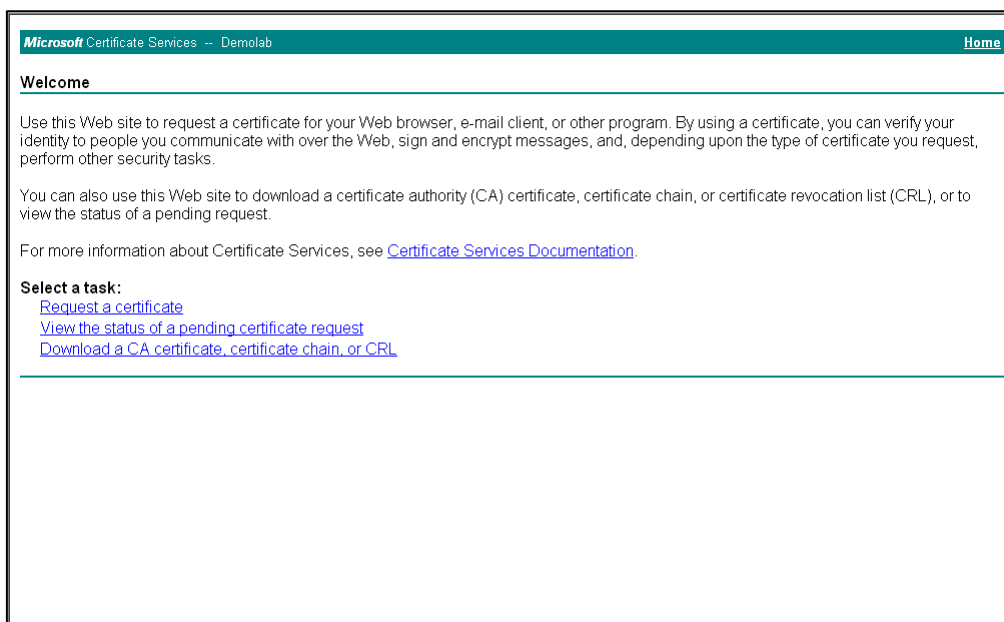


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13).

- 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*.

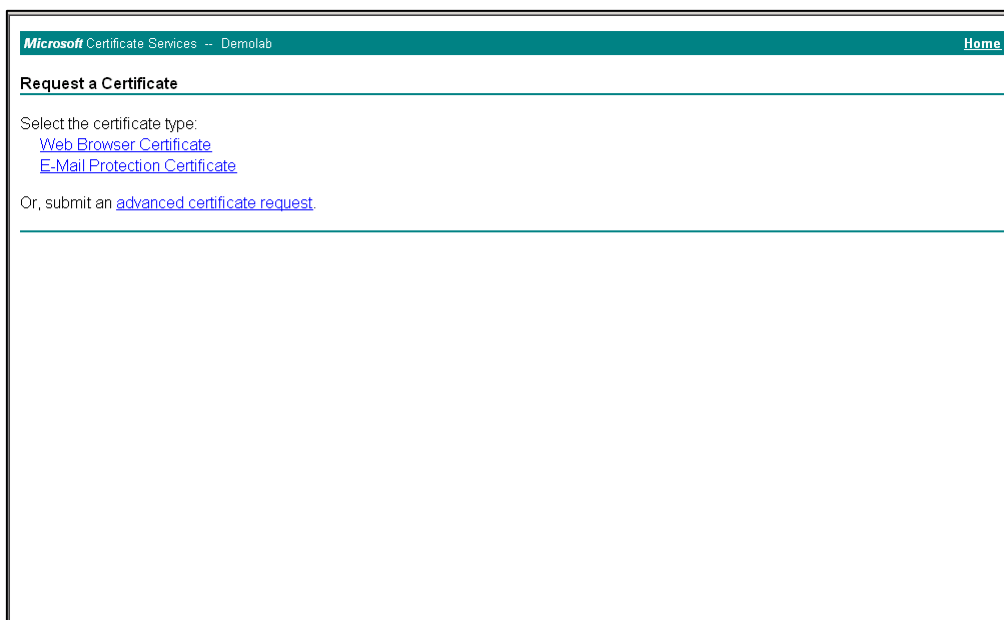
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at <http://<certificate server>/CertSrv>.

Figure 4-29: Microsoft Certificate Services Web Page



6. Click **Request a certificate**.

Figure 4-30: Request a Certificate Page



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

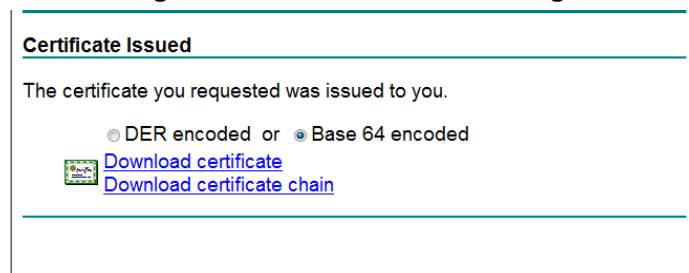
Figure 4-31: Advanced Certificate Request Page

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

Figure 4-32: Submit a Certificate Request or Renewal Request Page

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 4-33: Certificate Issued Page



Certificate Issued

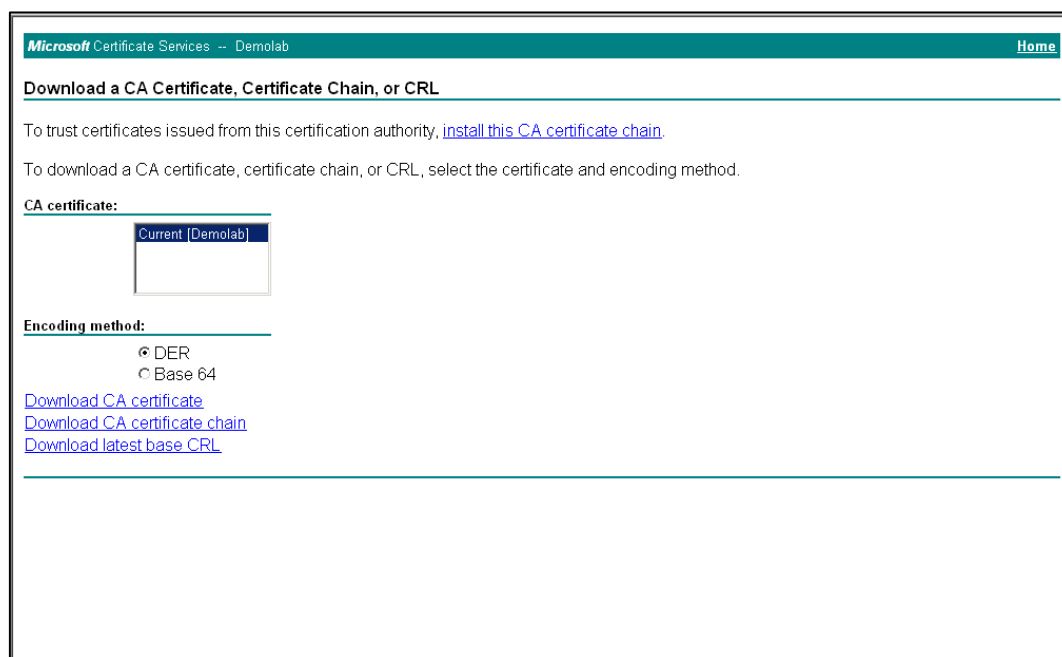
The certificate you requested was issued to you.

☐ 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 4-34: Download a CA Certificate, Certificate Chain, or CRL Page



Microsoft Certificate Services -- Demolab Home

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Current [Demolab]

Encoding method:

☒ DER
☐ Base 64

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

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

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

Figure 4-35: Certificates Page (Uploading Certificate)

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

- Private Key:** A text input field with the value "audc" and a label "Private key pass-phrase (optional)". Below it, instructions state: "Send **Private Key** file from your computer to the device. The file must be in either PEM or PFX (PKCS#12) format." There are "Browse..." and "Send File" buttons.
- Device Certificate:** Instructions state: "Send **Device Certificate** file from your computer to the device. The file must be in textual PEM format." There are "Browse..." and "Send File" buttons.
- Trusted Root Certificate Store:** Instructions state: "Send **Trusted Root Certificate Store** file from your computer to the device. The file must be in textual PEM format." There are "Browse..." and "Send File" buttons.

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

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 98).

4.9 Step 9: Configure SRTP

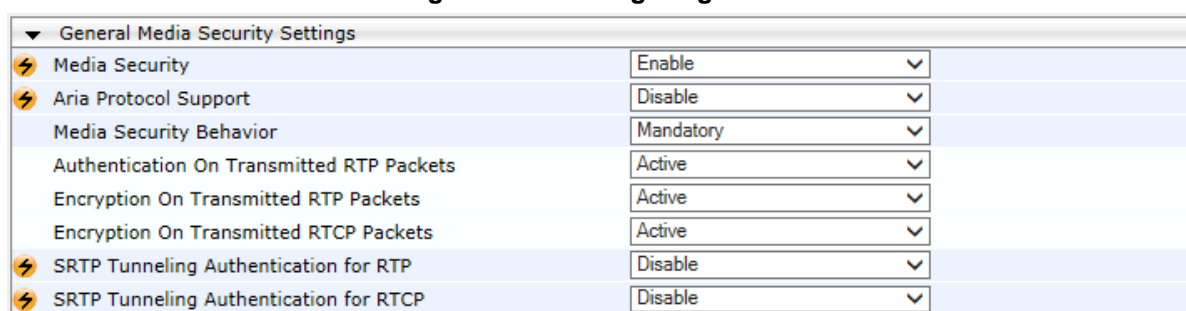
This step shows how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you must configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 45).

➤ **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 4-36: 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 98).

4.10 Step 10: Configure Maximum IP Media Channels

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



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

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

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

Figure 4-37: Configuring Number of IP Media Channels

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

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 98).

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

This step shows 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 43, IP Group 1 represents Lync Server 2013, and IP Group 2 represents Verizon SIP Trunk.

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

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to Verizon SIP Trunk
- Calls from Verizon SIP Trunk to Lync Server 2013
- Calls from Verizon SIP Trunk to Fax supporting ATA
- Calls from Fax supporting ATA to Verizon SIP trunk

➤ 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:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

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

Rule	Action
Index	0
Route Name	
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
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

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

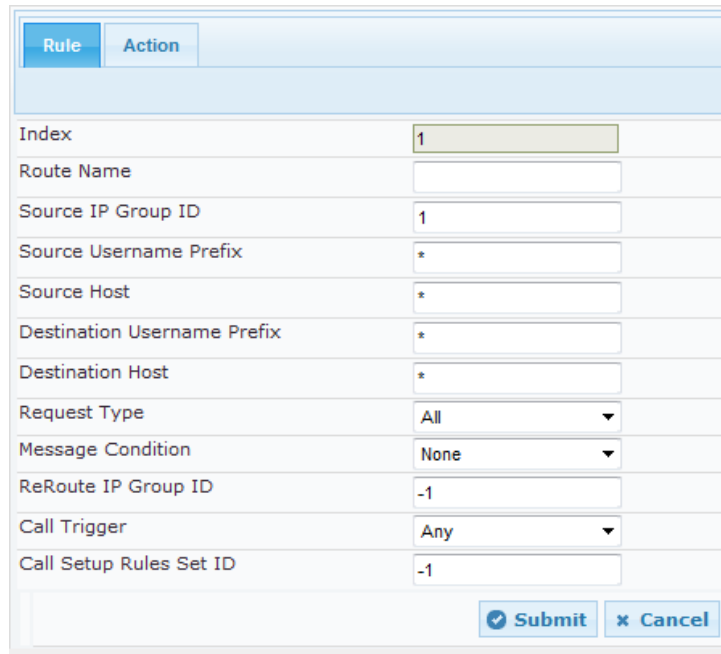
Rule	Action
Index	0
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

4. Click the **Submit** button.

5. Configure a rule to route calls from Lync Server 2013 to Verizon SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	Arbitrary descriptive name
Source IP Group ID	1

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



Parameter	Value
Index	1
Route Name	
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

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

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

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

The screenshot shows a configuration window with two tabs: 'Rule' and 'Action'. The 'Action' tab is selected. Below the tabs is a form with the following fields and values:

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

At the bottom right of the form are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

7. Click the **Submit** button.

8. Configure a rule to route calls from Verizon SIP Trunk to Fax supporting ATA:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	SIPtrunk2fax (arbitrary descriptive name)
Source IP Group ID	2
Destination Username Prefix	4089908837

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

Rule

Action

Index

2

Route Name

SIP trunk2fax

Source IP Group ID

2

Source Username Prefix

*

Source Host

*

Destination Username Prefix

4089908837

Destination Host

*

Request Type

All

Message Condition

None

ReRoute IP Group ID

-1

Call Trigger

Any

Call Setup Rules Set ID

-1

Submit

Cancel

9. 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	1

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

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

Index	2
Destination Type	IP Group
Destination IP Group ID	3
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None

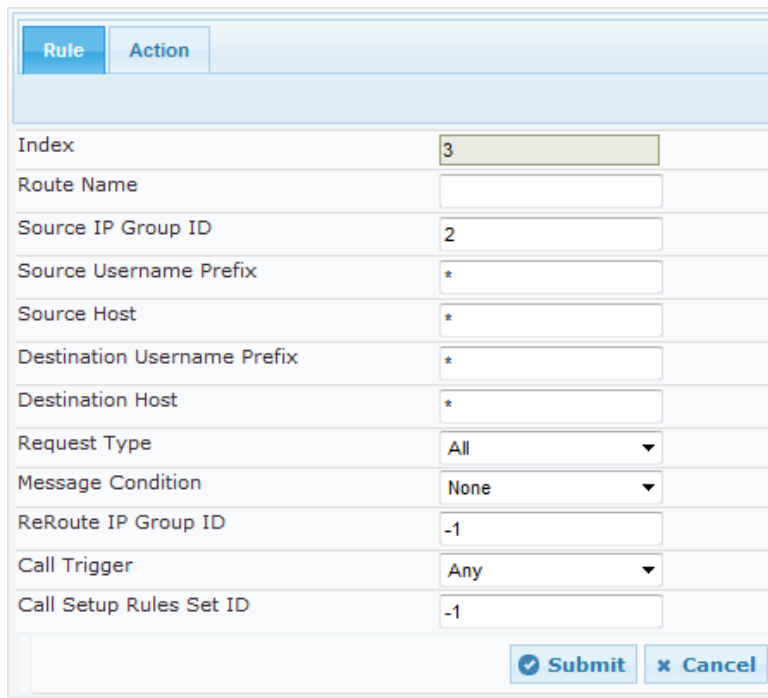
At the bottom right, there are two buttons: 'Submit' and 'Cancel'.

10. Click the **Submit** button.

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

Parameter	Value
Index	3
Route Name	Arbitrary descriptive name
Source IP Group ID	2

Figure 4-44: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab



Parameter	Value
Index	3
Route Name	
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

Submit Cancel

12. 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 4-45: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab

The screenshot shows a configuration window with two tabs: 'Rule' and 'Action'. The 'Action' tab is selected. Below the tabs are several configuration fields:

- Index: 3
- Destination Type: IP Group
- Destination IP Group ID: 1
- Destination SRD ID: 1
- Destination Address: (empty)
- Destination Port: 0
- Destination Transport Type: (empty)
- Alternative Route Options: Route Row
- Group Policy: None
- Cost Group: None

At the bottom right, there are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

13. Click the **Submit** button.

14. Configure a rule to route calls from Fax ATA to Verizon SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	4
Route Name	ata fax (arbitrary descriptive name)
Source IP Group ID	3

Figure 4-46: Configuring IP-to-IP Routing Rule for FAX ATA to ITSP Trunk – Rule tab

Rule

Action

Index

4

Route Name

ata fax

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

Submit

Cancel

15. 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 4-47: Configuring IP-to-IP Routing Rule for FAX ATA to ITSP Trunk – Action tab

16. Click the **Submit** button.

The configured routing rules are shown in the figure below:

Figure 4-48: 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		*	*	*	None	-1	Any	-1	Dest Address	None	
1		*	*	*	None	-1	Any	-1	IP Group	None	
2	SIP trunk2fax	*	4089908837	*	None	-1	Any	-1	IP Group	1	
3		*	*	*	None	-1	Any	-1	IP Group	None	
4	ata fax	*	*	*	None	-1	Any	-1	IP Group	2	

Page 1 of 1 Show 10 records per page View 1 - 5 of 5



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

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

This step shows 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 43, IP Group 1 represents Lync Server 2013, and IP Group 2 represents Verizon SIP Trunk. These manipulations can be utilized on the incoming message and/or the outgoing message.



Note: Adapt the manipulation table according to your environment's dial plan.

For this interoperability test topology, a set of normalization manipulation rules are configured to remove the '+1' from the Source and Destination numbers presented by Microsoft Lync. These were performed in the IP-to-IP Inbound manipulation rules. While using a set of IP-to-IP Outbound manipulation rules, add the "+" (plus sign) to the destination number for calls from IP Group 2 (Verizon SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

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

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

Parameter	Value
Index	1
Source IP Group	1
Source Username Prefix	+1
Destination Username Prefix	* (asterisk sign)
Manipulated URI	Source

Figure 4-49: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Rule	Action
Index	1
Manipulation Name	
Additional Manipulation	No
Manipulation Purpose	Normal
Source IP Group ID	1
Source Username Prefix	+1
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Manipulated URI	Source
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Parameter	Value
Remove From Left	2 (this removes the '+1')

Figure 4-50: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

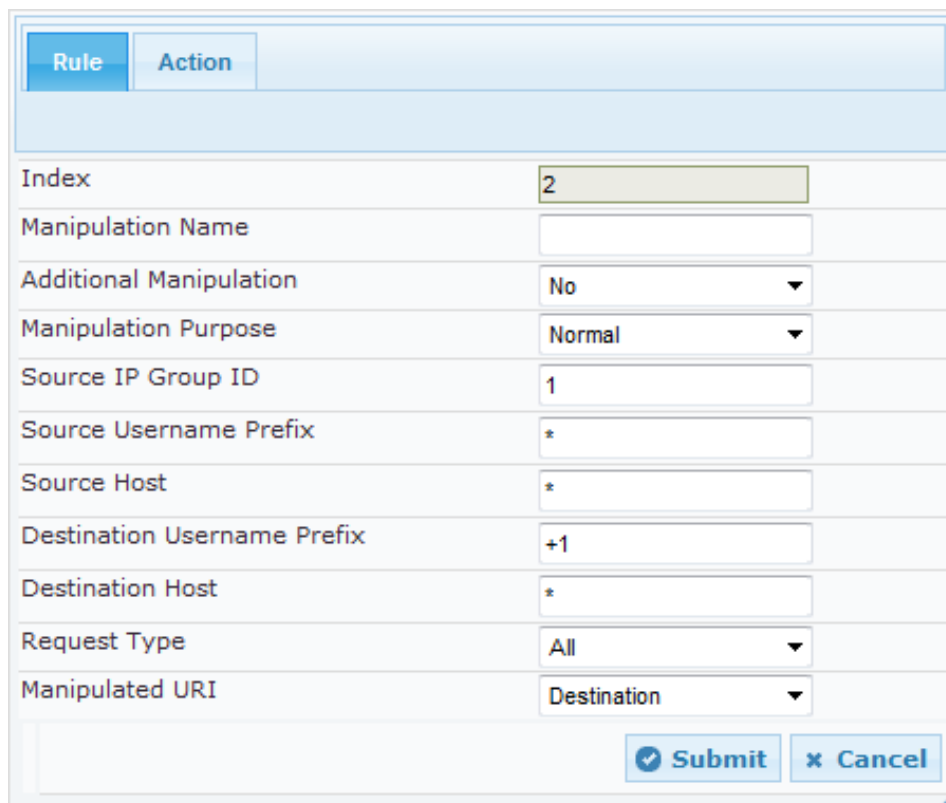
Rule	Action
Index	1
Remove From Left	2
Remove From Right	0
Leave From Right	255
Prefix to Add	
Suffix to Add	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

5. Click **Submit**.
 6. Click **Add**.

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

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

Figure 4-51: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



Parameter	Value
Index	2
Manipulation Name	
Additional Manipulation	No
Manipulation Purpose	Normal
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	+1
Destination Host	*
Request Type	All
Manipulated URI	Destination

Submit Cancel

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

Parameter	Value
Remove From Left	2 (this removes the '+1')

Figure 4-52: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

9. Click **Submit**.

The figure below shows an example of configured IP-to-IP inbound manipulation rules for calls from IP Group 1 (i.e., Lync Server 2013):

Figure 4-53: Example of Configured IP-to-IP Inbound Manipulation Rules

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

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

Rule Index	Description
1	Calls from IP Group 1 with a source number that contains a prefix of '+1' and with any destination number (*), remove the "+1" from the prefix of the source number.
2	Calls from IP Group 1 with a destination number that contains a prefix of '+1', remove "+1" from the destination number.

➤ **To configure an IP-to-IP Outbound number manipulation rule:**

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

Parameter	Value
Index	0
Source IP Group	2
Destination IP Group	1
Destination Username Prefix	* (asterisk sign)

Figure 4-54: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Rule

Action

Index

0

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	+1 (plus sign)

Figure 4-55: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

The screenshot shows a configuration window with two tabs: 'Rule' and 'Action'. The 'Action' tab is selected. The configuration fields are as follows:

Index	0
Manipulated Item	Destination URI
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+1
Suffix to Add	
Privacy Restriction Mode	Transparent

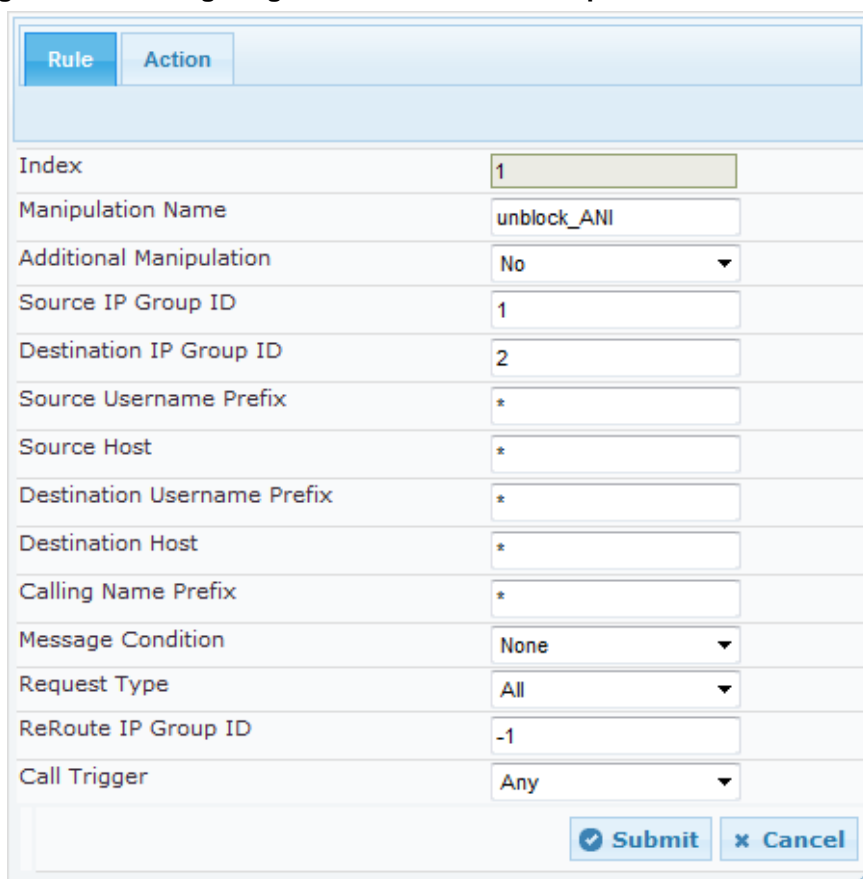
At the bottom right, there are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

5. Click **Submit**.
6. Click **Add**.

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

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

Figure 4-56: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



Parameter	Value
Index	1
Manipulation Name	unblock_ANI
Additional Manipulation	No
Source IP Group ID	1
Destination IP Group ID	2
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

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

Parameter	Value
Manipulated Item	Source URI
Privacy Restriction Mode	Remove Restriction

Figure 4-57: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

9. Click **Submit**.

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

Figure 4-58: 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	Destination Host	Request Type	Manipulated Item	Prefix to Add	Suffix to Add
0		No	2	1	*	*	*	*	All	Destination +1		
1	unblock_ANI	No	1	2	*	*	*	*	All	Source URI		

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

Rule Index	Description
0	Calls from IP Group 2 to IP Group 1 with any destination number (*), add "+1" to the prefix of the destination number.
1	Calls from IP Group 1 to IP Group 2 change the Privacy Restriction to allow presentation.

4.13 Step 13: Configure Message Manipulation Rules

This step shows 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).

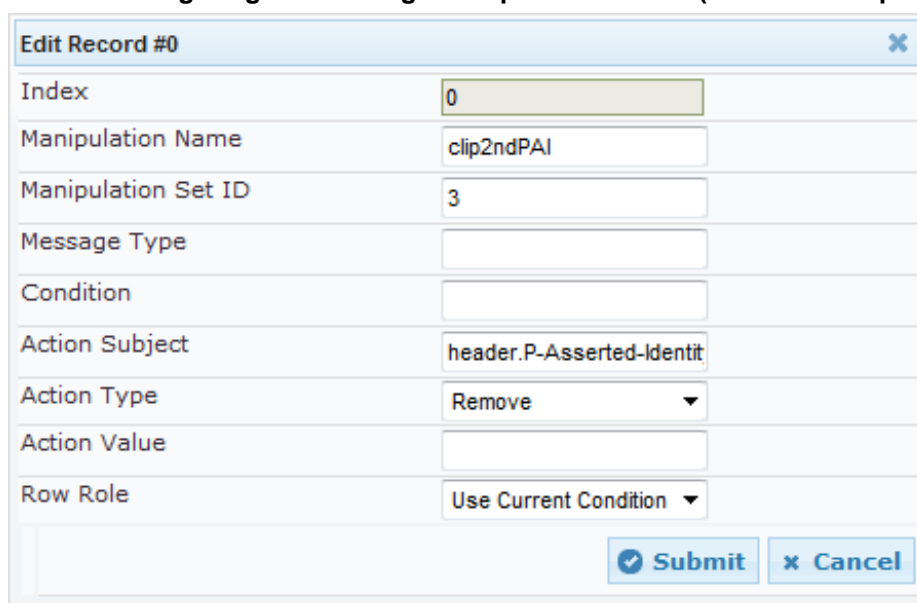
After configuring SIP message manipulation rules, you must assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Select **Add +**
3. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), calls initiated by the Lync Server 2013 (IP Group 1) which contain a long PAI. The SBC separates the P-Asserted Identity header into 2 separate PAI headers. This removes the second P-Asserted Identity header on the outgoing message towards the Verizon SIP Trunk.

Parameter	Value
Index	0
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Action Subject	header.P-Asserted-Identity.1
Action Type	Remove

Figure 4-59: Configuring SIP Message Manipulation Rule 0 (for Verizon Sip Trunk)



Edit Record #0

Index	0
Manipulation Name	clip2ndPAI
Manipulation Set ID	3
Message Type	
Condition	
Action Subject	header.P-Asserted-Identit
Action Type	Remove
Action Value	
Row Role	Use Current Condition

Submit
Cancel

4. Select **Add +**
5. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), for calls initiated by the Lync Server 2013 (IP Group 1) with the url type of 'Tel' rather than 'Sip'. This converts the header type for proper interworking towards the Verizon SIP Trunk.

Parameter	Value
Index	1
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	invite
Action Subject	header.P-Asserted-Identity.url.type
Action Type	Modify
Action Value	'1'

Figure 4-60: Configuring SIP Message Manipulation Rule 1 (for Verizon SIP Trunk)

The screenshot shows a web-based configuration interface for a SIP message manipulation rule. The window is titled 'Edit Record #1' and contains several input fields and dropdown menus. The fields are as follows:

- Index:** A text box containing the value '1'.
- Manipulation Name:** A text box containing the value 'pai sip'.
- Manipulation Set ID:** A text box containing the value '3'.
- Message Type:** A text box containing the value 'invite'.
- Condition:** An empty text box.
- Action Subject:** A text box containing the value 'header.P-Asserted-Identit'.
- Action Type:** A dropdown menu with 'Modify' selected.
- Action Value:** A text box containing the value ''1''.
- Row Role:** A dropdown menu with 'Use Current Condition' selected.

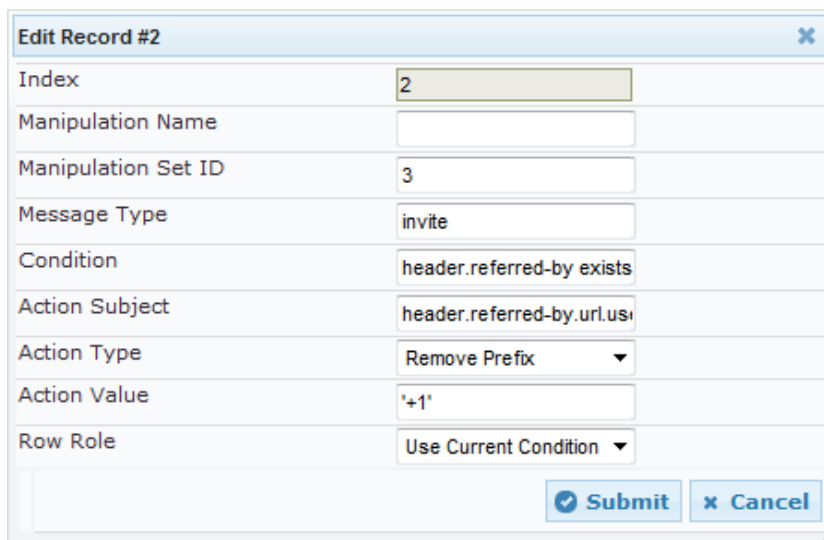
At the bottom right of the dialog are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

6. Click the **Submit** button.

7. Select **Add +**
8. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), for calls initiated by the Lync Server 2013 (IP Group 1) that include a referred-by header. This modifying Action Value modifies the Referred-By header, causing the E-SBC to remove the '+1' prefix from the Referred-By Header, if the Referred-By header exists.

Parameter	Value
Index	2
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	Invite
Condition	header.referred-by exists
Action Subject	header.referred-by.url.user
Action Type	Remove Prefix
Action Value	'+1'

Figure 4-61: Configuring SIP Message Manipulation Rule 2 (for Verizon SIP Trunk)



Edit Record #2

Index	2
Manipulation Name	
Manipulation Set ID	3
Message Type	invite
Condition	header.referred-by exists
Action Subject	header.referred-by.url.usi
Action Type	Remove Prefix
Action Value	'+1'
Row Role	Use Current Condition

Submit
Cancel

9. Click the **Submit** button.

10. Select **Add +**
11. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), when an invite containing a referred-by header is initiated by the Lync Server 2013 (IP Group 1). This adds an Action Value to add a Diversion header containing that which was received within the Referred-By header, that causing the E-SBC to add a Diversion Header towards the SIP Trunk.

Parameter	Value
Index	3
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	Invite
Condition	header.referred-by exists
Action Subject	header.diversion
Action Type	Add
Action Value	header.referred-by

Figure 4-62: Configuring SIP Message Manipulation Rule 3 (for Verizon SIP Trunk)

The screenshot shows a web-based configuration interface titled "Edit Record #3". It contains the following fields and values:

- Index: 3
- Manipulation Name: referred-by
- Manipulation Set ID: 3
- Message Type: invite
- Condition: header.referred-by exists
- Action Subject: header.diversion
- Action Type: Add (selected from a dropdown)
- Action Value: header.referred-by
- Row Role: Use Current Condition (selected from a dropdown)

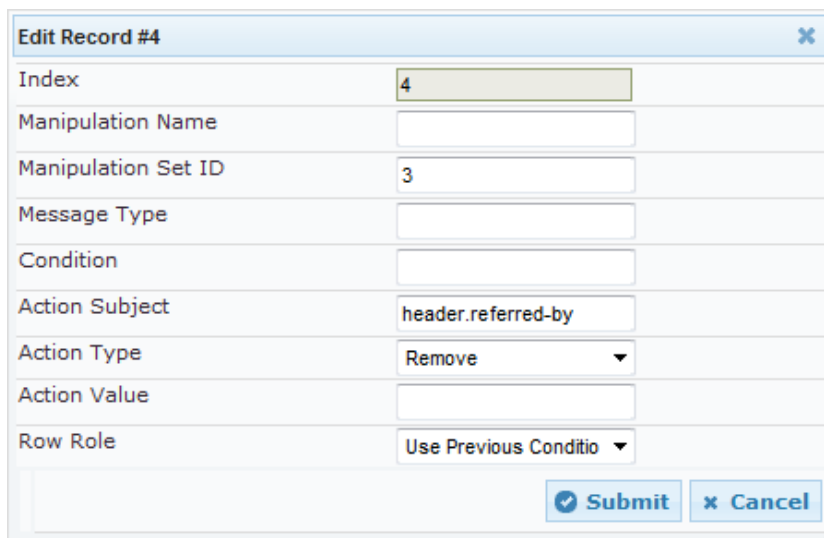
At the bottom right, there are two buttons: "Submit" (with a checkmark icon) and "Cancel" (with an 'x' icon).

12. Click the **Submit** button.

13. Select **Add +**
14. Configure a new rule as an extension manipulation rule to the previous rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), only if the previous rule was also applied. This removes the referred_by header from the outgoing invite towards the SIP Trunk.

Parameter	Value
Index	4
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Action Subject	header.referred-by
Action Type	Remove
Row Rule	Use Previous Rule

Figure 4-63: Configuring SIP Message Manipulation Rule 4 (for Verizon SIP Trunk)



Edit Record #4

Index	4
Manipulation Name	
Manipulation Set ID	3
Message Type	
Condition	
Action Subject	header.referred-by
Action Type	Remove
Action Value	
Row Role	Use Previous Condition

15. Click the **Submit** button.

16. Select **Add +**
17. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), for PSTN originated call being forwarded back to the PSTN initiated by the Lync Server 2013 (IP Group 1). This removes a prefix Action Value containing '+1' from the Diversion header, causing the E-SBC to manipulate the Diversion Header towards the SIP Trunk.

Parameter	Value
Index	5
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	Invite
Condition	header.diversion exists
Action Subject	header.diversion.url.user
Action Type	Remove Prefix
Action Value	'+1'

Figure 4-64: Configuring SIP Message Manipulation Rule 5 (for Verizon SIP Trunk)

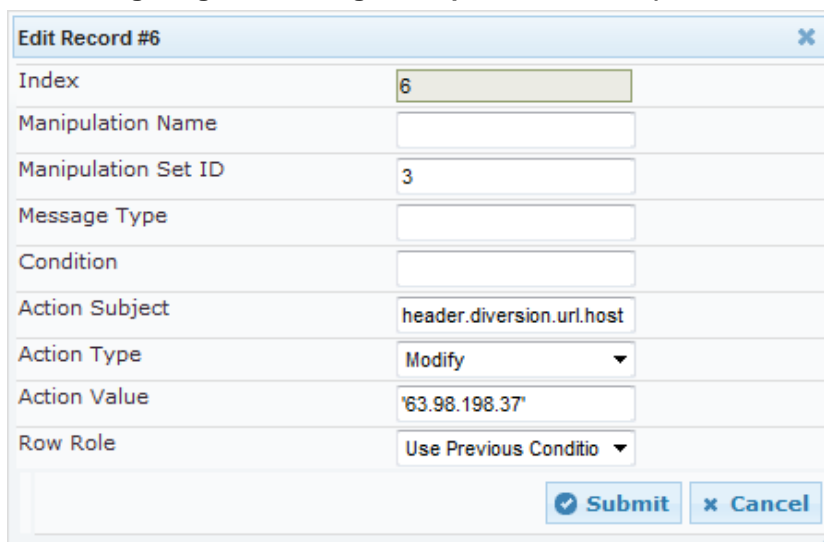
The screenshot shows a web-based configuration interface for a SIP message manipulation rule. The window is titled 'Edit Record #5'. It contains several input fields and dropdown menus. The 'Index' field is set to 5. The 'Manipulation Name' field contains the text 'forward offnet'. The 'Manipulation Set ID' field is set to 3. The 'Message Type' dropdown is set to 'Invite'. The 'Condition' dropdown is set to 'header.diversion exists'. The 'Action Subject' dropdown is set to 'header.diversion.url.user'. The 'Action Type' dropdown is set to 'Remove Prefix'. The 'Action Value' field contains the text '+1'. The 'Row Role' dropdown is set to 'Use Current Condition'. At the bottom right of the dialog are two buttons: 'Submit' and 'Cancel'.

18. Click the **Submit** button.

19. Select **Add +**
20. Configure a new manipulation rule as a continuation rule to the previous rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies only if the previous rule was applied. This modifies an Action Value to change the URL host of the outgoing Diversion header to reflect that of the E-SBC host towards the SIP Trunk.

Parameter	Value
Index	6
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Action Subject	header.diversion.url.host
Action Type	Modify
Action Value	'63.98.198.37'
Row Rule	User Previous Condition

Figure 4-65: Configuring SIP Message Manipulation Rule 6 (for Verizon SIP Trunk)



Edit Record #6

Index: 6

Manipulation Name:

Manipulation Set ID: 3

Message Type:

Condition:

Action Subject: header.diversion.url.host

Action Type: Modify

Action Value: '63.98.198.37'

Row Role: Use Previous Condition

Submit Cancel

21. Click the **Submit** button.

22. Select **Add +**
23. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), for calls initiated by the Lync Server 2013 (IP Group 1). This modifies an Action Value of the From header, causing the E-SBC to remove the 'phone-context=enterprise' from the From Header towards the SIP Trunk.

Parameter	Value
Index	7
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	invite
Condition	header.from regex (.*)(;phone-context=enterprise)(.*)
Action Subject	header.from
Action Type	Modify
Action Value	\$1+\$3

Figure 4-66: Configuring SIP Message Manipulation Rule 7 (for Verizon SIP Trunk)

Edit Record #7

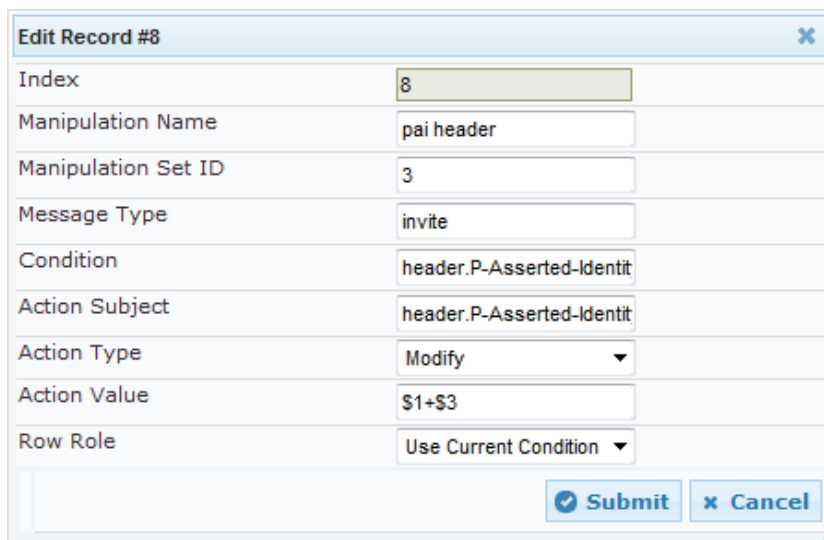
Index	7
Manipulation Name	from header
Manipulation Set ID	3
Message Type	invite
Condition	header.from regex (.*)(;phone-context=enterprise)(.)
Action Subject	header.from
Action Type	Modify
Action Value	\$1+\$3
Row Role	Use Current Condition

24. Click the **Submit** button.

25. Select **Add +**
26. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), for calls initiated by the Lync Server 2013 (IP Group 1). This modifies an Action Value of the P-Asserted-Identity header, causing the E-SBC to remove the 'phone-context=enterprise' from the P-Asserted-Identity Header towards the SIP Trunk.

Parameter	Value
Index	8
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	invite
Condition	header.P-Asserted-Identity regex (.*) (;phone-context=enterprise)(.*)
Action Subject	header.P-Asserted-Identity
Action Type	Modify
Action Value	\$1+\$3

Figure 4-67: Configuring SIP Message Manipulation Rule 8 (for Verizon SIP Trunk)



Edit Record #8	
Index	8
Manipulation Name	pai header
Manipulation Set ID	3
Message Type	invite
Condition	header.P-Asserted-Identity
Action Subject	header.P-Asserted-Identity
Action Type	Modify
Action Value	\$1+\$3
Row Role	Use Current Condition
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

27. Click the **Submit** button.

28. Select **Add +**
29. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), for conference bridge initiated calls to add a PSTN user by the Lync Server 2013 (IP Group 1). This modifying Action Value modifies the From header into a format which the Verizon SIP Trunk accepts as the invite is sent towards the SIP Trunk.

Parameter	Value
Index	9
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	3
Message Type	Invite
Condition	header.from regex (.*)(user=phone)(.*)>(;tag=)(.*)<
Action Subject	header.from
Action Type	Modify
Action Value	\$1+\$2+\$4+\$5+\$6

Figure 4-68: Configuring SIP Message Manipulation Rule 9 (for Verizon SIP Trunk)

Edit Record #9

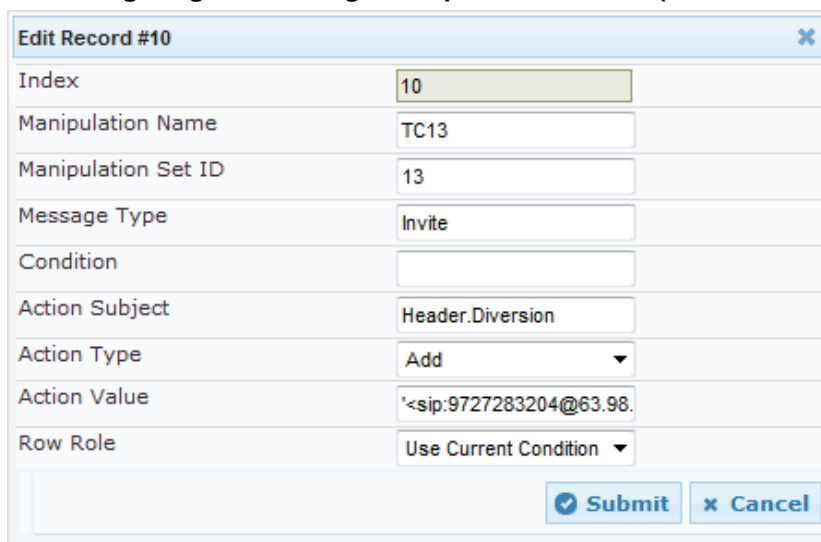
Index	9
Manipulation Name	conf add pstn
Manipulation Set ID	3
Message Type	Invite
Condition	header.from regex (.*)(user=phone)(.*)>(;tag=)(.*)<
Action Subject	header.from
Action Type	Modify
Action Value	\$1+\$2+\$4+\$5+\$6
Row Role	Use Current Condition

30. Click the **Submit** button.

31. Select **Add +**
32. Configure a new manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to Invite messages being sent to the Verizon SIP trunk (IP Group 2), when Unscreened ANI Delivery is required for calls initiated by the Lync Server 2013 (IP Group 1). This adds an Action Value to include an Unscreened ANI to be delivered within a Diversion header towards the SIP Trunk.

Parameter	Value
Index	10
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	13 (set to 3 if required, otherwise it will not be used if not associated)
Message Type	invite
Condition	header.history-info.0==regex(<.*)(user=phone)(>)(.*)
Action Subject	Header.Diversion
Action Type	Add
Action Value	'<sip:9727283204@63.98.198.37>;reason=unknown;privacy="off"'

Figure 4-69: Configuring SIP Message Manipulation Rule 10 (for Verizon SIP Trunk)



Edit Record #10	
Index	10
Manipulation Name	TC13
Manipulation Set ID	13
Message Type	Invite
Condition	
Action Subject	Header.Diversion
Action Type	Add
Action Value	'<sip:9727283204@63.98.198.37>;reason=unknown;privacy="off"'
Row Role	Use Current Condition
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

33. Click the **Submit** button.

34. Configure another manipulation rule (Manipulation Set 3) for Verizon SIP Trunk. This rule applies to messages being sent to the Verizon SIP trunk (IP Group 2), when Unscreened ANI Delivery is required for calls initiated by the Lync Server 2013 (IP Group 1). This adds an Action Value to include an Unscreened ANI to be delivered within a P-Asserted-Identity header towards the SIP Trunk.

Parameter	Value
Index	11
Manipulation Name	Arbitrary descriptive name
Manipulation Set ID	13 (set to 3 if required, otherwise it will not be used if not associated)
Action Subject	header.P-Asserted-Identity.url.user
Action Type	Modify
Action Value	'9727283204'

Figure 4-70: Configuring SIP Message Manipulation Rule 11 (for Verizon SIP Trunk)

The screenshot shows a web-based configuration interface for SIP Message Manipulation rules. The 'Edit Record #11' dialog is open, displaying the following configuration details:

- Index:** 11
- Manipulation Name:** TC14
- Manipulation Set ID:** 13
- Message Type:** (empty field)
- Condition:** (empty field)
- Action Subject:** header.P-Asserted-Identity
- Action Type:** Modify (dropdown menu)
- Action Value:** '9727283204'
- Row Role:** Use Current Condition (dropdown menu)

At the bottom right of the dialog, there are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

35. Click the **Submit** button.

Figure 4-71 shows an example of configured SIP Message Manipulation rules.

Figure 4-71: Example of Configured SIP Message Manipulation Rules

Message Manipulations							
Add +		Insert +					
Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	clip2ndPAI	3			header.P-Asserted-Id	Remove	
1	pai sip	3	invite		header.P-Asserted-Id	Modify	'1'
2		3	invite	header.referred-by e	header.referred-by.u	Remove Prefix	'+'
3	referred-by	3	invite	header.referred-by e	header.diversion	Add	header.referred-by
4		3			header.referred-by	Remove	
5	forward offnet	3	Invite	header.diversion exis	header.diversion.url.i	Remove Prefix	'+'
6		3			header.diversion.url.i	Modify	'63.98.198.37'
7	from header	3	invite	header.from regex (.	header.from	Modify	\$1+\$3
8	pai header	3	invite	header.P-Asserted-Id	header.P-Asserted-Id	Modify	\$1+\$3
9	conf add pstn	3	Invite	header.from regex (.	header.from	Modify	\$1+\$2+\$4+\$5+\$6
Page 1 of 2 Show 10 records per page View 1 - 10 of 12							

Message Manipulations							
Add +		Insert +					
Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
10	TC13	13	Invite		Header.Diversion	Add	'<sip:9727283204@63
11	TC14	13			header.P-Asserted-Id	Modify	'9727283204'
Page 2 of 2 Show 10 records per page View 11 - 12 of 12							

The table below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs which are executed for messages sent to the Verizon SIP Trunk (IP Group 2). These rules are specifically required to enable correct interworking between Verizon SIP Trunk and Lync Server 2013. The specific items are needed to support the interoperability. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Reason	Description
0	Removal of second PAI	Microsoft Lync 2013 sends a long P-Asserted-Identity which the E-SBC changes into two separate PAI headers. This rule is utilized to remove the second PAI.
1	PAI header URL type to SIP	This rule is utilized to change the URL type from 'TEL' to 'SIP' for the P-Asserted-Identity Header.
2	Remove '+1' prefix from referred-by header	Since Verizon SIP Trunk does not support "Referred-By" Header in SIP INVITE messages, the rule is needed to first modify it. To perform this, the prefix of '+1' is removed.
3	Add diversion header for transferred calls	Since Verizon SIP Trunk does not support "Referred-By" Header in SIP INVITE messages, the rule is needed to copy the contents of it to a new Diversion header.
4	Verizon SIP Trunk not supports "Referred-By" Header in SIP INVITE messages, so it is needed to remove it.	Since Verizon SIP Trunk does not support "Referred-By" Header in SIP INVITE messages, the rule is needed to remove it. To perform this rule; manipulation rule 3 must first be utilized for the Verizon SIP Trunk.

Rule Index	Reason	Description
5	Remove '+1' prefix from Diversion header	If a Diversion Header exists within an Invite message, the following rule removes prefix '+1' from the User part in Diversion Header if it is found to have this.
6	Set the URL host of the Diversion header to that of the E-SBC WAN	Rule replaces Host part in Diversion Header with value of the WAN address of the E-SBC that is recognized by the Verizon SIP Trunk. To perform this rule; manipulation rule 5 must first be utilized for the Verizon SIP Trunk.
7	From header normalization	This rule normalizes the From header by removing the ' phone-context=enterprise ' from the header.
8	P-Asserted-Identity normalization from header normalization	This rule normalizes the P-Asserted-Identity header by removing the ' phone-context=enterprise ' from the header.
9	From header normalization	This rule normalizes the From header when adding a PSTN user from a conference bridge.
10	Verizon Unscreened ANI delivery Option 1	Optional usage to insert an Unscreened ANI within a Diversion Header. To utilize this method, set the Message Manipulation ID to 3 for this rule.
11	Verizon Unscreened ANI delivery Option 2	Optional usage to insert an Unscreened ANI within a P-Asserted-Identity Header. To utilize this method, set the Message Manipulation ID to 3 for this rule.

36. Assign Manipulation Set IDs 3 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 **3**.

Figure 4-72: Assigning Manipulation Set to IP Group 2

<div>Common</div> <div>GW</div> <div>SBC</div>	
Index	<input type="text" value="2"/>
Classify By Proxy Set	<input type="text" value="Enable"/>
Max. Number of Registered Users	<input type="text" value="-1"/>
Inbound Message Manipulation Set	<input type="text" value="-1"/>
Outbound Message Manipulation Set	<input type="text" value="3"/>
Registration Mode	<input type="text" value="User Initiates Registra"/>
Authentication Mode	<input type="text" value="User Authenticates"/>
Authentication Method List	<input type="text"/>
SBC Client Forking Mode	<input type="text" value="Sequential"/>
Source URI Input	<input type="text"/>
Destination URI Input	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Msg Man User Defined String1	<input type="text"/>
Msg Man User Defined String2	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- e. Click the **Submit** button.

4.14 Step 14: Configure Miscellaneous E-SBC Settings

This section shows how to configure miscellaneous E-SBC settings.

4.14.1 Step 14a: Configure Call Forking Mode

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

➤ **To configure call forking:**

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

Figure 4-73: Configuring Forking Mode

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

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

3. Click **Submit**.

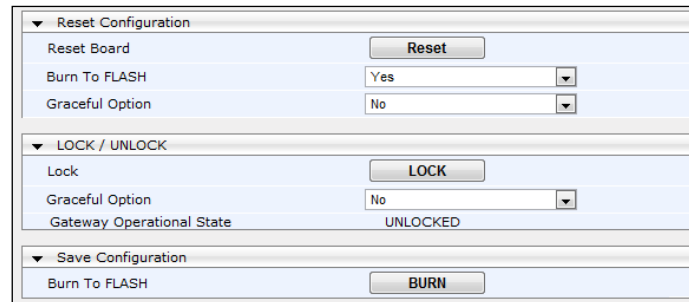
4.15 Step 15: Reset the E-SBC

After completing configuration of the E-SBC, 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 4-74: Resetting the E-SBC



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

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

A AudioCodes *ini* File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 31, is shown below:



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

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

;Board: Mediant 1000
;HW Board Type: 47  FK Board Type: 71
;Serial Number: 2967088
;Slot Number: 1
;Software Version: 6.80A.018.005
;DSP Software Version: 624AE3=> 660.10
;Board IP Address: 10.133.4.43
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.133.4.1
;Ram size: 497M  Flash size: 64M
;Num of DSP Cores: 8  Num DSP Channels: 30
;Num of physical LAN ports: 7
;Profile: NONE
;Key features:;Board Type: Mediant 1000 ;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 ;PSTN FALLBACK Supported ;E1Trunks=4 ;T1Trunks=4
;DSP Voice features: IpmDetector RTCP-XR ;Eth-Port=6 ;DATA features: ;IP Media:
Conf VoicePromptAnnounc(H248.9) TrunkTesting ;Channel Type: RTP DspCh=30
IPMediaDspCh=30 ;PSTN Protocols: IUA=4 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;Control Protocols: MSFT CLI TRANSCODING=20
TestCall=10 CODER-TRANSCODING=531 MGCP MEGACO H323 SIP TPNCP SASurvivability
SBC=120 ;Default features:;Coders: G711 G726;

;----- Mediant 1000 HW components -----
;
; Slot # : Module type : # of ports : # of DSPs
;-----
;      1 : Empty
;      2 : FALC56      :          1 :          2
;      3 : Empty
;      4 : Empty
;      5 : Empty
;      6 : Empty
;-----

[BSP Params]

PCMLawSelect = 3
BaseUDPPort = 20010
PREMIUMSERVICECLASSCONTROLDIFFSERV = 28
UdpPortSpacing = 10

[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]

CNGDetectorMode = 1
DisableRTCPRandomize = 1
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value

[SIP Params]

MEDIACHANNELS = 30
SIPDESTINATIONPORT = 5067
GWDEBUGLEVEL = 5
PROXYREDUNDANCYMODE = 1
TCPLOCALSIPPORT = 5068
TLSLOCALSIPPORT = 5067
MEDIASECURITYBEHAVIOUR = 3
FAXCNGMODE = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCMAXFORWARDSLIMIT = 70
T38FAXSESSIONIMMEDIATESTART = 1
ENABLESYMMETRICMKI = 1
SBCPREFERENCESEMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10485760

[SCTP Params]

[VXML 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_0_1", 1, 1, 4, "LAN Port#1", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 1, 4, "LAN Port#2", "GROUP_1", "Redundant";
PhysicalPortsTable 2 = "GE_7_1", 1, 2, 4, "WAN Port#1", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_7_2", 1, 2, 4, "WAN Port#2", "GROUP_2", "Redundant";
PhysicalPortsTable 4 = "GE_7_3", 1, 3, 4, "User Port #4", "GROUP_3", "Active";
PhysicalPortsTable 5 = "GE_7_4", 1, 3, 4, "User Port #5", "GROUP_3", "Redundant";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode,
EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_0_1", "GE_0_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_7_1", "GE_7_2";
EtherGroupTable 2 = "GROUP_3", 2, "GE_7_3", "GE_7_4";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID, DeviceTable_UnderlyingInterface,
DeviceTable_DeviceName;
DeviceTable 0 = 1, "GROUP_1", "vlan 1";
DeviceTable 1 = 2, "GROUP_2", "vlan 2";
DeviceTable 2 = 3, "GROUP_3", "vlan 3";

[ \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, 10.133.4.43, 16, 10.133.4.1, 1, "Voice", 10.133.4.40,
0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 63.98.198.37, 28, 63.98.198.38, 2, "Public", 198.6.1.2,
198.6.1.3, "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 1 = "MRLan", "Voice", "", 21010, 10, 21100, 1, "", "";
CpMediaRealm 2 = "MRWan", "Public", "", 20010, 10, 20100, 0, "", "";

[ \CpMediaRealm ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password, WebUsers_Status,
WebUsers_PwAgeInterval, WebUsers_SessionLimit, WebUsers_SessionTimeout,
WebUsers_BlockTime, WebUsers_UserLevel, WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$na/8r5WWlJKSnZTCnpGcz8nMnZyIhIrShtaFgYuKjt2Ej9+OpPTy9Kb896Opr/L4+qms/rHgt+u2t+H
v6rvrvu0=", 1, 0, 2, 15, 60, 200, "491d805ea8ee4c45b389866b777e9061";
WebUsers 1 = "User",
"$1$vIyE3N3zpKD2/f3z966t+K/6qff65bOx6rHl5rTvV0jTurvq79fWldWB04fTid7d2NvZj9eVw8rBxMz
Bx5rPzZg=", 1, 0, 2, 15, 60, 50, "88406e8d54c36142d8dee7d55dbc8fac";

[ \WebUsers ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "LanSRD", "MRLan", 0, 0, -1, 1;
SRD 2 = "WanSRD", "MRWan", 0, 0, -1, 1;

[ \SRD ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "63.79.179.178:5208", 0, 2;
ProxyIp 1 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 2 = "10.133.4.101:5060", 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_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport,
IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource, IpProfile_GenerateSRTPKeys,
IpProfile_SBCPlayHeldTone, IpProfile_SBCRemoteHoldFormat,
IpProfile_SBCRemoteReplacesBehavior, IpProfile_SBCSDPPTimeAnswer,
IpProfile_SBCPreferredPTime, IpProfile_SBCUseSilenceSupp,
IpProfile_SBCRTPRedundancyBehavior, IpProfile_SBCPlayRBTToTransferee,
IpProfile_SBCRTCPMode, IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection, IpProfile_JitterBufMaxDelay;
IpProfile 1 = "Microsoft Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 1,
-1, 1, 0, 1, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0, 1, "", 1, -1, 2, 1, 0, 0, 0, 0, 8,
300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1, 0, 3, 2, 1, 2, 1, 1, 1, 1, 1, 0, 1, 0,
0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 250;
IpProfile 2 = "Vzn Trunk", 1, 0, 1, 10, 10, 46, 28, 0, 0, 0, 0, 2, 0, 0, 0, 1, -1,
1, 0, 2, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 2, 2, 0, 0, 1, 0, 8,
300, 400, 1, 2, 0, 4, 2, 0, 1, 3, 0, 2, 2, 0, 3, 0, 0, 2, 1, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 250;
IpProfile 3 = "FAX ATA", 1, 0, 1, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -1, 1,
0, 3, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, 4, 2, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 250;

[ \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 = "", 1, 30, 0, 1, 1, 0, -1, -1, "";
ProxySet 2 = "", 1, 60, 0, 0, 2, 0, -1, -1, "";
ProxySet 3 = "fax ata", 0, 60, 0, 0, 1, 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, "Microsoft Lync", 1, "63.98.198.37", "", 0, -1, 0, 0, -1, 1,
"MRlan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "",
0, "", "";

```

```

IPGroup 2 = 0, "Vzn Trunk", 2, "icrcnln0002.customer08.tsengr.com", "", 0, -1, 0,
0, -1, 2, "MRWan", 1, 2, -1, -1, 3, 0, 0, "", 0, -1, -1, "", "", "$l$gQ==", 0, "",
"", "", 0, "", "";
IPGroup 3 = 0, "fax ata", 3, "63.98.198.37", "", 0, -1, -1, 0, -1, 1, "MRLan", 1,
3, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$l$gQ==", 0, "", "", "", 0, "", "";

[ \IPGroup ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName, IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress,
IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,
IP2IPRouting_AltRouteOptions, IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "", -1, "*", "*", "*", "*", 6, "", -1, 0, -1, 1, -1, "",
"internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "", 1, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 2, "2", "", 0, -1,
0, 0, "";
IP2IPRouting 2 = "SIP trunk2fax", 2, "*", "*", "4089908837", "*", 0, "", -1, 0, -1,
0, 3, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 3 = "", 2, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 1, "1", "", 0, -1,
0, 0, "";
IP2IPRouting 4 = "ata fax", 3, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 2, "2", "",
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_PreClassificationManSet;
SIPInterface 1 = "", "Voice", 2, 5060, 5068, 5067, 1, "", -1, 0, 500, -1;
SIPInterface 2 = "", "Public", 2, 5060, 0, 0, 2, "", -1, 0, 500, -1;

[ \SIPInterface ]

[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index = IPInboundManipulation_ManipulationName,
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose, IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft, IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 1 = "", 0, 0, 1, "+1", "*", "*", "*", 0, 0, 2, 0, 255, "",
"";
IPInboundManipulation 2 = "", 0, 0, 1, "*", "*", "+1", "*", 0, 1, 2, 0, 255, "",
"";

[ \IPInboundManipulation ]

[ IPOutboundManipulation ]

```



```

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

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0;

[ \CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 1;
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 1;

[ \CodersGroup1 ]

[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = "g729", 20, 0, -1, 0;
CodersGroup2 1 = "g711Ulaw64k", 20, 0, -1, 0;
CodersGroup2 2 = "g711Alaw64k", 20, 0, -1, 0;

[ \CodersGroup2 ]

[ CodersGroup4 ]

FORMAT CodersGroup4_Index = CodersGroup4_Name, CodersGroup4_pTime,
CodersGroup4_rate, CodersGroup4_PayloadType, CodersGroup4_Sce;
CodersGroup4 0 = "t38fax", 255, 255, -1, 255;

[ \CodersGroup4 ]

[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Ulaw64k";
AllowedCodersGroup1 1 = "g711Alaw64k";

[ \AllowedCodersGroup1 ]

```

```
[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
AllowedCodersGroup2 1 = "g711Ulaw64k";
AllowedCodersGroup2 2 = "g711Alaw64k";

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName,
MessageManipulations_ManSetID, MessageManipulations_MessageType,
MessageManipulations_Condition, MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 0 = "clip2ndPAI", 3, "", "", "header.P-Asserted-Identity.1",
1, "", 0;
MessageManipulations 1 = "pai sip", 3, "invite", "", "header.P-Asserted-
Identity.url.type", 2, "'1'", 0;
MessageManipulations 2 = "", 3, "invite", "header.referred-by exists",
"header.referred-by.url.user", 6, "'+1'", 0;
MessageManipulations 3 = "referred-by", 3, "invite", "header.referred-by exists",
"header.diversion", 0, "header.referred-by", 0;
MessageManipulations 4 = "", 3, "", "", "header.referred-by", 1, "", 1;
MessageManipulations 5 = "forward offnet", 3, "Invite", "header.diversion exists",
"header.diversion.url.user", 6, "'+1'", 0;
MessageManipulations 6 = "", 3, "", "", "header.diversion.url.host", 2,
"'63.98.198.37'", 1;
MessageManipulations 7 = "from header", 3, "invite", "header.from regex
(.*)(:phone-context=enterprise)(.*)", "header.from", 2, "$1+$3", 0;
MessageManipulations 8 = "pai header", 3, "invite", "header.P-Asserted-Identity
regex (.*)(:phone-context=enterprise)(.*)", "header.P-Asserted-Identity", 2,
"$1+$3", 0;
MessageManipulations 9 = "conf add pstn", 3, "Invite", "header.from regex
(.*)(user=phone)(.*)>(:tag=)(.*)", "header.from", 2, "$1+$2+$4+$5+$6", 0;
MessageManipulations 10 = "TC13", 13, "Invite", "", "Header.Diversion", 0,
''<sip:9727283204@63.98.198.37>;reason=unknown;privacy="off"''', 0;
MessageManipulations 11 = "TC14", 13, "", "", "header.P-Asserted-
Identity.url.user", 2, "'9727283204'", 0;

[ \MessageManipulations ]
```

B Configuring Analog Devices (ATAs) for Fax Support

This section shows how to configure the analog device entity to route its calls to the AudioCodes Media Gateway for supporting faxes. The analog device entity must be configured to send all calls to the Media Gateway without any registration process.

**Note:**

- The configuration described in this section is for ATA devices configured for AudioCodes MP-11x series.
- Instead of the ATA, FXS ports on devices that support FXS ports can be used.

B.1 Step 1: Configure the Endpoint Phone Number Table

The 'Endpoint Phone Number Table' page allows you to activate the MP-11x ports (endpoints) by defining telephone numbers. The configuration below uses the example of ATA destination phone number "4089908877" (IP address 10.133.4.101) with all routing directed to the AudioCodes E-SBC device (10.133.4.43).

➤ **To configure the Endpoint Phone Number table:**

- Open the 'Endpoint Phone Number Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Hunt Group** sub-menu > **Endpoint Phone Number**).

Figure B-1: Endpoint Phone Number Table Page

Endpoint Phone Number Table				
	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1	4089908837		0
2				
3				
4				

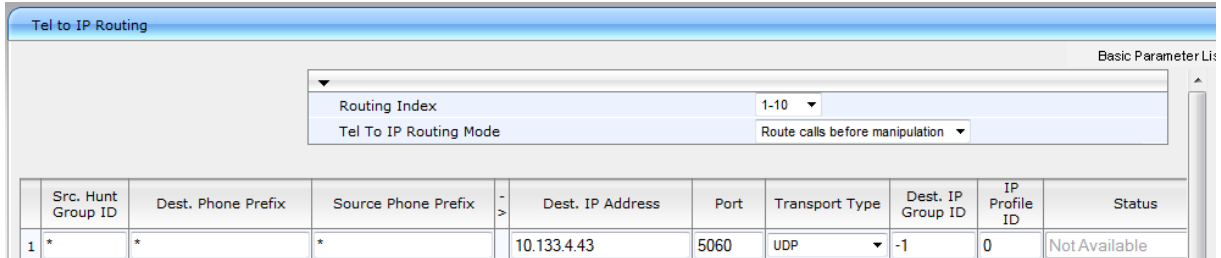
B.2 Step 2: Configure the Tel to IP Routing Table

This step shows how to configure the Tel to IP Routing rules to ensure that the MP-11x device sends all calls to the AudioCodes central E-SBC device.

➤ **To configure the Tel to IP Routing table:**

- Open the 'Tel to IP Routing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** sub-menu > **Routing** sub-menu > **Tel to IP Routing**).

Figure B-2: Tel to IP Routing Page



	Src. Hunt Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IP Group ID	IP Profile ID	Status
1	*	*	*	10.133.4.43	5060	UDP	-1	0	Not Available

B.3 Step 3: Configure the Coders Table

This step shows how to configure the coders for the MP-11x device.

➤ **To configure MP-11x coders:**

- Open the 'Coders' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** sub-menu > **Coders**).

Figure B-3: Coders Table Page

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711U-law ▼	20 ▼	64 ▼	0	Disabled ▼
▼	▼	▼		▼
▼	▼	▼		▼
▼	▼	▼		▼
▼	▼	▼		▼

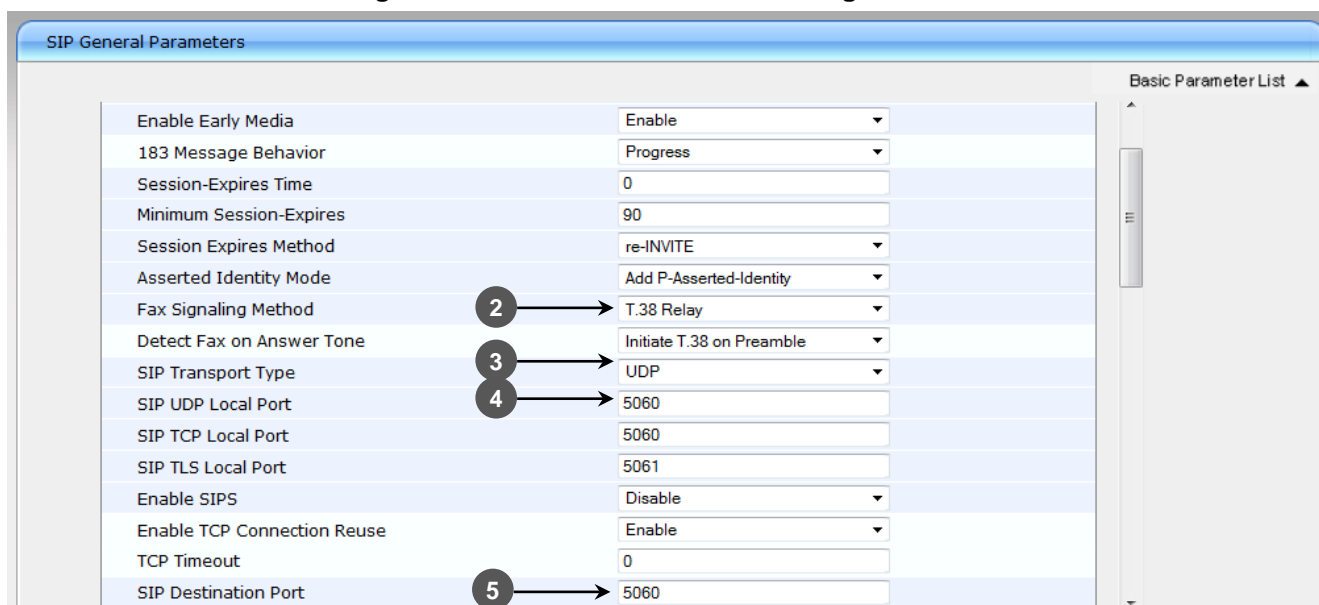
B.4 Step 4: Configure SIP UDP Transport Type and Fax Signaling Method

This step shows how to configure the fax signaling method for the MP-11x device.

➤ To configure the fax signaling method:

1. Open the 'SIP General Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).

Figure B-4: SIP General Parameters Page



Parameter	Value
Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	re-INVITE
Asserted Identity Mode	Add P-Asserted-Identity
Fax Signaling Method	T.38 Relay
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060

2. From the 'FAX Signaling Method' drop-down list, select **T.38 Relay** (or **G.711 Transport** – if G.711 is preferred).
3. From the 'SIP Transport Type' drop-down list, select **UDP**.
4. In the 'SIP UDP Local Port' field, enter **5060** (corresponding to the Central Gateway UDP transmitting port configuration).
5. In the 'SIP Destination Port', enter **5060** (corresponding to the Central Gateway UDP listening port configuration).

B.5 Step 5: Configure FAX Settings

This step shows how to configure the fax settings for the MP-11x device.

➤ To configure the fax settings:

1. Open the 'FAX/Modem/CID Settings' page (**Configuration** tab > **VoIP** menu > **Media** submenu > **FAX/Modem/CID Settings**).

Figure B-5: Fax/Modem/CID Settings Page

General Settings	
Fax Transport Mode	T.38 Relay
Caller ID Transport Type	Mute
Caller ID Type	Standard Bellcore
V.21 Modem Transport Type	Disable
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax CNG Mode	Sends on CNG tone
CNG Detector Mode	Relay

Fax Relay Settings	
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	14400bps

Submit

2. From the 'FAX Transport Mode' drop-down list, select **T.38 Relay**.
3. From the 'Fax CNG Mode' drop-down list, select **Sends on CNG tone**.

Because of interworking issues with the Verizon network, the ATA must initiate T.38 fax on both the CED as well as the CNG tone. Verizon does not initiate T.38 FAX relay within the Verizon SIP Trunking Network.



Configuration Note