

Microsoft® Lync™ and Telenet

Mediant E-SBC Series

SIP Protocol

Configuration Note

Connecting Microsoft® Lync™ and Telenet SIP Trunk using AudioCodes Mediant E-SBC Series



November 2011

Document #: LTRT-39210



Table of Contents

1	Introduction.....	9
2	Components Information.....	11
2.1	AudioCodes Gateway Version	11
2.2	Telenet SIP Trunking Version	11
2.3	Microsoft Lync Version.....	11
2.4	Topology.....	12
3	Configuring Lync Server 2010.....	13
3.1	Configuring the E-SBC device as an IP/PSTN Gateway	14
3.2	Associating the IP/PSTN Gateway with the Mediation Server	18
3.3	Configuring the Route on the Lync Server 2010.....	22
4	Configuring the E-SBC Device	29
4.1	Step 1: Configuring IP Addresses	30
4.1.1	Configuring LAN IP Addresses.....	30
4.1.1.1	Configuring VoIP IP Settings.....	30
4.1.1.2	Configuring LAN Data-Routing IP Settings	31
4.1.2	Configuring WAN IP Addresses.....	32
4.2	Step 2: Configuring Port Forwarding	33
4.3	Step 3: Enabling Application Mode.....	35
4.4	Step 4: Configuring Secure Real-Time Transport Protocol (SRTP)	36
4.5	Step 5: Configuring IP Media	37
4.6	Step 6: Configuring SIP General Parameters.....	38
4.7	Step 7: Configuring DTMF and Dialing	40
4.8	Step 8: Configuring Coders	41
4.9	Step 9: Configuring Proxy and Registration.....	42
4.10	Step 10: Configuring Proxy Sets Tables.....	43
4.11	Step 11: Configuring IP Profile	45
4.12	Step 12: Configuring IP Group Tables.....	47
4.13	Step 13: Configuring Trunk Group.....	49
4.14	Step 14: Configuring Routing	50
4.15	Step 15: Configuring Manipulation	52
4.16	Step 16: Configuring Message Manipulations	54
4.17	Step 17: Configuring SIP TLS Connection	57
4.17.1	Step 17-1: Configuring VoIP DNS Settings	57
4.17.2	Step 17-2: Configuring NTP Server	57
4.17.3	Step 17-3: Configuring a Certificate.....	58
4.18	Step 18: Resetting the Gateway.....	63
A	AudioCodes INI File.....	65

List of Figures

Figure 2-1: Topology.....	12
Figure 3-1: Opening the Lync Server Topology Builder	14
Figure 3-2: Topology Builder Options.....	14
Figure 3-3: Save Topology	15
Figure 3-4: Downloaded Topology	15
Figure 3-5: New IP/PSTN Gateway.....	16
Figure 3-6: Define New IP/PSTN Gateway	16
Figure 3-7: IP/PSTN Gateway	17
Figure 3-8: Associating Mediation Server with IP/PSTN Gateway.....	18
Figure 3-9: Before Associating IP/PSTN Gateway to Mediation Server	18
Figure 3-10: After Associating IP/PSTN Gateway to Mediation Server	19
Figure 3-11: Media Server PSTN Gateway Association Properties	19
Figure 3-12: Publishing Topology.....	20
Figure 3-13: Publish Topology Confirmation	20
Figure 3-14: Publish Topology Progress screen	21
Figure 3-15: Publish Topology Successfully Completed	21
Figure 3-16: Opening the Lync Server Control Panel	22
Figure 3-17: Lync Server Credentials.....	22
Figure 3-18: CSCP Home page.....	23
Figure 3-19: Voice Routing Option	23
Figure 3-20: Route Option	24
Figure 3-21: Adding New Voice Route	24
Figure 3-22: Adding New E-SBC Gateway.....	25
Figure 3-23: List of Deployed Gateways	25
Figure 3-24: Selected the E-SBC Gateway.....	26
Figure 3-25: Associating PSTN Usage to E-SBC Gateway	26
Figure 3-26: Confirmation of New Voice Route	27
Figure 3-27: Committing Voice Routes.....	27
Figure 3-28: Uncommitted Voice Configuration Settings	27
Figure 3-29: Voice Routing Configuration Confirmation.....	28
Figure 3-30: Voice Routing Screen Displaying Committed Routes.....	28
Figure 4-1: Web Interface Showing Basic/Full Navigation Tree Display.....	29
Figure 4-2: IP Settings	30
Figure 4-3: Connections Page	31
Figure 4-4: Defining LAN Data-Routing IP Address	31
Figure 4-5: WAN Settings.....	32
Figure 4-6: Applications Enabling.....	35
Figure 4-7: Media Security Page	36
Figure 4-8: IP Media Settings	37
Figure 4-9: General Parameters.....	38
Figure 4-10: INI file Output Window	39
Figure 4-11: DTMF & Dialing.....	40
Figure 4-12: Coders.....	41
Figure 4-13: Proxy & Registration	42
Figure 4-14: Proxy Sets Table 1.....	43
Figure 4-15: Proxy Sets Table 2.....	44
Figure 4-16: IP Profile Settings.....	45
Figure 4-17: IP Profile Settings.....	46
Figure 4-18: IP Group Table 1.....	47
Figure 4-19: IP Group Table 2.....	48
Figure 4-20: Trunk Group Table	49
Figure 4-21: Trunk Group Settings	49
Figure 4-22: IP to Trunk Group Routing Table	50
Figure 4-23: Tel to IP Routing Table	51
Figure 4-24: Manipulation Tables	52
Figure 4-25: VoIP DNS Settings.....	57
Figure 4-26: NTP Settings	57
Figure 4-27: Certificates Page.....	58
Figure 4-28: Microsoft Certificate Services Web Page.....	59
Figure 4-29: Request a Certificate Page	59

Figure 4-30: Advanced Certificate Request Page	60
Figure 4-31: Submit a Certificate Request or Renewal Request Page	61
Figure 4-32: Download a CA Certificate, Certificate Chain, or CRL Page	61
Figure 4-33: Certificates Page	62
Figure 4-34: Resetting the Gateway	63

List of Tables

Table 1-1: Acronym Descriptions	8
Table 2-1: AudioCodes Gateway Version	11
Table 2-2: Telenet Version	11
Table 2-3: Microsoft Lync Version	11

Notice

This document describes how to connect the Microsoft Lync 2010 with Telenet SIP Trunk using the AudioCodes Mediant E-SBC series, which includes the Mediant 800 MSBG, Mediant 800 Gateway and E-SBC, Mediant 1000 MSBG, Mediant 1000B Gateway and E-SBC, and Mediant 3000 Gateway and E-SBC.

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

© Copyright 2011 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: November-20-2011

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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



Note: Throughout this manual, unless otherwise specified, the term *E-SBC device* refers to the Mediant 800 Gateway and E-SBC, Mediant 800 MSBG, Mediant 1000B Gateway and E-SBC, Mediant 1000 MSBG and the Mediant 3000 Gateway and E-SBC.

Table 1-1: Acronym Descriptions

Acronym	Description
Transferee	The party being transferred to the transfer target
Transferor	The party initiating the transfer
Transfer target	The new party being introduced into a call with the transferee
Blind or semi-attended transfer	The transferor having a session in hold state with the transferee and initiating the transfer by a consultation call to the target performs the transfer while the target is in ringing state
Attended transfer or transfer on conversation	The transferor waits to be in conversation state with the target before completing the transfer
CLIP	Calling Line Identification Presentation
CNIP	Calling Name Identification Presentation
CLIR	Calling Line Identification Restriction
CNIR	Calling Name Identification Restriction
COLP	Connected Line Identification Presentation
CONP	Connected Name Identification Presentation
COLR	Connected Line Identification Restriction
CONR	Connected Name Identification Restriction
CRC	Customer Relationship Centre
PG	SIP GW XXX Peripheral Gateway
ICM	SIP GW XXX Intelligent Call Manager
CCM	SIP GW XXX Call Manager
CVP	Customer voice Portal
BC	ALU Business Contact
CTI	Computer Telephony Integration

1 Introduction

This document describes how to setup the device to work with the Telenet SIP Trunking and Microsoft Lync 2010 Communication platform.

This configuration note is intended for Installation Engineers or AudioCodes and Telenet Partners who are installing and configuring the Telenet SIP Trunking and Microsoft Lync 2010 Communication platform, to place VoIP calls using the AudioCodes E-SBC.

The Mediant 800 MSBG is a networking device that combines multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server.

The Mediant 800 Media Gateway and SBC enable connectivity and security between small and medium businesses (SMB) and service providers' VoIP networks. The Mediant 800 SBC functionality provides perimeter defense for protecting the enterprise 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.

The Mediant 1000 MSBG is an all-in-one multi-service access solution product for Service Providers (SME's) offering managed services and distributed Enterprises seeking integrated services. This multi-service business gateway is designed to provide converged Voice & Data services for business customers at wire speed, while maintaining SLA parameters for superior voice quality.

The Mediant 1000B media gateway and SBC enables connectivity and security between small and medium businesses and service providers' VoIP networks. The Mediant 1000B SBC functionality provides perimeter defense for protecting the enterprise 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. The Mediant 1000B media gateway functionality is based on field-proven VoIP services.

The Mediant 3000 E-SBC Media Gateway is a High Availability VoIP Gateway and Enterprise Class SBC for medium and large enterprises.



Note: The scope of this document does not cover security aspects for connecting the SIP Trunk to the Microsoft Lync 2010 environment. Security measures should be implemented in accordance with your organization's security policies. For basic security guidelines, see the 'AudioCodes Security Guidelines'.

Reader's Notes

2 Components Information

2.1 AudioCodes Gateway Version

Table 2-1: AudioCodes Gateway Version

Gateway Vendor	AudioCodes
Model	Mediant 800 Media Gateway and E-SBC, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000B Media Gateway and E-SBC, Mediant 3000 Media Gateway and E-SBC
Software Version	SIP_6.20A.036.004
Interface Type	SIP/IP
VoIP Protocol	SIP/UDP – to the Telenet Sip Trunk SIP/TCP or TLS – to the Lync FE Server
Additional Notes	None

2.2 Telenet SIP Trunking Version

Table 2-2: Telenet Version

Service Vendor	Telenet
Models	
Software Version	N/A
VoIP Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Version

Table 2-3: Microsoft Lync Version

PBX Vendor	Microsoft
Models	Microsoft Lync
Software Version	RTM: Release 2010 4.0.7577.0
VoIP Protocol	SIP
Additional Notes	None

2.4 Topology

The procedures described in this document describe the following example scenario:

- An enterprise has a deployed Lync Server 2010 in its private network for enhanced communication within the company.
- The enterprise decides to offer its employees enterprise voice capabilities and to connect the company to the PSTN network using the Telenet SIP Trunking service.
- The AudioCodes Enterprise Session Border Controller (E-SBC) is used to manage the connection between the Enterprise LAN and the ITSP SIP trunk.

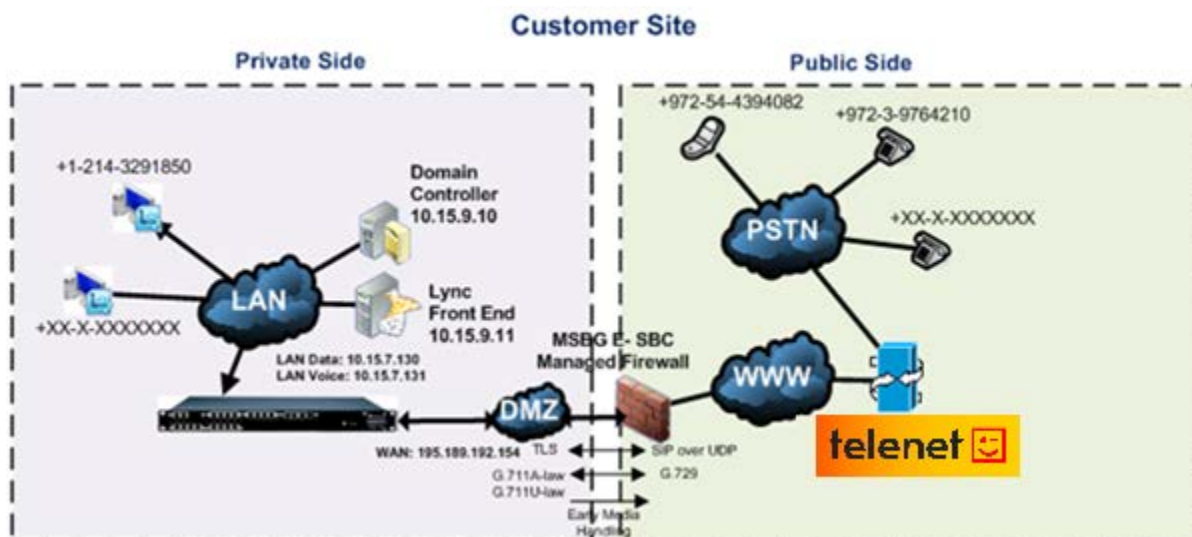
The "session" refers to the real-time voice session using IP SIP signaling protocol. The "border" refers to the IP-to-IP network border between the Microsoft Lync network in the Enterprise LAN and the Telenet SIP trunk in the public network.

Figure 2-1 below illustrates a typical topology of using the E-SBC device to connect the Lync Server 2010 LAN to the Telenet SIP Trunking site.

The setup requirements are characterized as follows:

- While the Lync Server 2010 environment is located on the Enterprise's LAN, the Telenet SIP Trunks are located on the WAN.
- Since the Mediant 1000 MSBG is used, the internal data routing capabilities of the device are used. Consequently, a separate WAN interface is configured in the LAN.
- Lync Server 2010 works with the TLS transport type, while the Telenet SIP trunk works on the SIP over UDP transport type.
- Lync Server 2010 supports G.711A-law and G.711U-law coders, while the Telenet SIP Trunk also supports the same coders' type.
- Support for early media handling.

Figure 2-1: Topology



3 Configuring Lync Server 2010

This section describes how to configure the Lync Server 2010 to operate with the E-SBC device. This section describes the following procedures:

1. Configuring the E-SBC device as a 'IP/PSTN Gateway'. See Section 3.1 on page 14.
2. Associating the 'IP/PSTN Gateway' with the Mediation Server. See Section 3.2 on page 18.
3. Configuring a 'Route' to utilize the SIP trunk connected to the E-SBC device. See Section 3.3 on page 22.



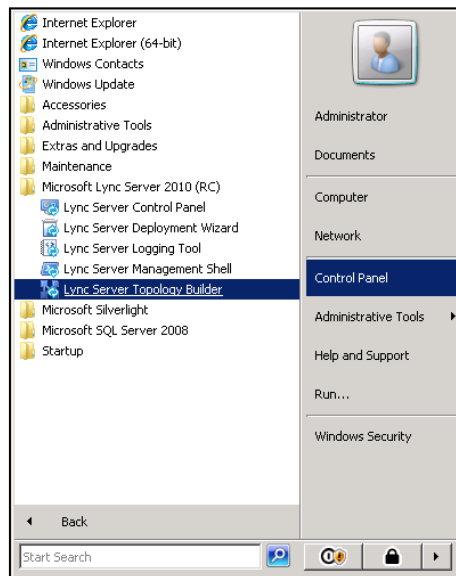
Note: Dial Plans, Voice Policies, and PSTN usages are also necessary for enterprise voice deployment; however, they are beyond the scope of this document.

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

This section describes how to configure the E-SBC device as an IP/PSTN Gateway.

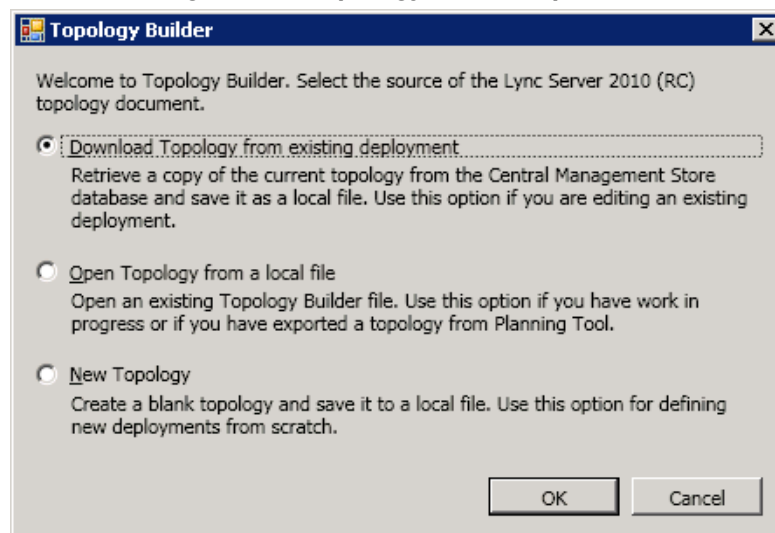
- **To configure the E-SBC device as a IP/PSTN Gateway and associating it with the Mediation Server:**
- 1. On the server where the Topology Builder is located, start the Lync Server 2010 Topology Builder (**Start > All Programs > Lync Server Topology Builder**).

Figure 3-1: Opening the Lync Server Topology Builder



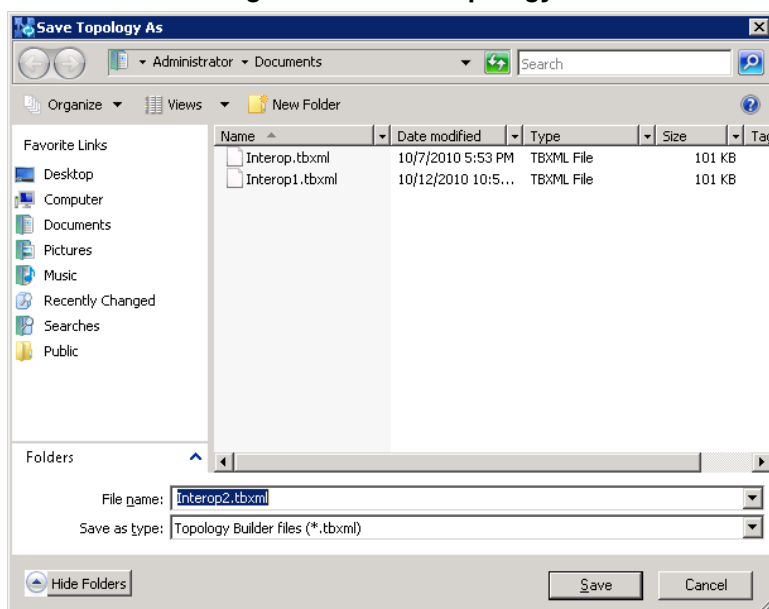
The following screen is displayed:

Figure 3-2: Topology Builder Options



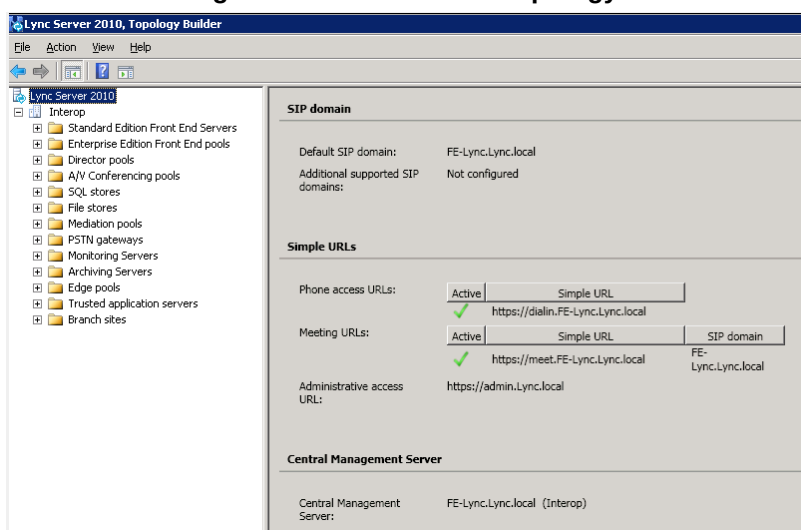
- 2. Click the **Download Topology from the existing deployment** option, and then click **OK**; you are prompted to save the Topology which you have downloaded.

Figure 3-3: Save Topology



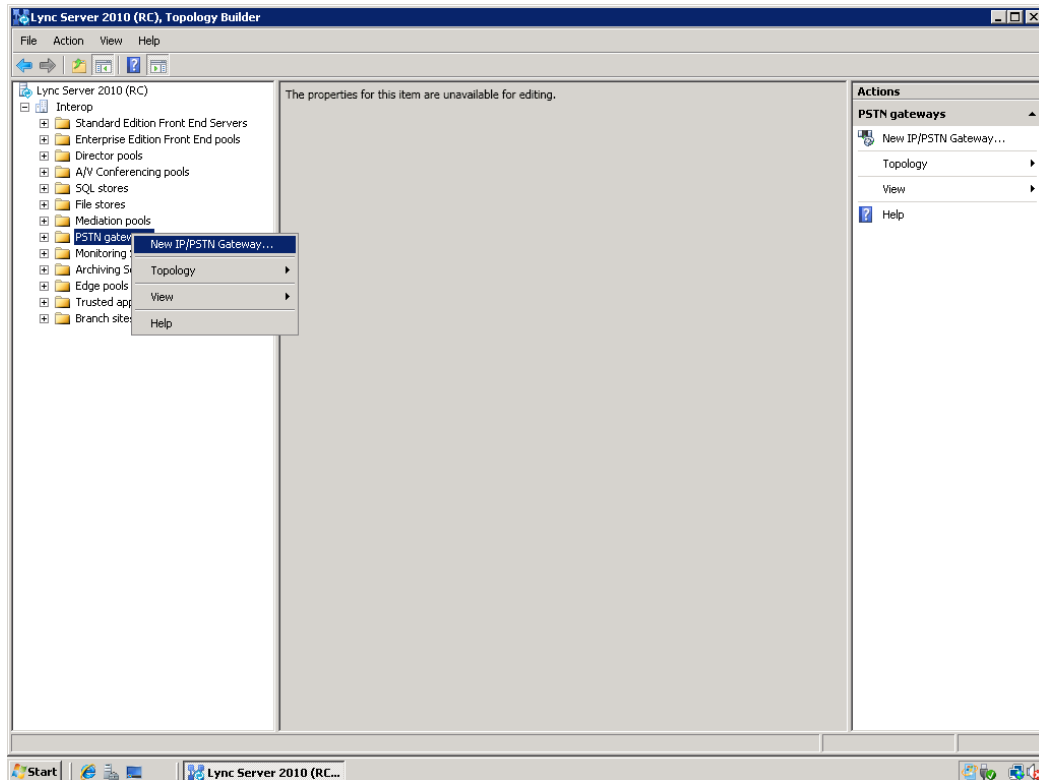
3. In the 'File name' field, enter the new filename, and then click **Save**. This enables you to rollback from any changes you made during the installation. The Topology Builder screen with the topology downloaded is displayed.

Figure 3-4: Downloaded Topology



4. Expand the 'PSTN Gateway' folder, and then choose **New IP/PSTN Gateway**.

Figure 3-5: New IP/PSTN Gateway

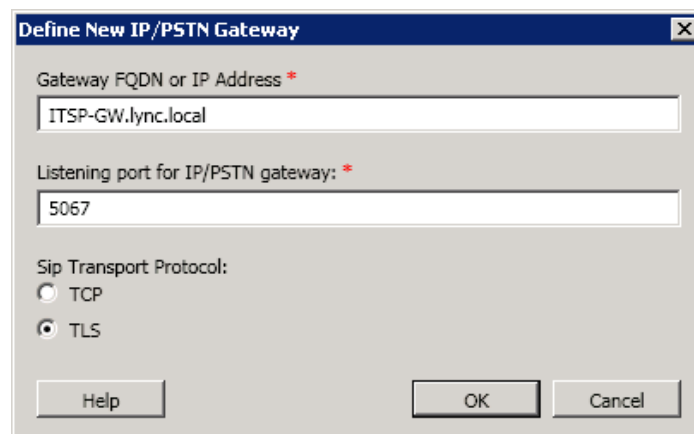


5. In the 'Gateway FQDN or IP Address' field, enter the FQDN of the E-SBC (i.e. 'ITSP-GW.lync.local'), and then click **OK**.



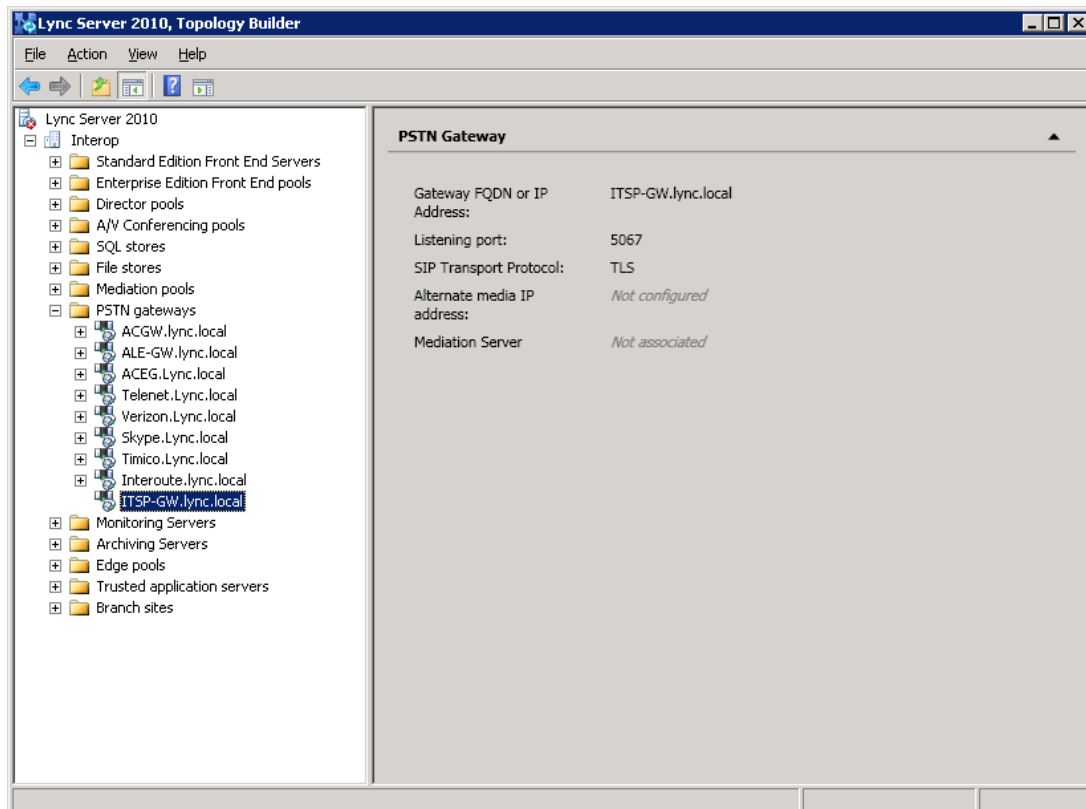
Note: The listening port for the Gateway is **5067** and the SIP Transport Protocol is **TLS**.

Figure 3-6: Define New IP/PSTN Gateway



The E-SBC device has now been added as an 'IP/PSTN Gateway'.

Figure 3-7: IP/PSTN Gateway



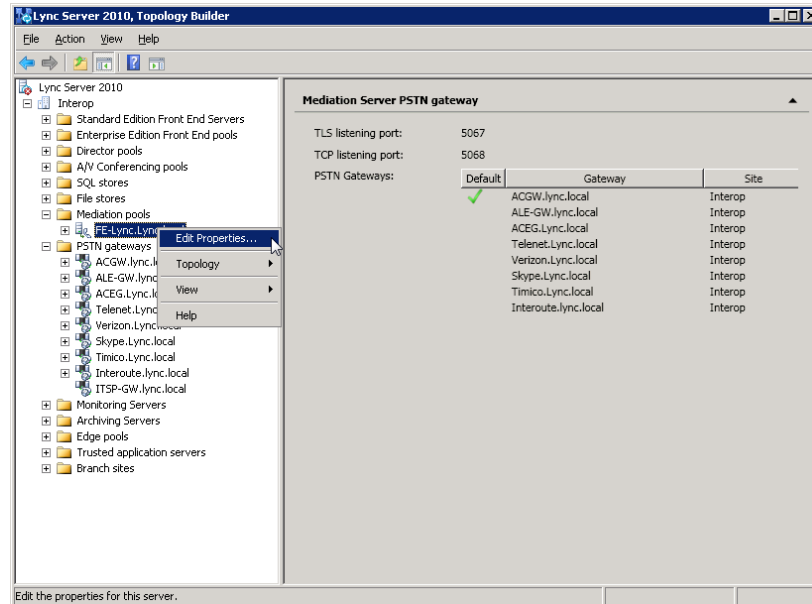
3.2 Associating the IP/PSTN Gateway with the Mediation Server

This section describes how to associate the 'IP/PSTN Gateway' with the Mediation Server.

➤ To associate the IP/PSTN Gateway with the Mediation Server:

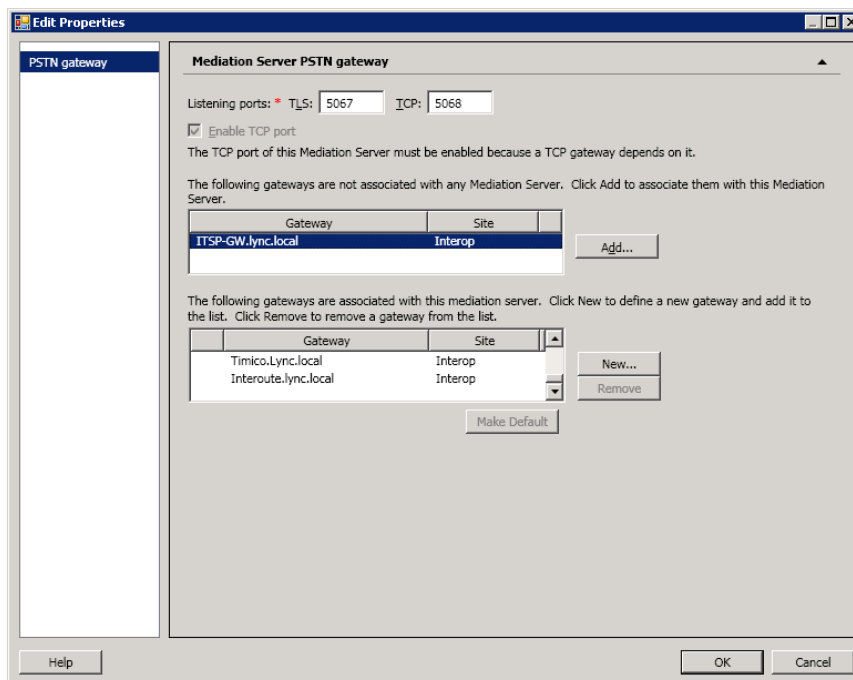
1. Expand the 'Mediation pools' folder.
2. Expand the 'FE-Lync.Lync.local' folder and then choose **Edit Properties**.

Figure 3-8: Associating Mediation Server with IP/PSTN Gateway



The following screen is displayed:

Figure 3-9: Before Associating IP/PSTN Gateway to Mediation Server



3. In the top-left menu pane, choose **PSTN gateway**.
4. In the Mediation Server PSTN gateway pane, click the E-SBC gateway - **ITSP-GW.Lync.local**.

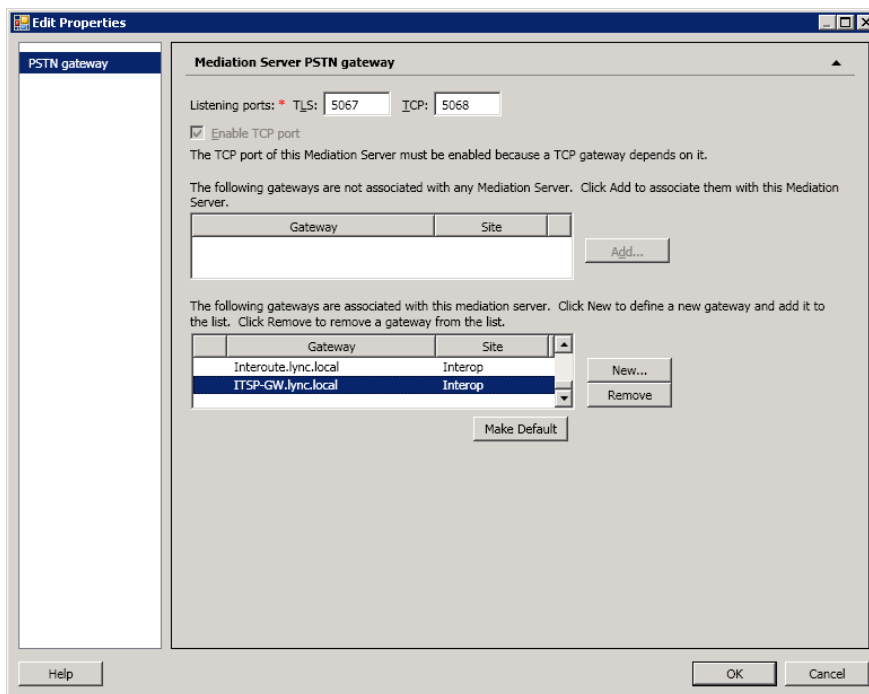
5. Click **Add** to associate it with this Mediation Server.



Note: There are two sub-panes - one including a list of gateways **not** associated with the Mediation server and one including a list of gateways associated with the Mediation server.

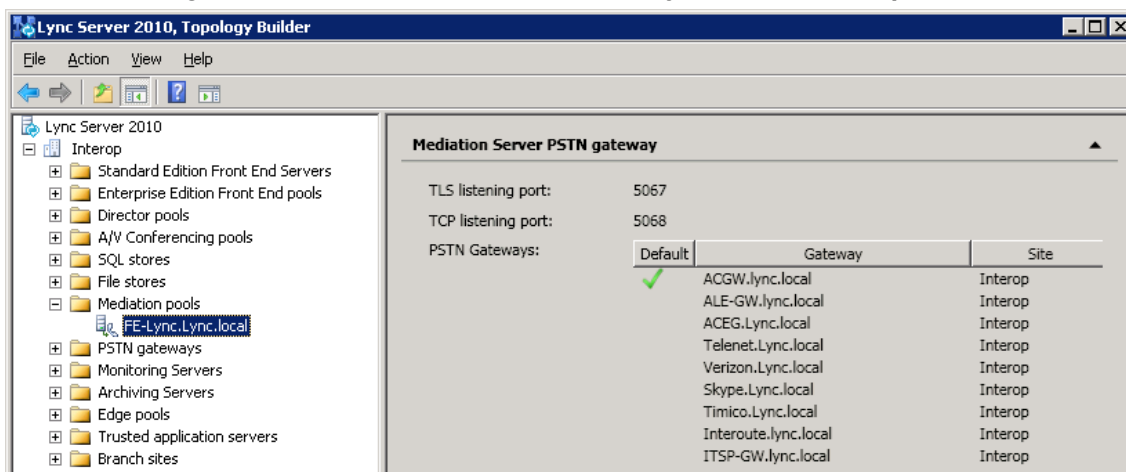
The following screen appears:

Figure 3-10: After Associating IP/PSTN Gateway to Mediation Server



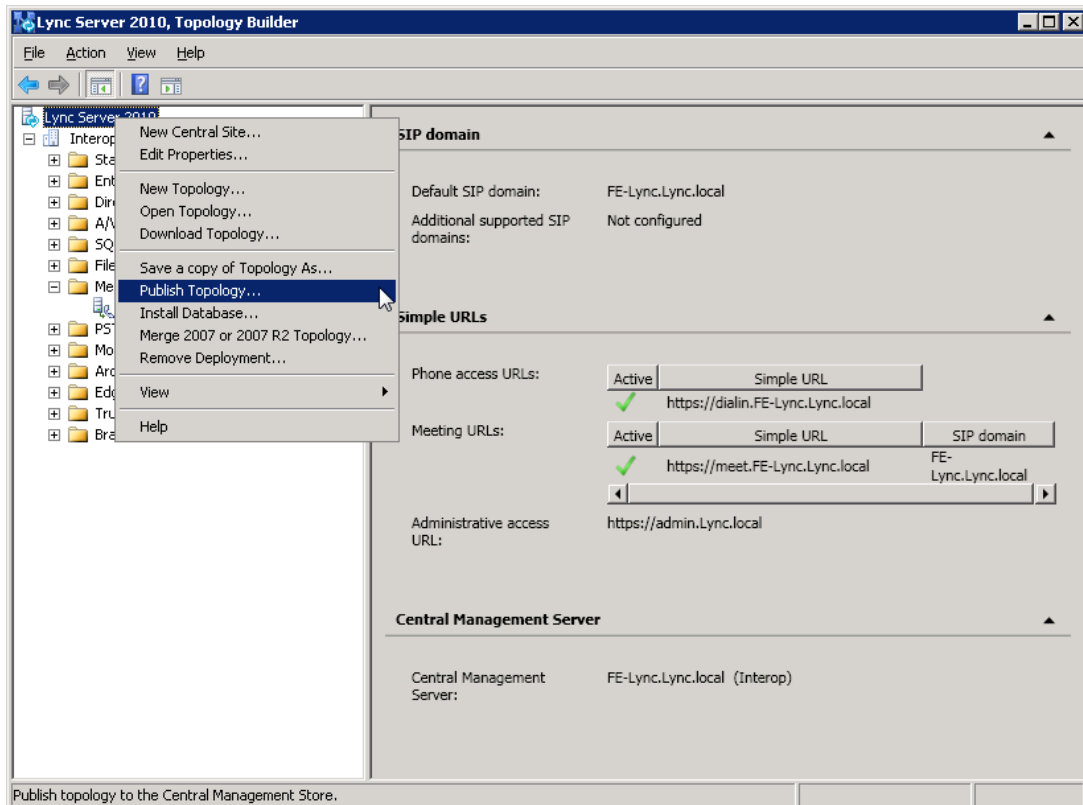
6. Click **OK**; the following screen appears:

Figure 3-11: Media Server PSTN Gateway Association Properties



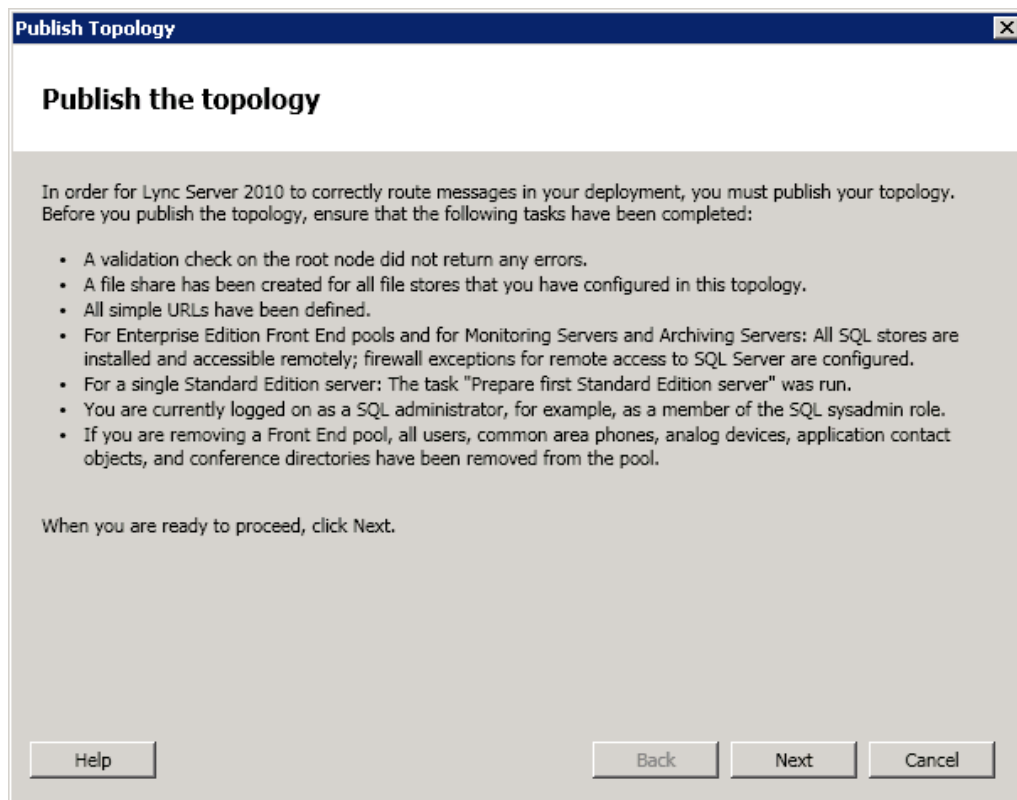
7. In the Lync Server 2010 main menu, choose **Publish Topology**.

Figure 3-12: Publishing Topology

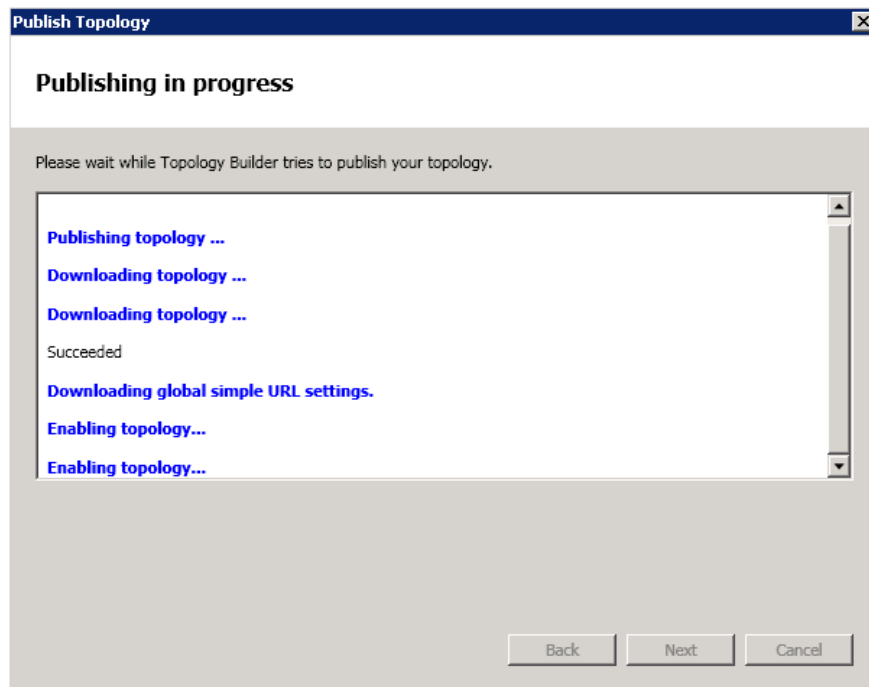


The following screen appears.

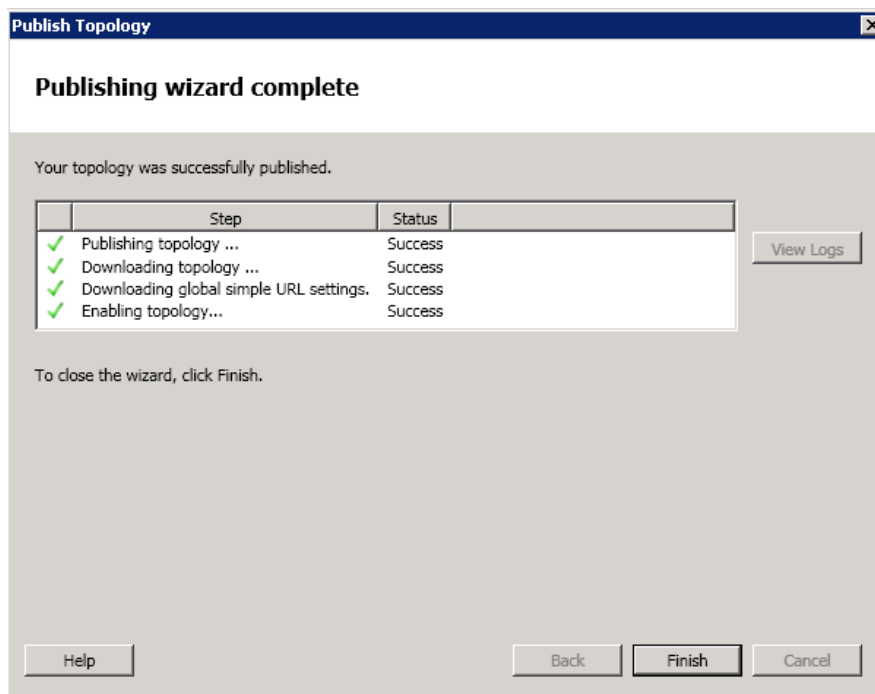
Figure 3-13: Publish Topology Confirmation



8. Click **Next**; the Topology Builder attempts to publish your topology.

Figure 3-14: Publish Topology Progress screen

9. Wait until the publish topology process has ended successfully.

Figure 3-15: Publish Topology Successfully Completed

10. Click **Finish**.

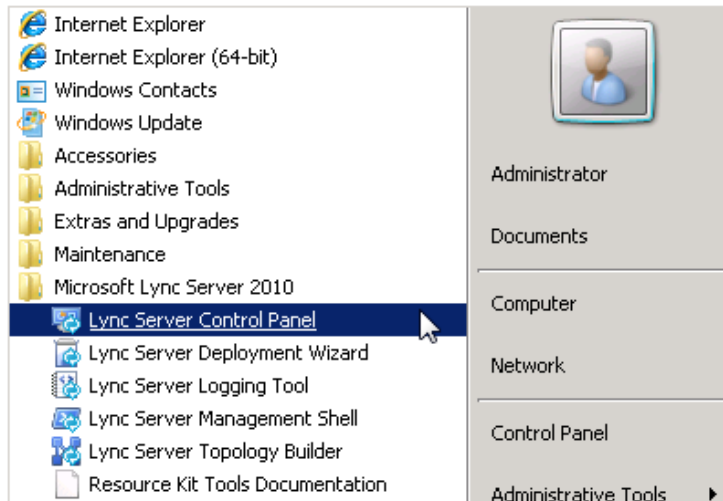
3.3 Configuring the Route on the Lync Server 2010

This section describes how to configure a Route on the Lync server and associate it with the E-SBC PSTN gateway.

➤ **To configure the route on the Lync server:**

1. Open the Communication Server Control Panel (CSCP).
2. Click **Start**.
3. Click **All Programs**, and select **Lync Server Control Panel**.

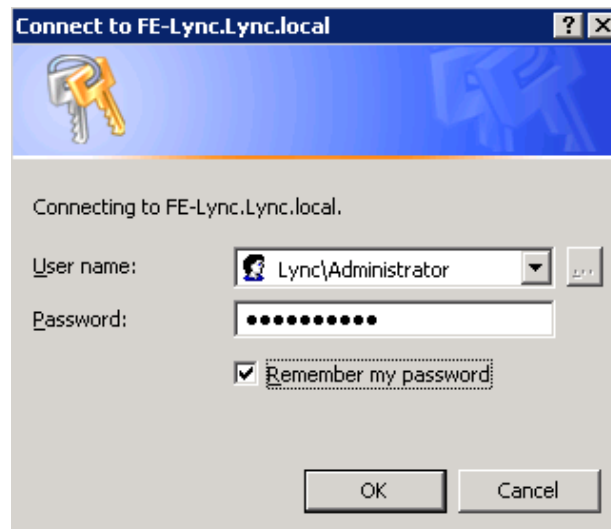
Figure 3-16: Opening the Lync Server Control Panel



The **Connect to FE-Lync.Lync.local** screen appears.

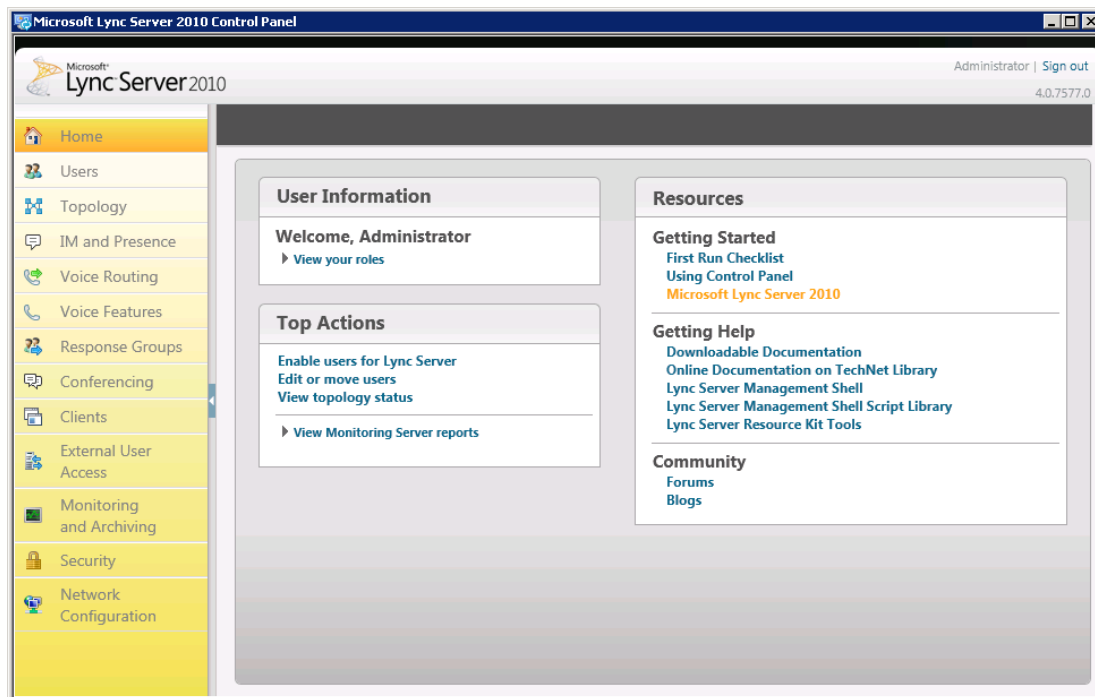
4. Enter your domain Username and Password.

Figure 3-17: Lync Server Credentials



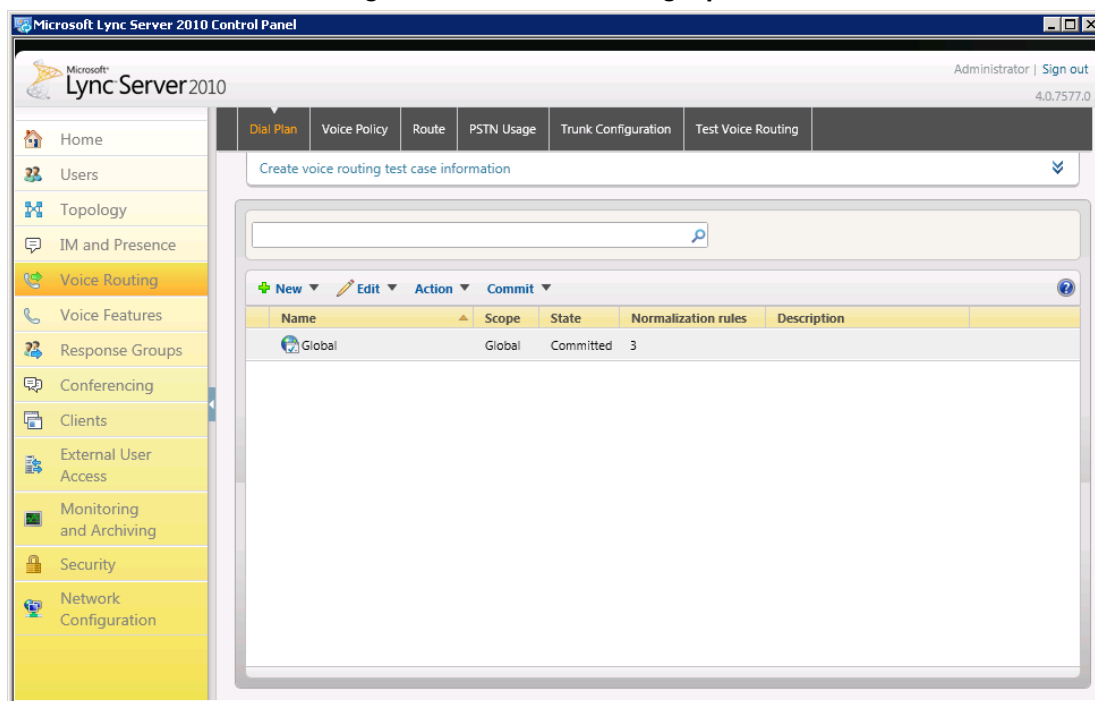
The CSCP Home page is displayed.

Figure 3-18: CSCP Home page



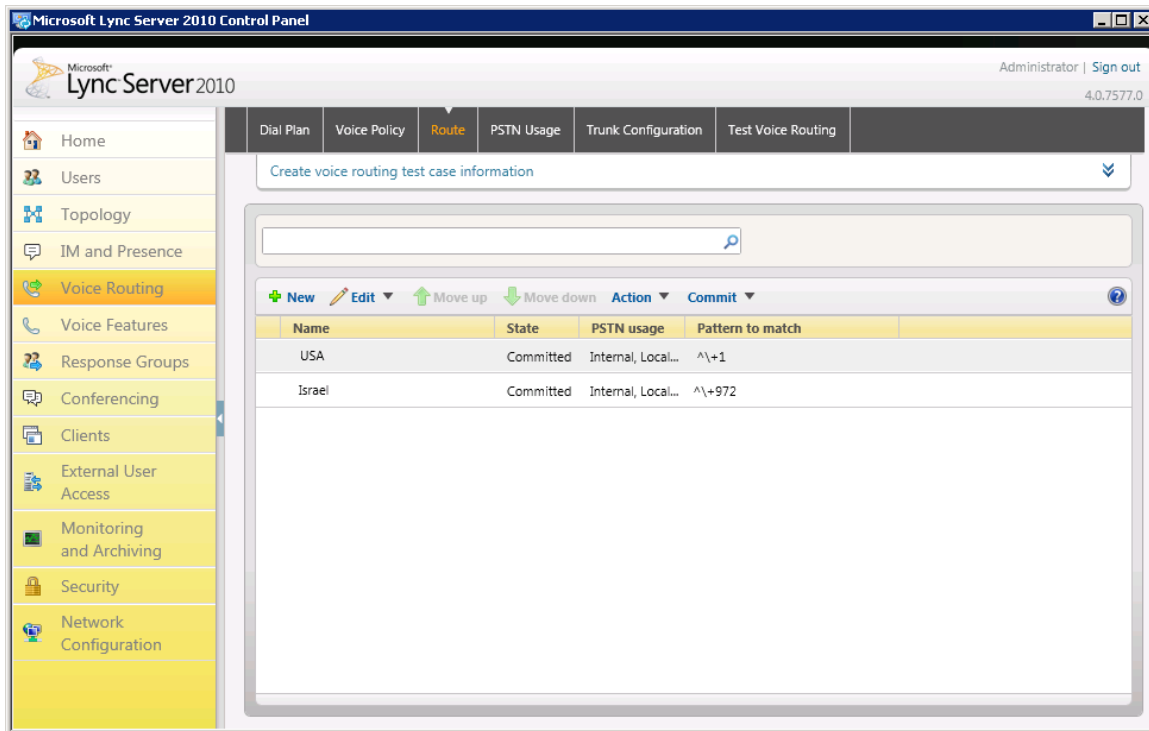
5. In the Navigation pane, select the **Voice Routing** menu option.

Figure 3-19: Voice Routing Option



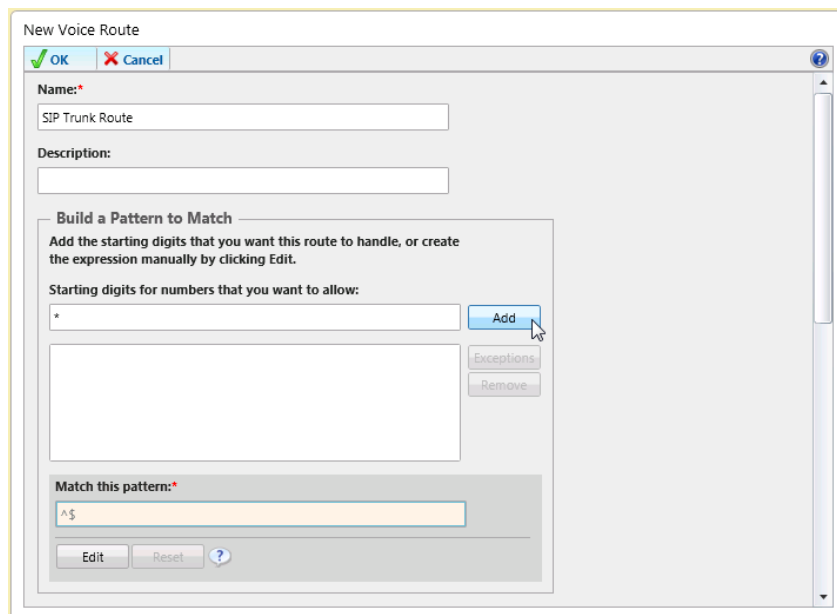
6. In the Voice Routing menu at the top of the page, click the **Route** tab.

Figure 3-20: Route Option



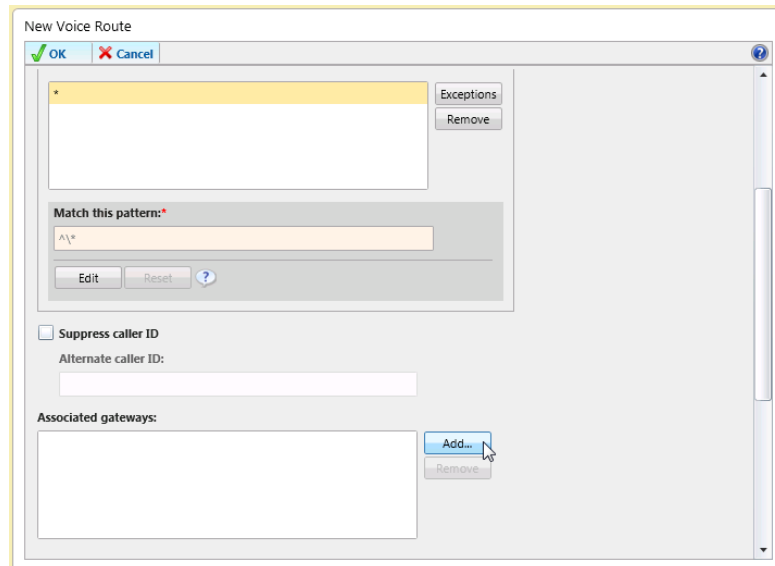
7. In the content area toolbar, click ; the following screen appears:

Figure 3-21: Adding New Voice Route

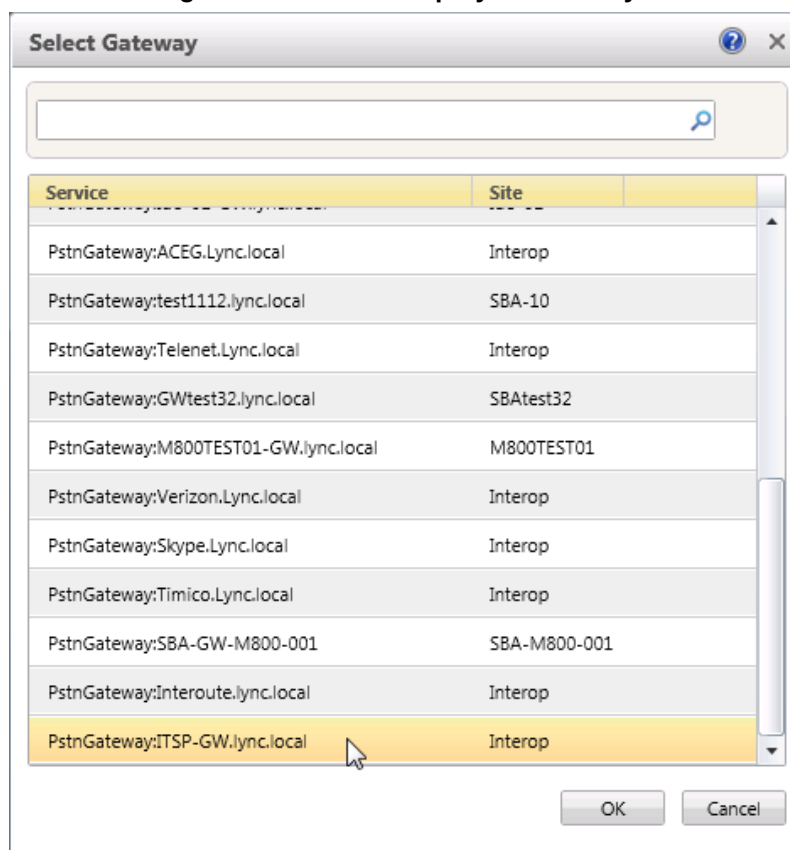


8. In the New Voice Route screen, enter a Name for this route (i.e. SIP Trunk Route).
9. Under 'Build a Pattern to Match', add the starting digits you wish this route to handle. In this example, the pattern to match is '*', which means "to match all numbers".
10. Click **Add**.

11. Associate the route with the E-SBC IP/PSTN gateway you created above by scrolling down to the Associated Gateways pane and click **Add**.

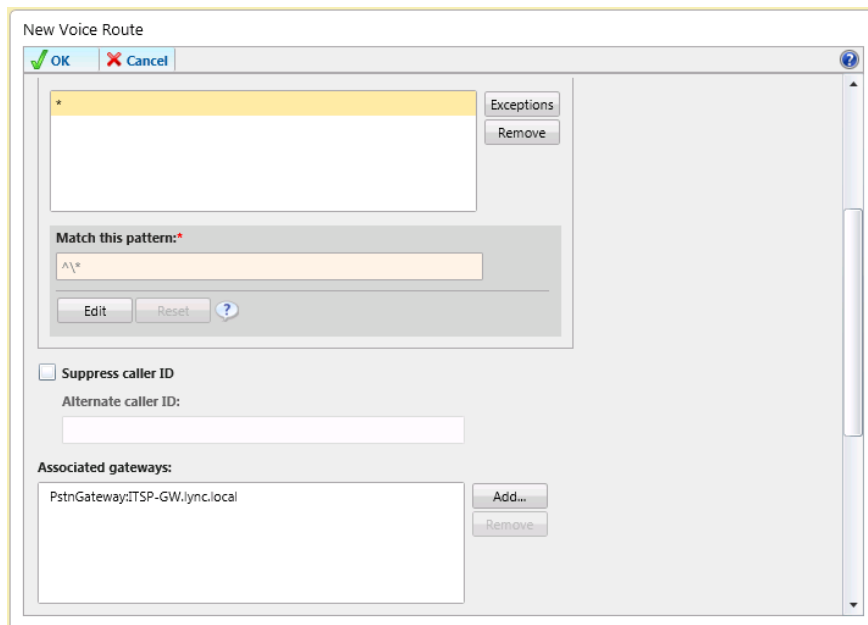
Figure 3-22: Adding New E-SBC Gateway

A list of all the deployed Gateways is displayed.

Figure 3-23: List of Deployed Gateways

12. Select the E-SBC Gateway you created above and click **OK**.

Figure 3-24: Selected the E-SBC Gateway



New Voice Route

✓ OK ✗ Cancel

Exceptions
Remove

Match this pattern:*

^*

Edit Reset ?

☐ Suppress caller ID

Alternate caller ID:

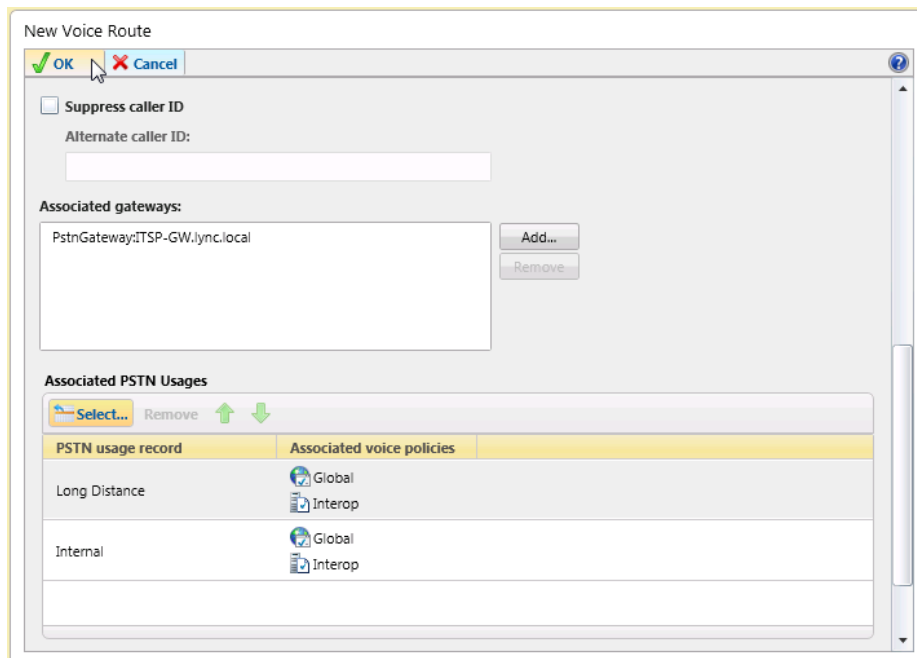
Associated gateways:

PstnGateway:TSP-GW.lync.local

Add...
Remove

14. In the Associated PSTN Usages toolbar, click **Select** and add the associated PSTN Usage.

Figure 3-25: Associating PSTN Usage to E-SBC Gateway



New Voice Route

✓ OK ✗ Cancel

☐ Suppress caller ID

Alternate caller ID:

Associated gateways:

PstnGateway:TSP-GW.lync.local

Add...
Remove

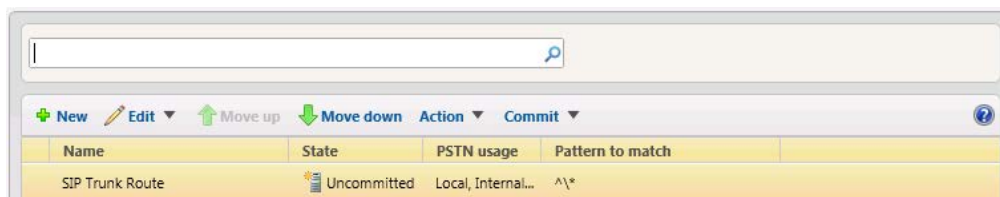
Associated PSTN Usages

Select... Remove ↑ ↓

PSTN usage record	Associated voice policies
Long Distance	Global Interop
Internal	Global Interop

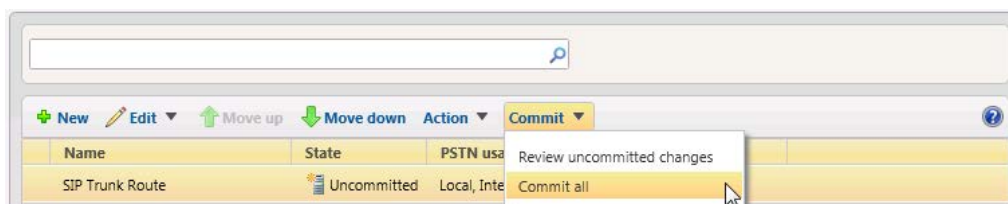
15. In the toolbar at the top of the New Voice Route pane, click **OK**.
The New Voice Route (Uncommitted) is displayed.

Figure 3-26: Confirmation of New Voice Route



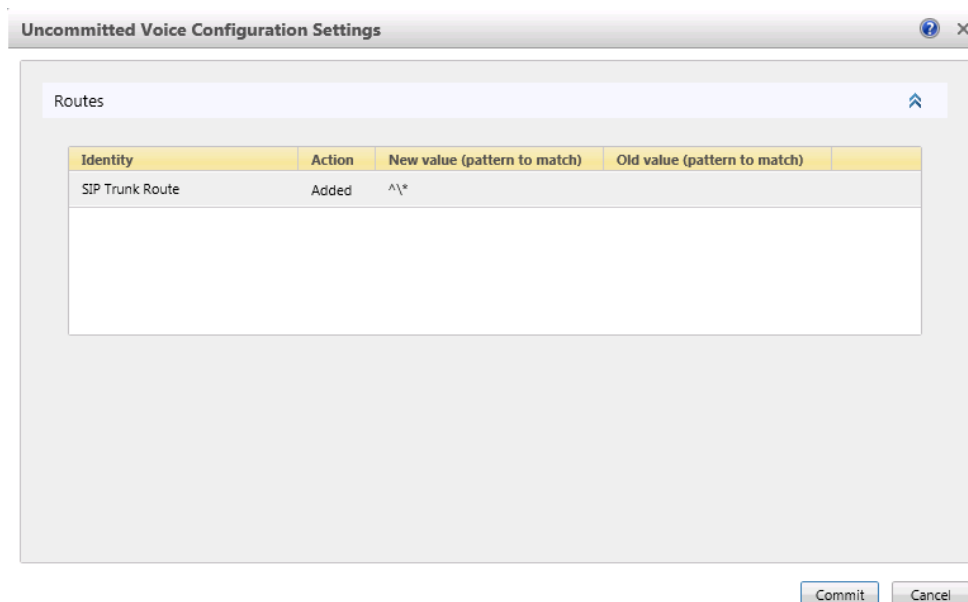
16. From the Commit drop-down menu, on the Content area Toolbar, select the **Commit All** option.

Figure 3-27: Committing Voice Routes



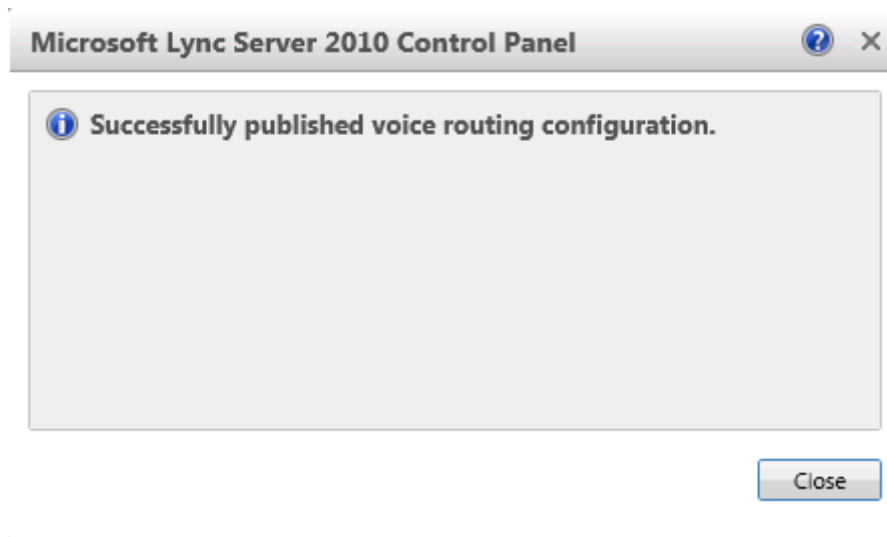
17. In the Uncommitted Voice Configuration Settings window, click **Commit**.

Figure 3-28: Uncommitted Voice Configuration Settings



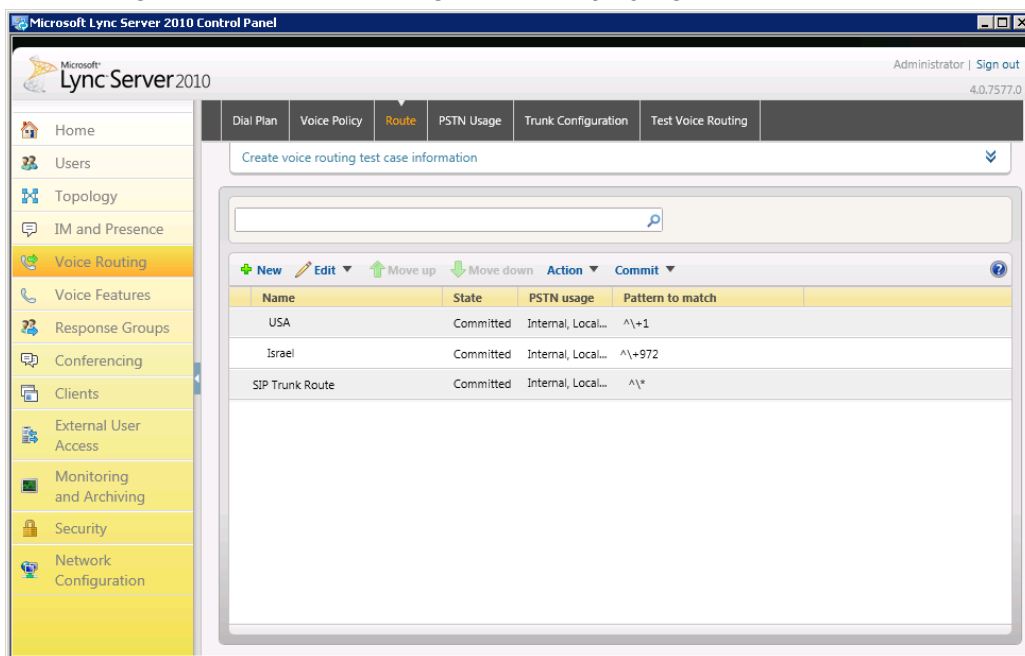
18. A message is displayed, confirming a successful voice routing configuration; click **Close**.

Figure 3-29: Voice Routing Configuration Confirmation



The new committed Route is now displayed in the Voice Routing screen.

Figure 3-30: Voice Routing Screen Displaying Committed Routes



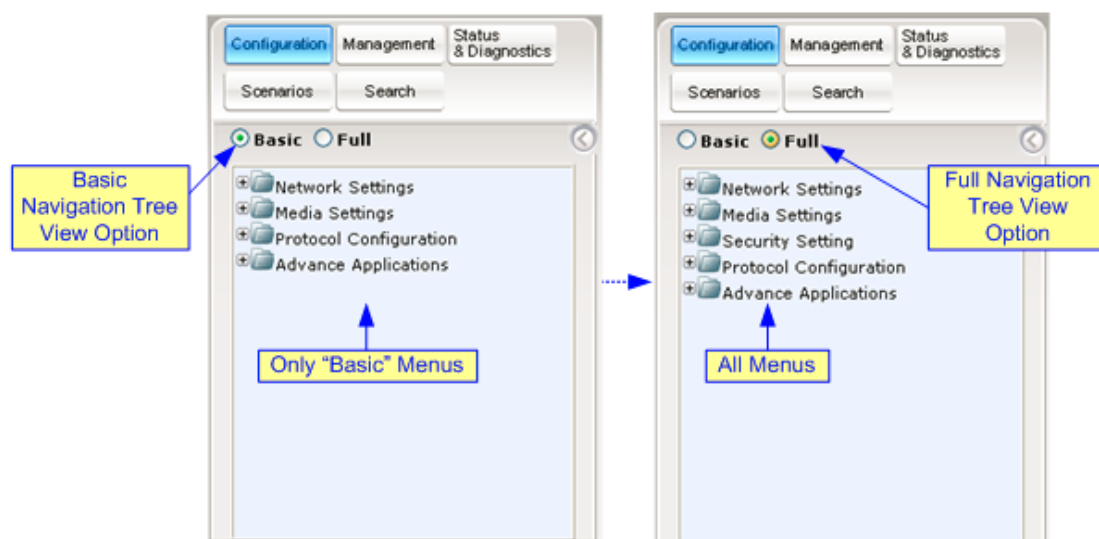
4 Configuring the E-SBC Device

This section describes the following steps for configuring the E-SBC device in the Telenet SIP Trunking environment. The following describes the steps required to configure the E-SBC device:

- **Step 1:** Configuring IP Addresses. See Section 4.1 on page 30.
- **Step 2:** Configuring Port Forwarding. See Section 4.2 on page 33.
- **Step 3:** Enabling Application Mode. See Section 4.3 on page 35.
- **Step 4:** Configuring Secure Real-Time Transport Protocol (SRTP). See Section 4.4 on page 36.
- **Step 5:** Configuring IP Media. For more information, see Section 4.5 on page 37.
- **Step 6:** Configuring SIP General Parameters. For more information, see Section 4.6 on page 38.
- **Step 7:** Configuring DTMF & Dialing. See Section 4.7 on page 40.
- **Step 8:** Configuring Coders. See Section 4.8 on page 41.
- **Step 9:** Configuring Proxy & Registration. See Section 4.9 on page 42.
- **Step 10:** Configuring Proxy Sets Table. See Section 4.10 on page 43.
- **Step 11:** Configuring IP Profile. See Section 4.11 on page 45.
- **Step 12:** Configuring IP Group Tables. See Section 4.12 on page 47.
- **Step 13:** Configuring Trunk Group. See Section 4.13 4.11on page 49.
- **Step 14:** Configuring Routing. See Section. See Section 4.13 on page 49.
- **Step 15:** Configuring Manipulation. See Section 4.15 on page 52.
- **Step 16:** Configuring Message Manipulations. See Section 4.16 on page 54.
- **Step 17:** Configuring SIP TLS Connection. See Section 4.17 4.16on page 57.
- **Step 18:** Resetting the Gateway. See Section 4.18 on page 63.

The procedures described in this section are performed using the E-SBC devices' Web-based management tool (i.e., Web interface). Before you begin configuring the E-SBC device, ensure that the Web interface's navigation tree is in full menu display mode (i.e., the **Full** option on the Navigation bar is selected), as displayed below:

Figure 4-1: Web Interface Showing Basic/Full Navigation Tree Display



4.1 Step 1: Configuring IP Addresses

This step describes how to configure LAN IP addresses when the internal data-routing capabilities of the E-SBC device are used in order to connect to the Telenet SIP Trunk. In this case, you must configure a separate WAN interface as described below.



Notes:

- The VoIP and Management interface must be in the same subnet as the data-routing interface as shown in the figure below.
- When operating with both VoIP and Data-Routing functionalities, it is recommended to define the Default Gateway IP address for the VoIP network interface in the same subnet and with the same VLAN ID as the IP address for the data-routing LAN interface, as shown below.

4.1.1 Configuring LAN IP Addresses

The following describes how to configure VoIP IP Settings and LAN Data-Routing IP Settings.

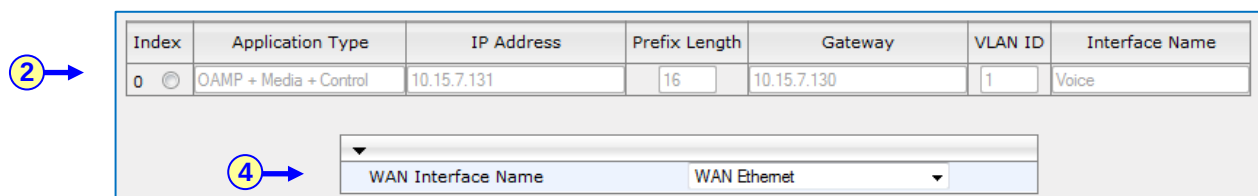
4.1.1.1 Configuring VoIP IP Settings

The section describes how to configure VoIP IP Settings.

➤ **To configure the VoIP IP settings:**

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

Figure 4-2: IP Settings



Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP + Media + Control	10.15.7.131	16	10.15.7.130	1	Voice

Below the table, there is a dropdown menu labeled 'WAN Interface Name' with 'WAN Ethernet' selected.

2. Click the **Index** option corresponding to the "OAMP + Media + Control" (i.e., VoIP and management interface) Application Type, and then click **Edit**.
3. Set the following parameters:
 - **IP-Address:** <Gateway IP-Address> (e.g., 10.15.7.131).
 - **Prefix Length:** The Subnet Mask in bits (e.g., 16 for 255.255.0.0).
 - **Gateway:** <Gateway Default Gateway> (e.g., 10.15.7.130). For Mediant 800 or Mediant 1000, this IP should be same as you set up in the LAN data-routing IP address. For Mediant 3000, it should be the corporate router IP.
4. From the 'WAN Interface Name' drop-down list, select **WAN Ethernet**. This is the WAN interface on which your VoIP traffic interfaces with the public network.

4.1.1.2 Configuring LAN Data-Routing IP Settings

The following describes how to configure LAN data-routing IP settings.



Notes: This step is only relevant for the Mediant 800 MSBG and the Mediant 1000 MSBG devices.

➤ **To define the MSBG device's LAN data-routing IP address:**

1. Access the MSBG device's Web interface with the IP address that you assigned to the VoIP and Management interface.

Open the 'Connections' page (**Configuration** tab > **Data** menu > **Data System** > **Connections**).

Figure 4-3: Connections Page

Name	Status	Action
LAN switch	1 Ports Connected	
WAN Ethernet	Cable Disconnected	
LAN switch VLAN 1	Connected	
New Connection		

Click the **Edit** icon corresponding to the 'LAN Switch VLAN 1' connection, and then click the **Settings** tab.

In the 'IP Address' and 'Subnet Mask' fields, enter the required IP address (e.g., 10.15.7.130) and subnet respectively, and then click **OK**.

Figure 4-4: Defining LAN Data-Routing IP Address

General		Settings		Routing		Advanced	
Device Name:	eth0.1						
Status:	Connected						
Schedule:	Always ▼						
Network:	LAN ▼						
Connection Type:	Ethernet						
Physical Address:	00:90:8f:36:c4:f7						
Underlying Connection:	LAN switch						
Internet Protocol				Use the Following IP Address ▼			
IP Address:	10	15	7	130			
Subnet Mask:	255	255	0	0			
DNS Server				No DNS Server ▼			

4.1.2 Configuring WAN IP Addresses

The following describes how to configure the MSBG device IP address used to connect to the WAN.

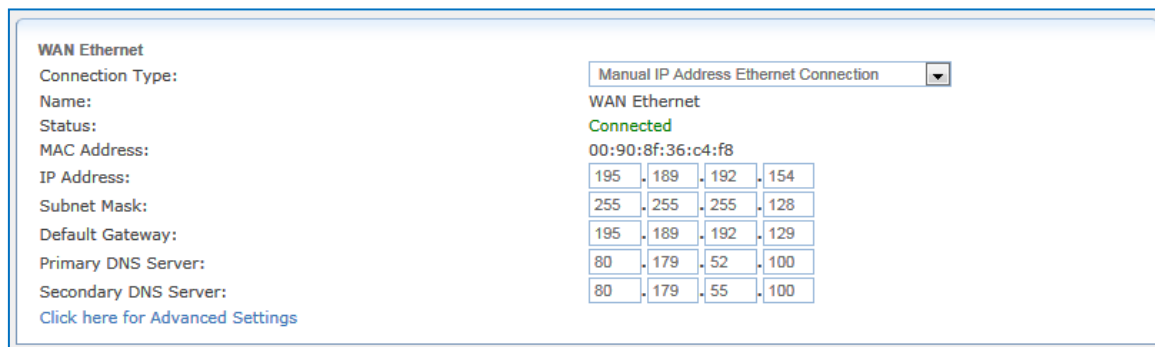


Notes: This step is only relevant for the Mediant 800 MSBG and the Mediant 1000 MSBG devices.

➤ **To configure the WAN IP address:**

1. Cable the MSBG device to the WAN network (i.e., ADSL or Cable modem), using the WAN port.
2. Open the 'Settings' page (**Configuration** tab > **Data** menu > **WAN Access** > **Settings**).

Figure 4-5: WAN Settings



WAN Ethernet

Connection Type: Manual IP Address Ethernet Connection

Name: WAN Ethernet

Status: Connected

MAC Address: 00:90:8f:36:c4:f8

IP Address:

195	189	192	154
-----	-----	-----	-----

Subnet Mask:

255	255	255	128
-----	-----	-----	-----

Default Gateway:

195	189	192	129
-----	-----	-----	-----

Primary DNS Server:

80	179	52	100
----	-----	----	-----

Secondary DNS Server:

80	179	55	100
----	-----	----	-----

[Click here for Advanced Settings](#)

3. Set the following parameters:
 - **IP Address:** <WAN IP-Address> (e.g., 195.189.192.154).
 - **Subnet Mask:** <Subnet Mask> (e.g., 255.255.255.128).
 - **Default Gateway:** <WAN Default GW IP-Address> (e.g., 195.189.192.129).
 - **Primary DNS Server:** <First DATA DNS IP-Address> (e.g., 80.179.52.100).
 - **Secondary DNS Server:** <Second Data DNS IP-Address> (e.g., 80.179.55.100).

4.2 Step 2: Configuring Port Forwarding

This step describes how to configure the MSBG device's Port Forwarding.

The Port Forwarding item enables you to define the applications that require special handling by the device. This allows you to select the application's protocol or ports (SIP and RTP) and the local IP address of the device (e.g., Gateway's IP: 10.15.7.131) that will be using the service.



Notes: This step is only relevant for the Mediant 800 MSBG and the Mediant 1000 MSBG devices.

➤ **To configure a port forwarding service:**

1. Open the 'Settings' page (**Configuration** tab > **Data** menu > **Firewall and ACL** > **Port Forwarding**).

Figure 4-6: Configure Port Forwarding

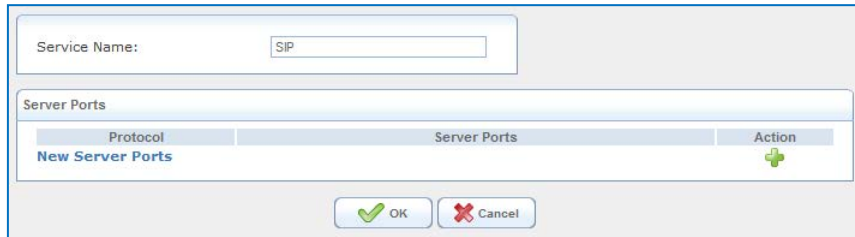
2. Click the 'New Entry' link; the following page appears:

Figure 4-7: Adding Port Forwarding Rule

3. In the 'Local Host' field, enter the host name or IP address (e.g., 10.15.7.131).
4. From the 'Protocol' drop-down list, select or specify the type of protocol. Add a new protocol using the 'User Defined' option, and then add a new Service, representing the protocol.

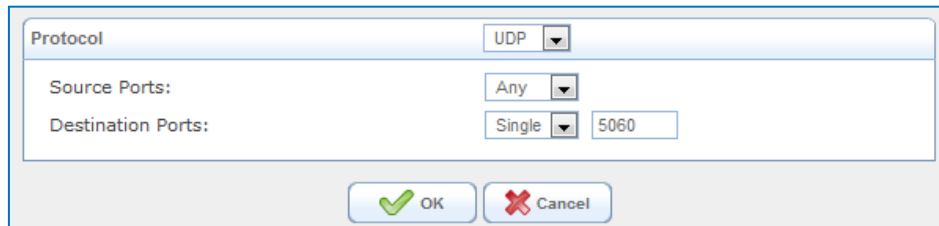
5. In the 'Service Name' name field, enter "SIP".
6. Click the **New Server Ports** link.

Figure 4-8: Adding a Service Protocol



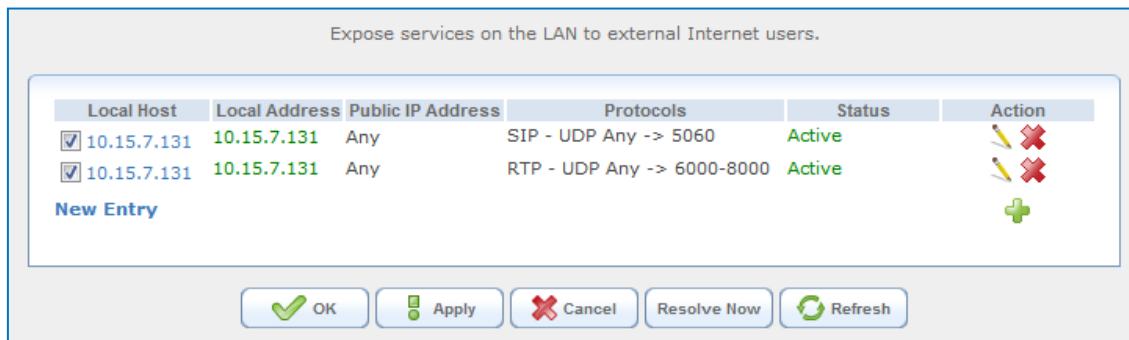
7. From the 'Protocol' drop-down list, select **UDP**.

Figure 4-9: Defining Service Server Ports



8. In the "Destination Ports" field, enter the range (e.g., 5060 for SIP and 6000-8000 for RTP).
9. Click **OK**; the main Port Forwarding page displays a summary of the rules that you added:

Figure 4-10: Display Port Forwarding Rules



Local Host	Local Address	Public IP Address	Protocols	Status	Action
☒ 10.15.7.131	10.15.7.131	Any	SIP - UDP Any -> 5060	Active	 
☒ 10.15.7.131	10.15.7.131	Any	RTP - UDP Any -> 6000-8000	Active	 
New Entry					

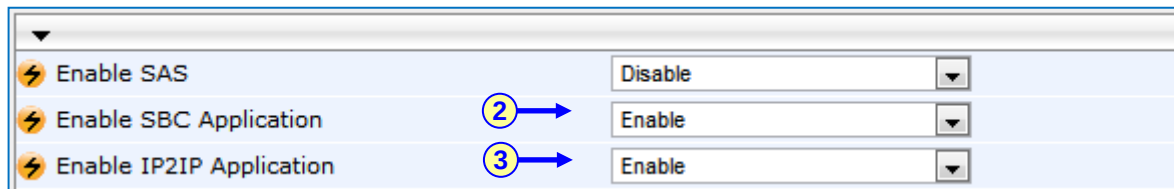
4.3 Step 3: Enabling Application Mode

The following describes how to enable the IP-to-IP and SBC application mode.

➤ **To enable the IP-to-IP application mode:**

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

Figure 4-6: Applications Enabling



Enable SAS	Disable
Enable SBC Application	Enable
Enable IP2IP Application	Enable

2. From the 'Enable SBC Application' drop-down list, select **Enable**. (This application is enabled for the purpose of configuring the Message Manipulation Table on the SBC menu. This application can be disabled after setting the Message Manipulation Table).
3. From the 'Enable IP2IP Application' drop-down list, select **Enable**.



Notes:

1. To enable the IP-to-IP capabilities on the AudioCodes gateway, your gateway must be loaded with the feature key that includes the **IP-to-IP** feature.
2. The E-SBC device must be running SIP Version 6.2 or later.
3. A reset with BURN to FLASH is required.

4.4 Step 4: Configuring Secure Real-Time Transport Protocol (SRTP)

If you configure TLS for the SIP transport link between the E-SBC and the Mediation Server, you must specify Secure RTP (SRTP) encryption with one of the following options:

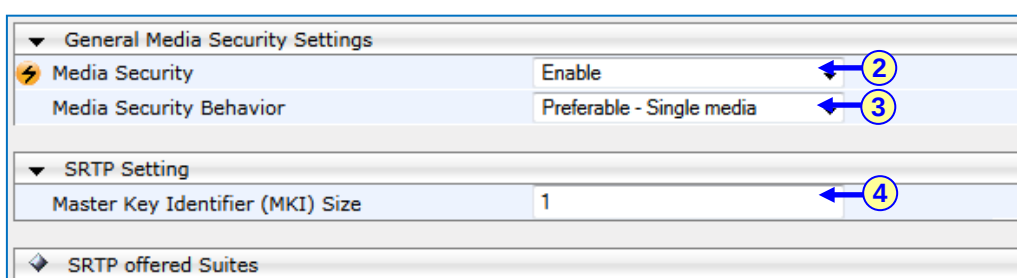
- **Required:** SRTP should be attempted, but do not use encryption if negotiation for SRTP is unsuccessful.
- **Optional:** Attempt to negotiate the use of SRTP to secure media packets. Use RTP if SRTP cannot be negotiated.
- **Not used:** Send media packets using RTP.

If you choose to configure the Mediation Server to use SRTP (Required or Optional), you need to configure the Media Gateway to operate in the same manner.

➤ To configure the media security:

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

Figure 4-7: Media Security Page



2. From the 'Media Security' drop-down list, select **Enable**.
3. From the 'Media Security Behavior' drop-down list, select one of the following:
 - **Mandatory** - if the Mediation Server is configured to **SRTP Required**.
 - **Preferable-Single media** - if Mediation Server is configured to **SRTP Optional**.
4. In the 'Master Key Identifier (MKI) Size' field, enter "1".
5. Click **Submit**.
6. Save (burn) the configuration and reset the Gateway.



Notes: In order to set the 'Media Security Behavior' to the IP Profile of the Mediation Server, see the IP Profile Settings (see Section 4.9 on page 42).

4.5 Step 5: Configuring IP Media

This step describes how to configure the number of media channels for the IP media. In order to reform the coder transcoding, you need to define DSP channels. The number of media channels represents the number of digital signaling processors (DSP) channels that the device allocates to IP-to-IP calls (the remaining DSP channels can be used for PSTN calls). Two IP media channels are used per IP-to-IP call.

The maximum number of media channels available on the Mediant 800 E-SBC device is 30 (i.e., up to 15 IP-to-IP calls).

The maximum number of media channels available on the Mediant 1000 E-SBC device is 120 (i.e., up to 60 IP-to-IP calls).

The maximum number of media channels available on the Mediant 3000 E-SBC device is 2016 (i.e., up to 1008 IP-to-IP calls).

In this configuration, 120 channels are configured.

➤ **To configure IP Media Settings:**

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

Figure 4-8: IP Media Settings

▼	
⚡ Number of Media Channels	120
⚡ Voice Streaming	Disable
NetAnn Announcement ID	annc
MSCML ID	ivr
Transcoding ID	trans
▼ Conference	
Conference ID	conf
Beep on Conference	Enable
Enable Conference DTMF Clamping	Enable
Enable Conference DTMF Reporting	Disable

2. In the 'Number of Media Channels' field, enter "120".

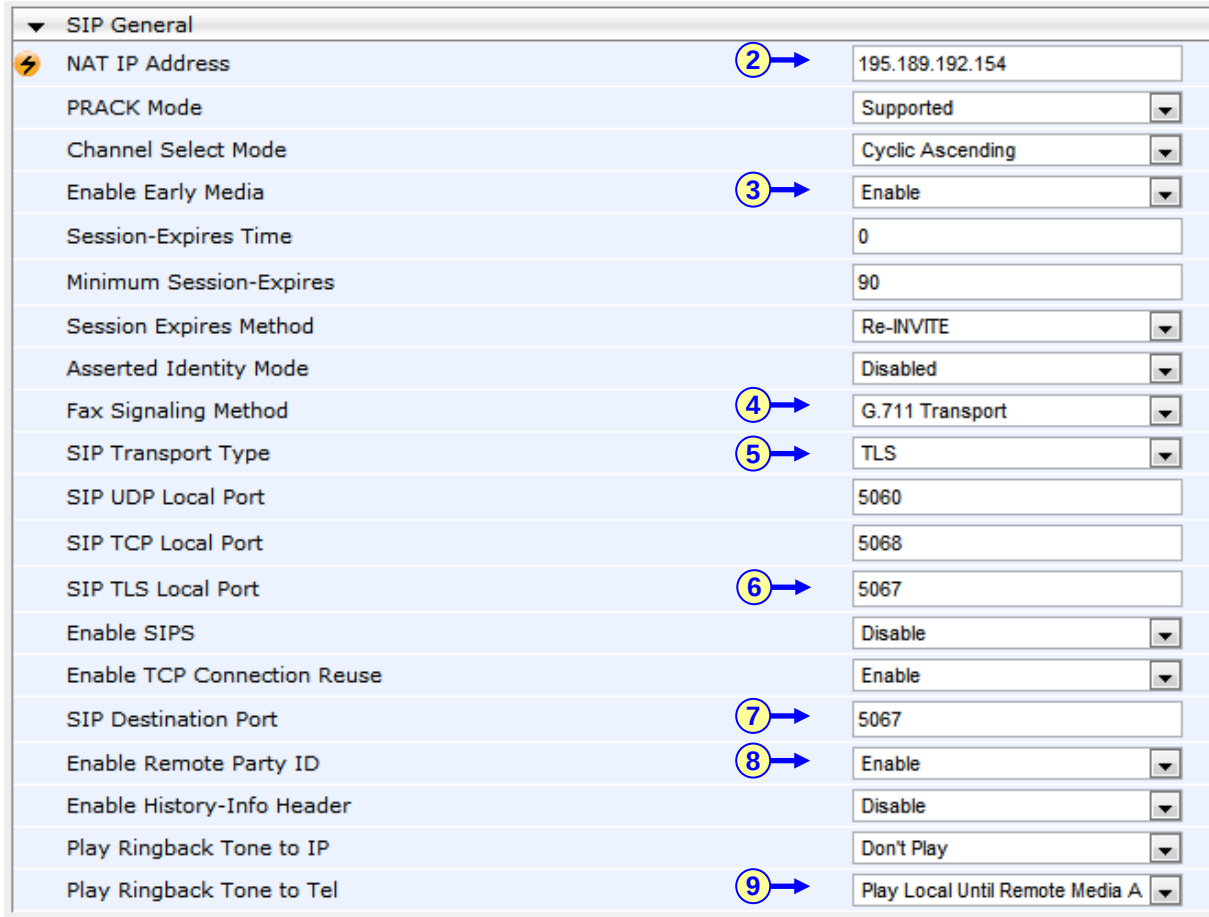
4.6 Step 6: Configuring SIP General Parameters

The following describes how to enable SIP General parameters.

➤ **To configure SIP General Parameters:**

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

Figure 4-9: General Parameters



SIP General	
NAT IP Address	195.189.192.154
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Enable
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	G.711 Transport
SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5068
SIP TLS Local Port	5067
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
SIP Destination Port	5067
Enable Remote Party ID	Enable
Enable History-Info Header	Disable
Play Ringback Tone to IP	Don't Play
Play Ringback Tone to Tel	Play Local Until Remote Media A

2. In the 'NAT IP Address' field, enter the Global (public) IP address of the E-SBC device.
3. From the 'Enable Early Media' drop-down list, select **Enable**.
4. From the 'Fax Signaling Method' drop-down list, select **G.711 Transport**.
5. From the 'SIP Transport Type' drop-down list, select **TLS**.
6. In the 'SIP TLS Local Port' field, enter "5067".
7. In the 'SIP Destination Port' field, enter "5067" (Lync Server listening port).
8. From the 'Enable Remote Party ID' drop-down list, select **Enable**.
9. From the 'Play Ringback Tone to Tel' drop-down list, select **Play Local Until Remote Media Arrives**.

Figure 4-11: General Parameters (Cont.)

Forking Handling Mode	Sequential handling
Enable Comfort Tone	Disable
Add Trunk Group ID as Prefix to Source	No
Fake Retry After	0
Enable Reason Header	Enable

10. From the 'Forking Handling Mode' drop-down list, select **Sequential handling**.
11. Open the 'Admin' page, by appending the case-sensitive suffix 'AdminPage' to the Media Gateway's IP address in your Web browser's URL field (e.g., <http://10.15.7.131/AdminPage>).
12. On the left pane, click **ini Parameters**.

Figure 4-10: INI file Output Window

Image Load to Device
ini Parameters
Back to Main

Parameter Name:

Enter Value:

Output Window

```

Parameter Name: IGNOREALERTAFTEREARLYMEDIA
Parameter Current Value: 1
Parameter Description:Interwork of Alert from ISDN to SIP

Parameter Name: ENABLEEARLY183
Parameter Current Value: 1
Parameter Description:Enable Early 183

Parameter Name: OPTIONSUSERPART
Parameter Current Value: empty
Parameter Description:Allow to configure the OPTIONS userpart string for all gateways.

Parameter Name: USESIPURIFORDIVERSIONHEADER
Parameter Current Value: 1
Parameter Description:Use Tel uri or Sip uri for Diversion header

```

13. In the 'Parameter Name' field, enter the following parameters:
 - **IGNOREALERTAFTEREARLYMEDIA**; in the 'Enter Value' field, enter "1".
 - **ENABLEEARLY183**; in the 'Enter Value' field, enter "1".
 - **OPTIONSUSERPART**; in the 'Enter Value' field, enter "empty".
 - **USESIPURIFORDIVERSIONHEADER**; in the Enter Value field, enter "1".
14. Click **Apply New Value**.

4.7 Step 7: Configuring DTMF and Dialing

The following describes how to configure the DTMF and Dialing settings.

➤ **To configure DTMF and Dialing:**

1. Open the 'DTMF & Dialing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **DTMF & Dialing**).

Figure 4-11: DTMF & Dialing

Max Digits In Phone Num	30
Inter Digit Timeout [sec]	4
Declare RFC 2833 in SDP	Yes
1st Tx DTMF Option	RFC 2833
2nd Tx DTMF Option	
RFC 2833 Payload Type	101
Dial Plan Index	-1
Default Destination Number	1000

2. In the 'RFC 2833 Payload Type' field, enter "101".

4.8 Step 8: Configuring Coders

The following describes how to configure the SIP coders. This is the general coder table. Because Microsoft Lync and Telenet both support only G.711 coders, there no need for Transcoding and different Coder Groups.

➤ **To configure coders:**

1. Open the 'Coders' page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders**).

Figure 4-12: Coders

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

2. From the 'Coder Name' drop-down list, select **G.711A-law** and **G.711U-law**.
3. Click **Submit**.

4.9 Step 9: Configuring Proxy and Registration

The following describes how to configure the SIP Proxy and Registration. This configuration includes setting a redundant route for the Microsoft Lync Proxy Set.

➤ **To configure Proxy and Registration:**

1. Open the 'Proxy & Registration' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).

Figure 4-13: Proxy & Registration

Use Default Proxy	No
Proxy Name	
Redundancy Mode	Parking
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Always Use Proxy	Disable
Redundant Routing Mode	Routing Table
SIP ReRouting Mode	Standard Mode
Enable Registration	Disable
Registrar Transport Type	Not Configured
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	ITSP-GW.lync.local
Gateway Registration Name	

2. In the 'Gateway Name' field, enter the Gateway FQDN Name (e.g., "ITSP-GW.lync.local").



Note: You configure this name in Section 4.17.3 on page 58).

4.10 Step 10: Configuring Proxy Sets Tables

The following describes how to configure the proxy set tables. You need to configure two proxy sets - one for the Telenet SIP trunk and the other for the Microsoft Lync server.

➤ **To configure Proxy Sets Table 1 for Microsoft Lync:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network**> **Proxy Sets Table**).

Figure 4-14: Proxy Sets Table 1

Proxy Set ID 2 → 1

	Proxy Address	Transport Type
1	FE-Lync.Lync.local 4 →	TLS
2		
3		
4		
5		

3 →

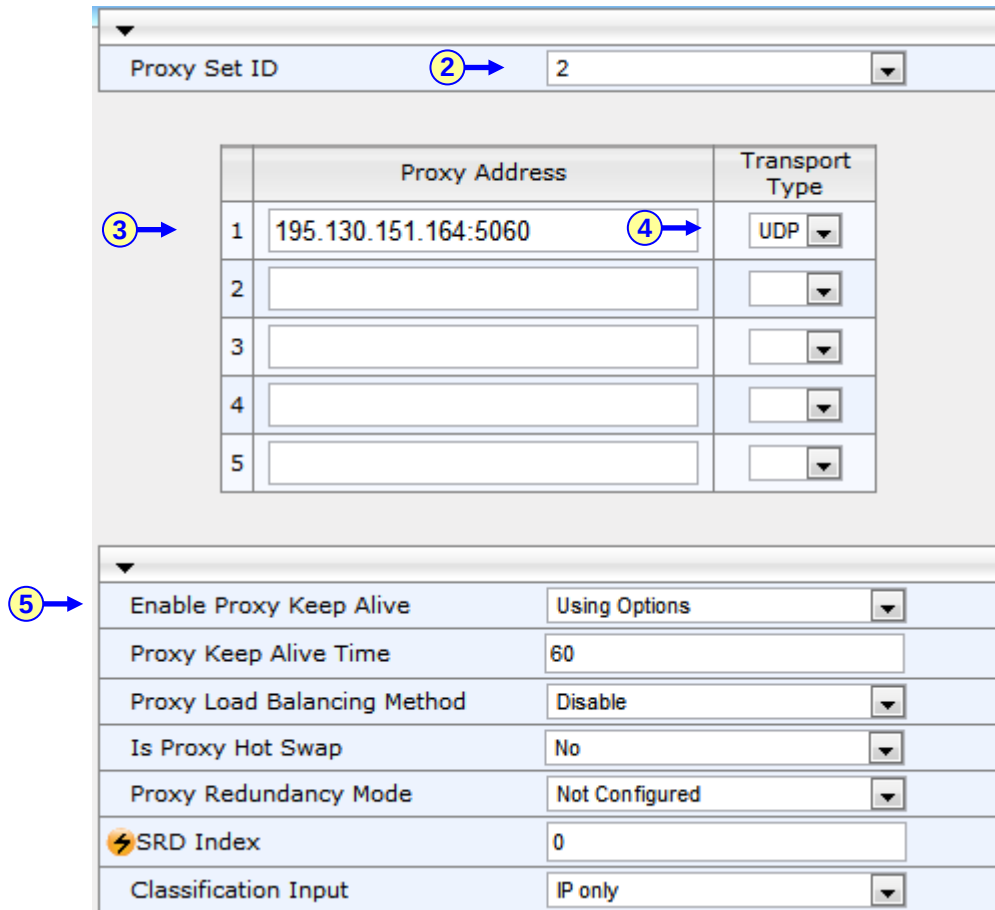
5 →	Enable Proxy Keep Alive	Using Options
	Proxy Keep Alive Time	60
6 →	Proxy Load Balancing Method	Round Robin
7 →	Is Proxy Hot Swap	Yes
	Proxy Redundancy Mode	Not Configured
	SRD Index	0
	Classification Input	IP only

2. From the 'Proxy Set ID' drop-down list, select **1**.
3. Configure the Microsoft Lync Server SIP Trunking IP address or FQDN and Destination Port (e.g., "FE-Lync.Lync.local").
4. From the 'Transport Type' drop-down list, select **TLS**.
5. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**.
6. From the 'Proxy Load Balancing Method' drop-down list, select **Round Robin**.
7. From the 'Is Proxy Hot Swap' drop-down list, select **Yes**.

➤ **To configure Proxy Sets Table 2 for Telenet SIP Trunk:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network**> **Proxy Sets Table**).

Figure 4-15: Proxy Sets Table 2



Proxy Set ID 2

	Proxy Address	Transport Type
1	195.130.151.164:5060	UDP
2		
3		
4		
5		

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 0

Classification Input IP only

2. From the 'Proxy Set ID' drop-down list, select **2**.
3. Configure the Telenet IP address or FQDN and Destination Port (e.g., 195.130.151.164:5060'.
4. From the 'Transport Type' drop-down list, select **UDP**.
5. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**.

4.11 Step 11: Configuring IP Profile

The following describes how to configure the IP Profile. In this configuration, the IP Profile is used to configure the SRTP/TLS mode and the Coder Group (see Section 4.8 on page 41).

You must configure Microsoft Lync to work in secure mode (SRTP/TLS); while, the Telenet SIP trunk is configured in non-secure mode RTP/UDP.

➤ **To configure IP Profile for Microsoft Lync:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** > **IP Profile Settings**).

Figure 4-16: IP Profile Settings

Profile ID	1
Profile Name	Lync
Common Parameters	
Gateway Parameters	
Fax Signaling Method	No Fax
Play Ringback Tone to IP	Don't Play
Enable Early Media	Enable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Preferable - Single Media
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Default Coder Group
Remote RTP Base UDP Port	0
First Tx DTMF Option	RFC 2833

2. From the 'Profile ID' drop-down list, select **1**.
3. From the 'Media Security Behavior' drop-down list, select **Preferable – Single Media**.
4. Click **Submit**.

➤ **To configure IP Profile for Telenet SIP Trunk:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** > **IP Profile Settings**).

Figure 4-17: IP Profile Settings

▼	
Profile ID	2
Profile Name	TeleneT
▲ Common Parameters	
▼ Gateway Parameters	
Fax Signaling Method	G.711 Transport
Play Ringback Tone to IP	Play
Enable Early Media	Disable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Disable
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Default Coder Group
Remote RTP Base UDP Port	0
First Tx DTMF Option	RFC 2833

2. From the 'Profile ID' drop-down list, select **2**.
3. From the 'Fax Signaling Method' drop-down list, select **G.711 Transport**.
4. From the 'Play Ringback Tone to IP' drop-down list, select **Play**.
5. From the 'Media Security Behavior' drop-down list, select **Disable**.
6. Click **Submit**.

4.12 Step 12: Configuring IP Group Tables

The following describes how to create IP groups. Each IP group represents a SIP entity in the gateway's network. You need to create IP groups for the following entities:

- Lync Server 2010 - Mediation Server
- Telenet SIP Trunk

These IP groups are later used by the IP-to-IP application for routing calls.

➤ **To configure IP Group Table 1:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network**> **IP Group Table**).

Figure 4-18: IP Group Table 1

▼	
Index	1
▼ Common Parameters	
Type	SERVER
Description	Lync
Proxy Set ID	1
SIP Group Name	
Contact User	
IP Profile ID	0
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

2. From the 'Index' drop-down list, select **1**.
3. From the 'Type' drop-down list, select **SERVER**.
4. From the 'Proxy Set ID' drop-down list, select **1**.

➤ **To configure IP Group Table 2:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network**> **IP Group Table**).

Figure 4-19: IP Group Table 2

▼	
Index	2
▼ Common Parameters	
Type	SERVER
Description	Telenet
Proxy Set ID	2
SIP Group Name	
Contact User	
IP Profile ID	0
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

2. From the 'Index' drop-down list, select **2**.
3. From the 'Type' drop-down list, select **SERVER**.
4. From the 'Proxy Set ID' drop-down list, select **2**.

4.13 Step 13: Configuring Trunk Group

The following describes how to add a Fax to the E-SBC device.

➤ **To configure Trunk Group Table:**

1. Open the 'Trunk Group Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group**).

Figure 4-20: Trunk Group Table

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 2 FXS			1	32997277	3	0

2. Configure **Group Index 1**:

- From the 'Module' drop-down list, select the Module FXS type (e.g., **Module 2 FXS**).
- In the 'Channels' field, enter the channel number (e.g., 1).
- In the 'Phone Number' field, enter the FAX number (e.g., 32997277).
- In the 'Trunk Group ID' field, enter the Trunk Group ID (e.g., 3).

➤ **To configure Trunk Group Settings:**

1. Open the 'Trunk Group Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group Settings**).

Figure 4-21: Trunk Group Settings

Index	Trunk Group ID	Channel Select Mode	Registration Mode
1	3	By Dest Phone Number	Don't Register

2. Configure **Row Index 1**:

- In the 'Trunk Group ID' field, enter the Trunk Group ID (e.g., 3).
- From the 'Channel Select Mode' drop-down list, enter the appropriate Channel Select mode (e.g., By Dest. Phone Number).

4.14 Step 14: Configuring Routing

The following describes how to configure the IP-to-IP routing table.

The device IP-to-IP routing rules are configured in the 'IP to Trunk Group Routing' and 'Tel to IP Routing' tables. These tables provide enhanced IP-to-IP call routing capabilities for routing received SIP messages, such as INVITE messages to a destination IP address. The routing rule must match one of the following input characteristics:

- Source IP Group
- Source Phone Prefix and/or Source Host Prefix

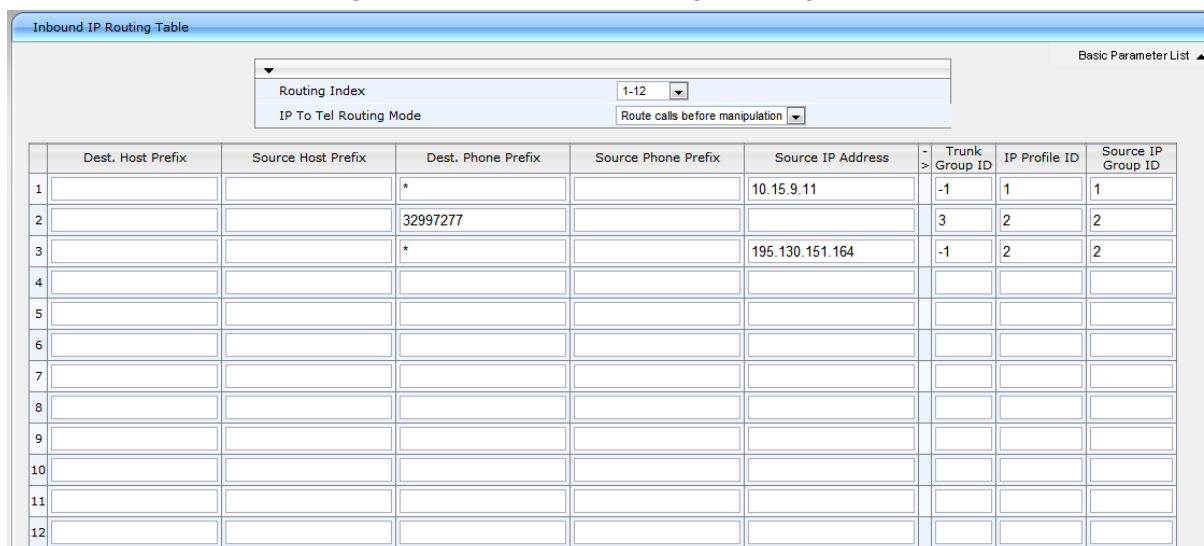
It is crucial that you adhere to the following guidelines when configuring your IP-to-IP routing rules:

- Ensure that your routing rules are accurate and correctly defined.
- Ensure that your routing rules from **source IP Group** to **destination IP Group** are accurately defined to be eligible for the desired call routing outcome.
- Avoid (if possible) using the asterisk (*) symbol to indicate "any" for a specific parameter in your routing rules. This constitutes a weak routing rule. For strong routing rules, enter specific letter or numeric character values.

➤ To configure the IP to Trunk Group Routing Table:

1. Open the 'IP to Trunk Group Routing Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP > Routing > IP to Trunk Group Routing Table**).

Figure 4-22: IP to Trunk Group Routing Table



	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IP Group ID
1			*		10.15.9.11	-1	1	1
2			32997277			3	2	2
3			*		195.130.151.164	-1	2	2
4								
5								
6								
7								
8								
9								
10								
11								
12								

2. **Configure Row Index 1:** Calls arriving from IP 10.15.9.11 (i.e., Microsoft Lync server) are sent to the 'Tel to IP Routing Table' (-1) with 'IP Profile ID' = **1** and marked as 'Source IPGroup ID' = **1**.
3. **Configure Row Index 2:** Calls arriving to number 32997277 (i.e., Fax number) are sent to Trunk Group ID **3** (i.e., FXS Card).
4. **Configure Row Index 3:** Calls arriving from IP 195.130.151.164 (i.e., Telenet Sip Trunk) are sent to the 'Tel to IP Routing Table' (-1) with 'IP Profile ID' = **2** and marked as 'Source IPGroup ID'=2.

➤ **To configure Tel to IP Routing Table:**

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

Figure 4-23: Tel to IP Routing Table

Outbound IP Routing Table

Routing Index

Tel To IP Routing Mode

1-10

Route calls before manipulation

Basic Parameter List

	Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	Dest. SRD	IP Profile ID	
1	1			*	*	*				Not Configured	2	-1	2	n/a
2	2			*	*	*				Not Configured	1	-1	1	n/a
3	-1			3	*	*				Not Configured	2	-1	2	n/a
4	-1									Not Configured	-1			
5	-1									Not Configured	-1			
6	-1									Not Configured	-1			
7	-1									Not Configured	-1			
8	-1									Not Configured	-1			
9	-1									Not Configured	-1			
10	-1									Not Configured	-1			

2. **Configure Row Index 1:** Calls from Source IPGroup ID **1** (i.e., from Microsoft Lync) is sent to 'Dest. IPGroup ID **2** (i.e., to Telenet).
3. **Configure Row Index 2:** Calls from Source IPGroup ID **2** (i.e., from Telenet) is sent to 'Dest. IPGroup ID **1** (i.e., to Lync)
4. **Configure Row Index 3:** Calls from Source Trunk Group ID **3** (i.e., FXS Card) is sent to 'Dest. IPGroup ID **2** (i.e., to Telenet).



Note: The Routing configuration may change according to the local deployment topology.

4.15 Step 15: Configuring Manipulation

The following describes how to configure the manipulation tables. The Manipulation Tables sub-menu allows you to configure number of manipulations and mappings of NPI/TON to SIP messages.

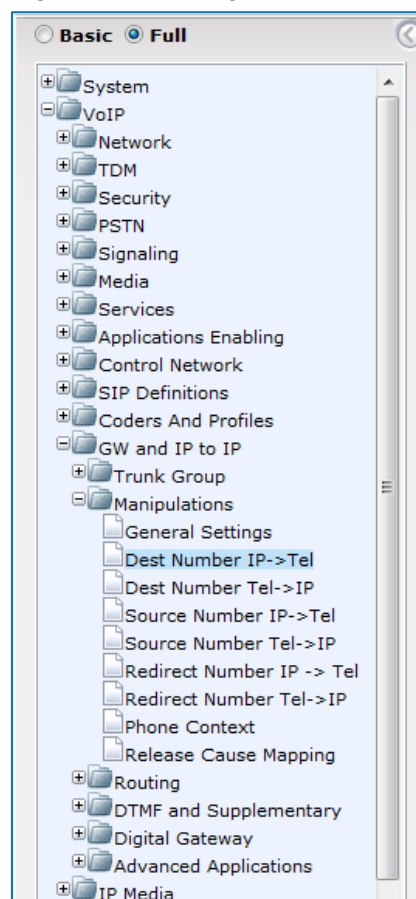


Note: Adapt the manipulation table according to your environment dial plan.

➤ **To configure Manipulation Tables:**

1. Open the 'Manipulation Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Manipulations**).

Figure 4-24: Manipulation Tables



The following includes examples for number manipulation on destination and source numbers in the Tel-to-IP tables:

➤ **To configure Destination Phone Number Manipulation Table for Tel -> IP Calls Table:**

1. Open the 'Destination Phone Number Manipulation Table for Tel -> IP calls' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Manipulations** sub-menu > **Dest Number Tel > IP**).

Figure 4-29: Destination Phone Number Manipulation Table for Tel -> IP Calls

Destination Phone Number Manipulation Table for Tel -> IP Calls									
Note: Select row index to modify the relevant row.									
Add									
Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave
1	-1	1	+	*	1	0	00		255
2	-1	2	32	*	0	0	+32		255

- **Index #1** defines the destination number manipulation of calls from Lync Server.
 - For all calls received from Source IP Group 1 (i.e., from Lync Server) and the destination number prefix begins with '+', remove the '+' and add '00' to the number.
- **Index #2** defines the destination number manipulation of calls from Telenet SIP Trunk.
 - For all calls received from Source IP Group 2 (i.e., from Telenet SIP Trunk) and the destination number prefix begins with '32', add the '+32' prefix to the number.

➤ **To configure Source Phone Number Manipulation Table for Tel -> IP Calls Table:**

1. Open the 'Source Phone Number Manipulation Table for Tel -> IP calls' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Manipulations** sub-menu > **Source Number Tel > IP**).

Figure 4-30: Source Phone Number Manipulation Table for Tel -> IP Calls Page

Source Phone Number Manipulation Table for Tel -> IP Calls										
Note: Select row index to modify the relevant row.										
Add										
Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave	Presentation
1	-1	1	*	+32	3	0			255	Not Configured
2	-1	2			0	0	+		255	Not Configured

- **Index #1** defines the Source number manipulation of calls from Lync Server.
 - For all calls received from Source IP Group 1 (i.e., from Lync Server) and the Source number prefix begins with '+', remove the '+32' to the number.
- **Index #2** defines the Source number manipulation of calls from Telenet SIP Trunk.
 - For all calls received from Source IP Group 2 (i.e., from Telenet SIP Trunk), add a '+' as a prefix to the number.

4.16 Step 16: Configuring Message Manipulations

The 'Message Manipulations' page allows you to define up to 200 SIP message manipulation rules. This manipulation includes insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. SIP message manipulation rules configured on this page will be assigned to an IP Group and determined whether they must be applied to inbound or outbound messages. This step describes the Message Manipulation for working with Telenet SIP Trunk for the Call Transfer/Forward feature using Microsoft Lync.

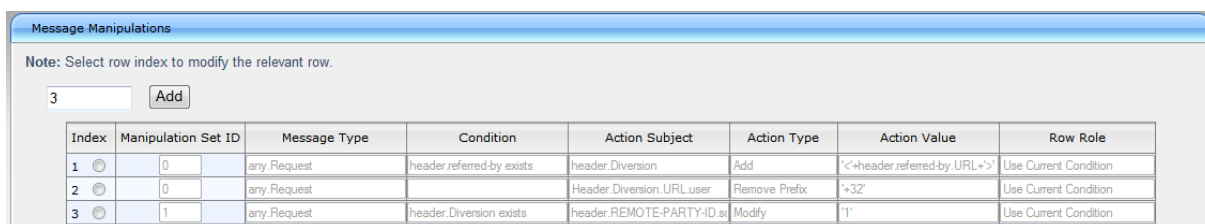
Two sets of manipulation are defined:

- **Set ID 0** is assigned to the gateway inbound manipulation set.
- **Set ID 1** is assigned to Telenet IP Group (IP Group 2) as an Outbound Message Manipulation Set (Row index 3)

➤ **To configure SIP message manipulations:**

1. Open the 'Message Manipulations' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** sub-menu > **Message**).

Figure 4-33: SIP Message Manipulation



Note: Select row index to modify the relevant row.

3

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
1	0	any Request	header.referred-by exists	header.Diversion	Add	'<'+header.referred-by.URL+>'	Use Current Condition
2	0	any Request	header.Diversion exists	Header.Diversion.URL.user	Remove Prefix	'+32'	Use Current Condition
3	1	any Request	header.Diversion exists	header.REMOTE-PARTY-ID.s	Modify	'1'	Use Current Condition

2. Configure the following manipulation rules:
 - **Row Index #1:** If a **Referred-By** header exists in the request coming from the Lync Server, then this manipulation row adds a **Diversion** Header with the **Referred-By URL** header.
 - **Row Index #2:** For any request coming from the Lync Server, this manipulation row removes the prefix of **'+32'**, in the **user** part in the **Diversion** header.
 - **Row Index #3:** If a **Diversion** header exists in the request coming to Telenet SIP Trunk, then this manipulation row modifies a **Remote-Party** Header with the **screen** part to **'1'** (i.e., yes).

- **To assign a manipulation Set ID 1 to IP Group 2:**
1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network**> **IP Group Table**).

Figure 4-34: IP Group Table

IP Group Table	
Index	2

2

Common Parameters	
Type	SERVER
Description	Telenet
Proxy Set ID	2
SIP Group Name	
Contact User	
IP Profile ID	2

Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

SBC Parameters	
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	1

3

2. From the 'Index' drop-down list, select **2**.
3. In the 'Outbound Message Manipulation Set' field, enter **"1"**.

- To assign manipulation set ID 0 to gateway inbound manipulation set:
1. Open the 'Admin' page, by appending the case-sensitive suffix 'AdminPage' to the Media Gateway's IP address in your Web browser's URL field (e.g., <http://10.15.7.131/AdminPage>).
 2. On the left pane, click **ini Parameters**.
 3. In the 'Parameter Name' field, enter "GWINBOUNDMANIPULATIONSET".
 4. In the 'Enter Value' field, enter "0".

Figure 4-35: Output Window

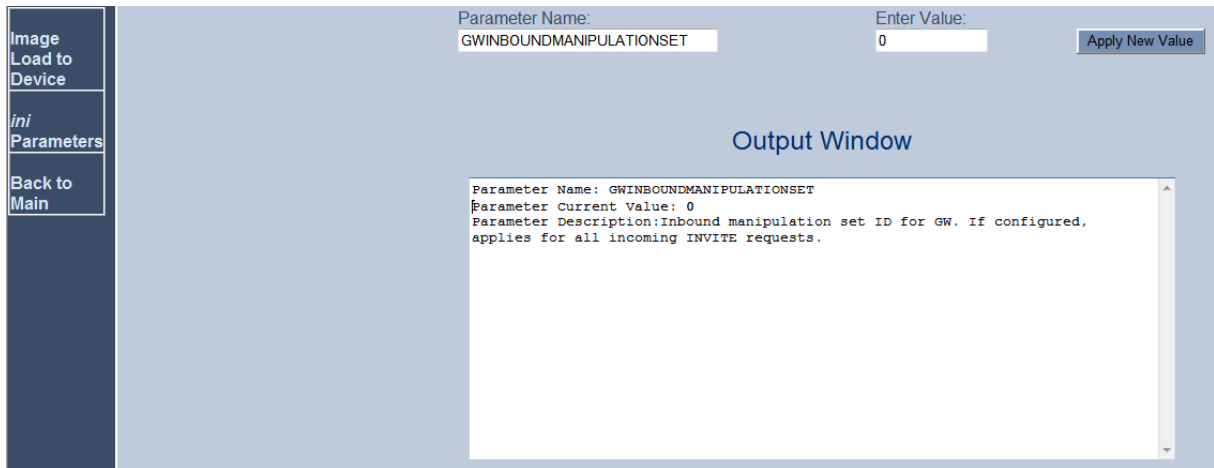


Image Load to Device

ini Parameters

Back to Main

Parameter Name: GWINBOUNDMANIPULATIONSET

Enter Value: 0

Apply New Value

Output Window

```
Parameter Name: GWINBOUNDMANIPULATIONSET
Parameter Current Value: 0
Parameter Description: Inbound manipulation set ID for GW. If configured,
applies for all incoming INVITE requests.
```

5. Click **Apply New Value**.

4.17 Step 17: Configuring SIP TLS Connection

The following describes how to configure the AudioCodes gateways for implementing a TLS connection with the Microsoft Lync Mediation server. The steps described in this section are essential elements for the configuration of a secure SIP TLS connection.

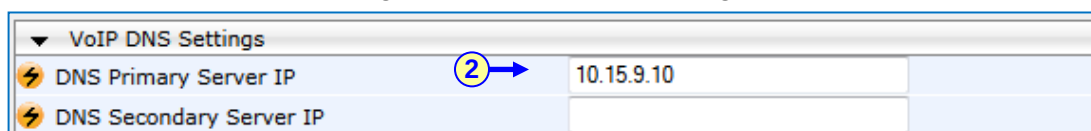
4.17.1 Step 17-1: Configuring VoIP DNS Settings

The following describes how to define the VoIP LAN DNS server, which is a necessary action when a FQDN is configured (as in this scenario configuration, see Section 4.9 on page 9).

➤ **To configure the VoIP DNS settings:**

1. Open the 'DNS Settings' page (**Configuration** tab > **VoIP** menu > **DNS** > **DNS Settings**).

Figure 4-25: VoIP DNS Settings



VoIP DNS Settings	
DNS Primary Server IP	10.15.9.10
DNS Secondary Server IP	

2. Set the following parameters:

- **DNS Primary Server IP:** <Primary DNS IP-Address> (e.g., 10.15.9.10).
- **DNS Secondary Server IP:** <Secondary DNS IP-Address>.

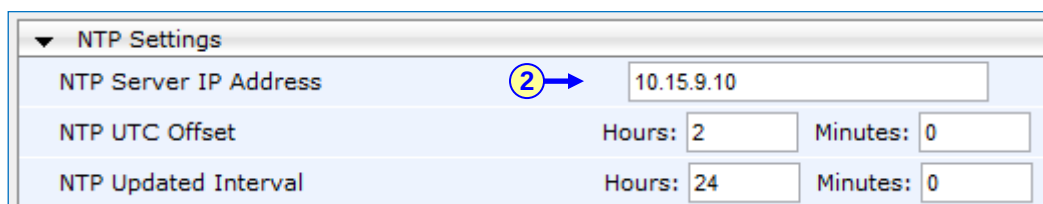
4.17.2 Step 17-2: Configuring NTP Server

The following describes how to configure the NTP Server IP address. It is recommended to implement an NTP server (third-party) so that the E-SBC device receives the accurate current date and time. This is necessary for validating remote parties' certificates.

➤ **To configure NTP Settings:**

1. Open the 'Application Settings' page (**Configuration** tab > **System** menu > **Application Settings**).

Figure 4-26: NTP Settings



NTP Settings	
NTP Server IP Address	10.15.9.10
NTP UTC Offset	Hours: 2 Minutes: 0
NTP Updated Interval	Hours: 24 Minutes: 0

2. In the 'NTP Server IP Address' field, enter the NTP Server IP-Address (e.g., 10.15.9.10).

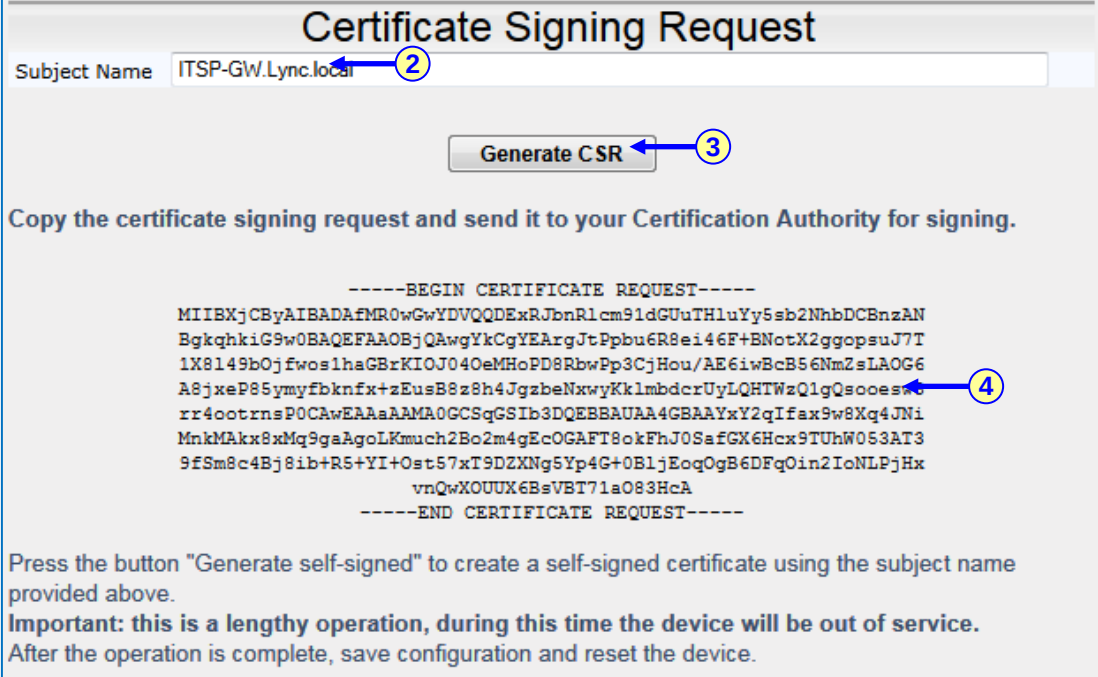
4.17.3 Step 17-3: Configuring a Certificate

The following describes how to exchange a certificate with the Microsoft Certificate Authority. The certificate is used by the E-SBC device to authenticate the connection with the management computer (i.e., the computer used to manage the E-SBC using the embedded Web interface.).

➤ **To configure a certificate:**

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

Figure 4-27: Certificates Page



Certificate Signing Request

Subject Name 2

3

Copy the certificate signing request and send it to your Certification Authority for signing.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBXjCBYwIBADAFMR0wGwYDVQQDEXRJbnRlcm91dGUuTHluYy5sb2NhbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwYkCgYEAJtPpbu6R8ei46F+BNotX2ggopsuJ7T
1X8149bOjfwos1haGBrKIOJ04OeMHoPD8RbwPp3CjHou/AE6iwBcB56NmZsLAOG6
A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxwyKklmbdcrUyLQHTWzQ1gQsooesw
rr4ootrnsPOCAwEAAsAAAMA0GCSqGSIb3DQEBAUAA4GBAAyY2qIfax9w8Xq4JNi
MnkMAkx8xMq9gaAgoLKMuch2Bo2m4gEcOGAFT8okFhJ0SafGX6Hcx9TUhW053AT3
9fSm8c4Bj8ib+R5+YI+Ost57xT9DZXNg5Yp4G+0BljEoqOgB6DFqOin2IoNLPjHx
vnQwXOUUX6BsVBT71aO83HcA
-----END CERTIFICATE REQUEST-----

```

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.

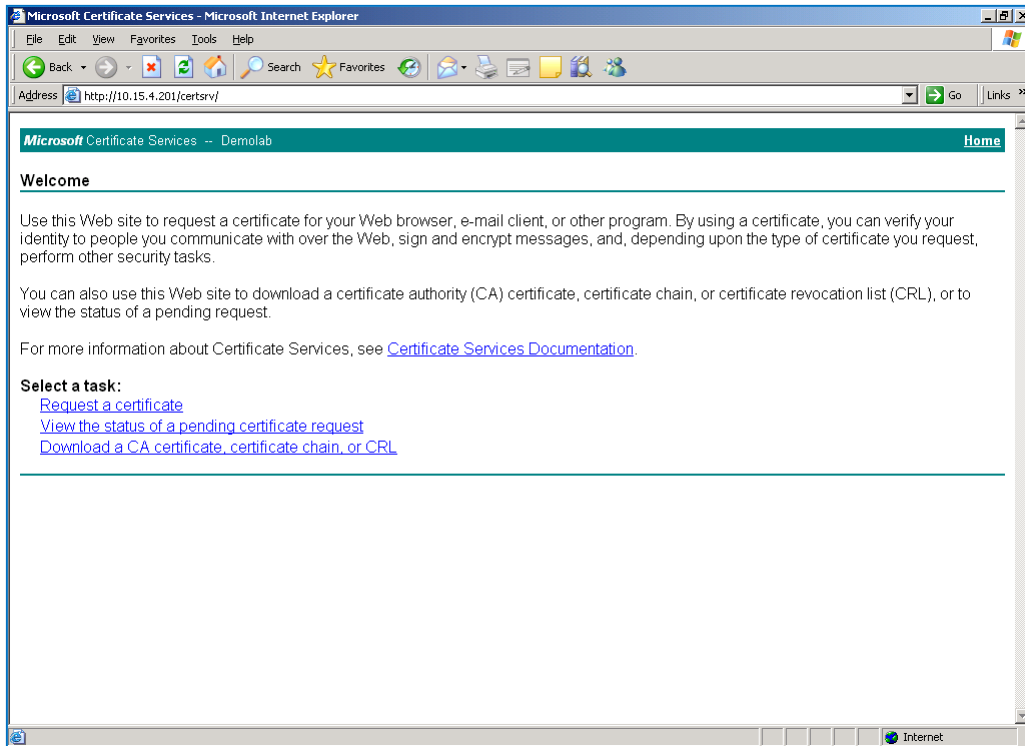
Important: this is a lengthy operation, during this time the device will be out of service.

After the operation is complete, save configuration and reset the device.

3. In the 'Subject Name' field, enter the Media Gateway name (i.e., ITSP-GW.Lync.local)
4. Click **Generate CSR**; a Certificate request will be generated.
5. Copy the CSR (from the line "-----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST-") to a .txt file (such as Notepad), and then save it to a folder on your computer as *certreq.txt*.

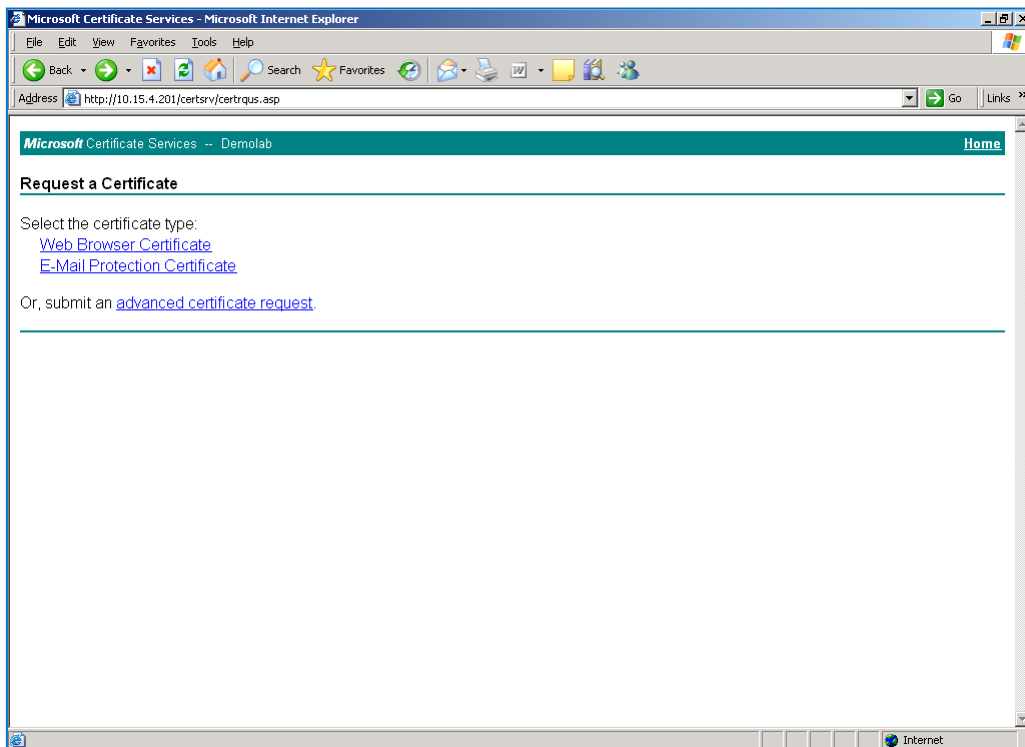
6. Navigate to the 'Server http://<Certificate Server>/CertSrv' certificate.

Figure 4-28: Microsoft Certificate Services Web Page



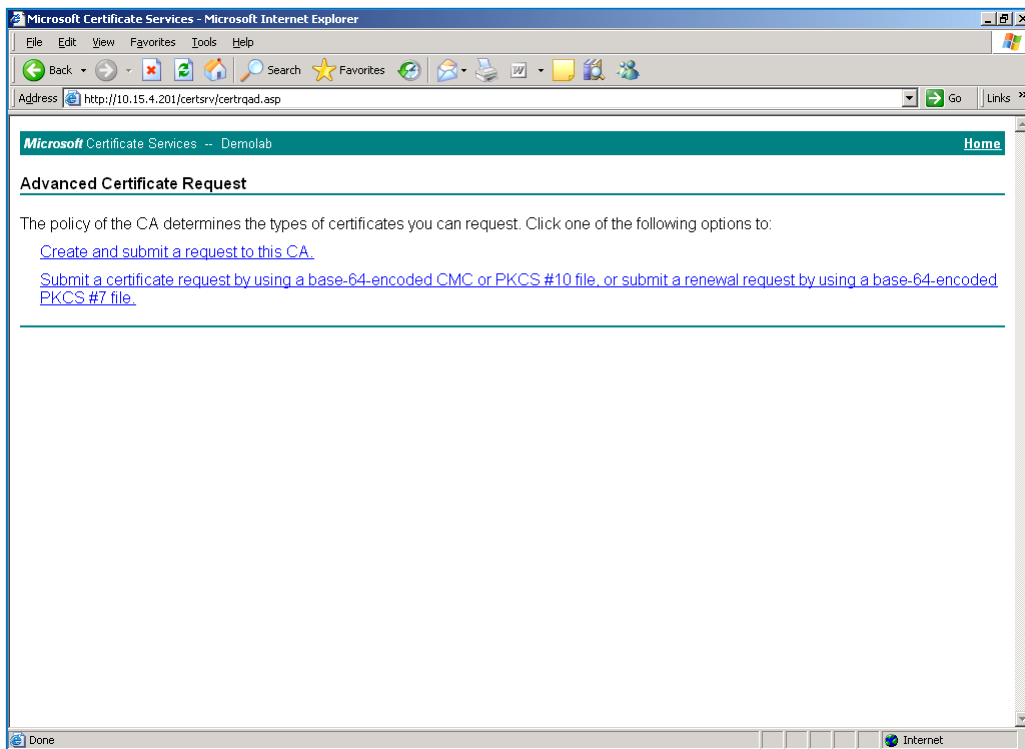
7. Click the **Request a Certificate** link; the following screen appears.

Figure 4-29: Request a Certificate Page



8. Click the **Advanced Certificate Request** link, and then click **Next**.

Figure 4-30: Advanced Certificate Request Page



9. Click the **Submit a Certificate request by using base64 encoded...** link, and then click **Next**.

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

The screenshot shows a web browser window titled "Microsoft Active Directory Certificate Services - Windows Internet Explorer" with the address bar showing "http://10.15.4.201/certsrv/certreq.asp". The page header is "Microsoft Active Directory Certificate Services -- Lync-DC-LYNC-CA" with a "Home" link. The main heading is "Submit a Certificate Request or Renewal Request". Below this, a text box explains: "To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box." The "Saved Request:" section contains a text area with a base-64 encoded request. Below this is a "Certificate Template:" dropdown menu set to "Web Server". The "Additional Attributes:" section has an empty "Attributes:" text box. A "Submit >" button is at the bottom right.

10. Open the *certreq.txt* file that you created and saved (see Step 5), and then copy its contents to the 'Base64 Encoded Certificate Request' text box.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**; the following screen appears:

Figure 4-32: Download a CA Certificate, Certificate Chain, or CRL Page

The screenshot shows a web browser window titled "Microsoft Certificate Services - Microsoft Internet Explorer" with the address bar showing "http://10.15.4.201/certsrv/certcar.asp". The page header is "Microsoft Certificate Services -- Demolab" with a "Home" link. The main heading is "Download a CA Certificate, Certificate Chain, or CRL". Below this, a text box explains: "To trust certificates issued from this certification authority, [install this CA certificate chain](#)." Another text box says: "To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method." The "CA certificate:" section has a dropdown menu with "Current [Demolab]" selected. The "Encoding method:" section has two radio buttons: "DER" (selected) and "Base 64". At the bottom, there are three links: "Download CA certificate", "Download CA certificate chain", and "Download latest base CRL".

13. Click the **Base 64** encoding option, and then click the **Download CA certificate** link.
14. Save the file as '*gateway.cer*' in a folder on your computer.
15. Navigate to the 'Server [http://<Certificate Server>/CertSrv](#)' certificate.
16. Click either one of the following links:
 - Download a CA certificate
 - Download CA certificate chain
 - Download latest base CRL
17. Under the Encoding method group, do the following:
18. Click the **Base 64** encoding method option.

19. Click the **Download CA certificate** link.
20. Save the file as 'certroot.cer' in a folder on your computer.
21. Navigate back (in the E-SBC device) to the 'Certificates' page.

Figure 4-33: Certificates Page

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
 After the operation is complete, save configuration and reset the device.

Certificate Files

Send "Server Certificate" file from your computer to the device
 C:\Gateway.cer 22

Send "Trusted Root Certificate Store" file from your computer to the device
 C:\Certroot.cer 23

Send "Private Key" file from your computer to the device

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

22. On the 'Certificates' page, under the 'Send Server Certificate...' field, click **Browse** and select the 'Gateway.cer' certificate file that you saved on your local disk (see Step 14), and then click **Send File** to upload the certificate.
23. On the 'Certificates' page, in the 'Trusted Root Certificate Store' field, click **Browse** and select the 'Certroot.cer' certificate file that you saved on your local disk (see Step 20), and then click **Send File** to upload the certificate.
24. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, choose **Maintenance Actions**).

4.18 Step 18: Resetting the Gateway

After you have completed the gateway configuration as described in the steps above, burn the configuration to the gateway's flash memory and reset the gateway.

- Click the **Reset** button to burn the configuration to flash and reset the gateway (ensure that the 'Burn to FLASH' field is set to **Yes**).

Figure 4-34: Resetting the Gateway

The screenshot shows the AudioCodes Mediant 1000 - MSBG web interface. The top navigation bar includes the AudioCodes logo, the device name 'Mediant 1000 - MSBG', and buttons for 'Submit', 'Burn', 'Device Actions', 'Home', 'Help', and 'Log off'. The left sidebar has tabs for 'Configuration', 'Maintenance', and 'Status & Diagnostics'. The 'Maintenance' tab is selected, showing a tree view with 'Maintenance Actions' highlighted. The main content area is titled 'Maintenance Actions' and contains three sections: 'Reset Configuration' with a 'Reset' button and a 'Burn To FLASH' dropdown set to 'Yes'; 'LOCK / UNLOCK' with a 'LOCK' button and 'Gateway Operational State' set to 'UNLOCKED'; and 'Save Configuration' with a 'BURN' button.



Note: Reset with BURN to FLASH is required.

Reader's Notes

A AudioCodes INI File

The following displays the E-SBC device ini file. This file reflects the configuration described in Section 4 on page 29.

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

;Board: Mediant 1000 - MSBG
;Serial Number: 3589366
;Slot Number: 1
;Software Version: 6.20A.036.004
;DSP Software Version: 620AE3 => 620.08
;Board IP Address: 10.15.7.131
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.7.130
;Ram size: 512M   Flash size: 64M
;Num of DSP Cores: 13   Num DSP Channels: 51
;Profile: NONE
;Key features;;Board Type: Mediant 1000 - MSBG ;PSTN Protocols: ISDN IUA=4
CAS ;Coders: G723 G729 GSM-FR G727 ILBC ;E1Trunks=4 ;T1Trunks=4 ;IP Media:
Conf VXML VoicePromptAnnounc(H248.9) ;Channel Type: RTP PCI DspCh=240
IPMediaDspCh=240 ;DSP Voice features: EC128mSec AdditionTimeslotSummation
FastSlowPlayback BargeIn PatternDetector IpmDetector ;DATA features: Routing
FireWall&VPN WAN Advanced-Routing ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;Control Protocols: MSFT MGCP MEGACO
SIP SASurvivability SBC=120 ;Default features;;Coders: G711 G726;

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

[SYSTEM Params]

DNSPriServerIP = 10.15.9.10
SyslogServerIP = 10.15.45.200
EnableSyslog = 1
NTPServerIP = 10.15.9.10
NTPServerUTCOffset = 7200
PM_VEDSPUtil = '1,64,72,15'

[BSP Params]
```

```
PCMLawSelect = 3
WanInterfaceName = 'GigabitEthernet 0/0'
```

```
[Analog Params]
```

```
[ControlProtocols Params]
```

```
AdminStateLockControl = 0
```

```
[MGCP Params]
```

```
[MEGACO Params]
```

```
EP_Num_0 = 0
```

```
EP_Num_1 = 1
```

```
EP_Num_2 = 1
```

```
EP_Num_3 = 0
```

```
EP_Num_4 = 0
```

```
[PSTN Params]
```

```
[SS7 Params]
```

```
[Voice Engine Params]
```

```
RFC2833TxPayloadType = 101
```

```
ENABLEMEDIASECURITY = 1
```

```
SRTPTxPacketMKISize = 1
```

```
CallProgressTonesFilename = 'usa_tones_13.dat'
```

```
[WEB Params]
```

```
LogoWidth = '145'
```

```
HTTPSCipherString = 'RC4:EXP'
```

```
[SIP Params]
```

```
MEDIACHANNELS = 120
```

```
SIPDESTINATIONPORT = 5067
```

```
PLAYRBTONE2TEL = 1
```

```
USESIPURIFORDIVERSIONHEADER = 1
```

```
GWDEBUGLEVEL = 5
```

```
ENABLERPIHEADER = 1
```

```
ENABLEEARLYMEDIA = 1
```

```
SIPGATEWAYNAME = 'ITSP-GW.Lync.local'
```

```
STATICNATIP = 195.189.192.154
```

```
ADDTON2RPI = 0
```

```
ISFAXUSED = 2
TLSLOCALSIPPORT = 5067
MEDIASEcurityBEHAVIOUR = 3
IGNOREALERTAFTEREARLYMEDIA = 1
OPTIONUSERPART = 'empty'
FORKINGHANDLINGMODE = 1
ENABLESBCAPPLICATION = 1
ENABLEIP2IPAPPLICATION = 1
ENABLEEARLY183 = 1
GWINBOUNDMANIPULATIONSET = 0
```

```
[SCTP Params]
```

```
[VXML Params]
```

```
[IPsec Params]
```

```
[Audio Staging Params]
```

```
[SNMP Params]
```

```
;
; *** TABLE InterfaceTable ***
;
;
```

```
[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID,
InterfaceTable_InterfaceName;
InterfaceTable 0 = 6, 10, 10.15.7.131, 16, 10.15.7.130, 1, Voice;
```

```
[ \InterfaceTable ]
```

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

```
;
; *** TABLE PREFIX ***
;
;
```

```
[ PREFIX ]
```

```
; ** NOTE: Changes were made to active configuration.
; **      The data below is different from current values.
FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress,
PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort,
PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID,
PREFIX_SrcHostPrefix, PREFIX_TransportType, PREFIX_SrcTrunkGroupID,
PREFIX_DestSRD;
PREFIX 0 = *, , *, 2, 255, 0, 1, , 2, , -1, -1, -1;
PREFIX 1 = *, , *, 1, 255, 0, 2, , 1, , -1, -1, -1;
PREFIX 2 = *, , *, 2, 255, 0, -1, , 2, , -1, 3, -1;
```

```
[ \PREFIX ]
```

```
;
; *** TABLE TrunkGroup ***
;
;
```

```
[ TrunkGroup ]
```

```
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId,
TrunkGroup_Module;
TrunkGroup 0 = 3, 255, 1, 1, 32997277, 0, 255, 2;
```

```
[ \TrunkGroup ]
```

```
;
; *** TABLE NumberMapTel2Ip ***
;
;
```

```
[ NumberMapTel2Ip ]
```

```
; ** NOTE: Changes were made to active configuration.
; **      The data below is different from current values.
FORMAT NumberMapTel2Ip_Index = NumberMapTel2Ip_DestinationPrefix,
NumberMapTel2Ip_SourcePrefix, NumberMapTel2Ip_SourceAddress,
NumberMapTel2Ip_NumberType, NumberMapTel2Ip_NumberPlan,
NumberMapTel2Ip_RemoveFromLeft, NumberMapTel2Ip_RemoveFromRight,
NumberMapTel2Ip_LeaveFromRight, NumberMapTel2Ip_Prefix2Add,
NumberMapTel2Ip_Suffix2Add, NumberMapTel2Ip_IsPresentationRestricted,
NumberMapTel2Ip_SrcTrunkGroupID, NumberMapTel2Ip_SrcIPGroupID;
NumberMapTel2Ip 1 = +, *, *, 255, 255, 1, 0, 255, 00, , 255, -1, 1;
NumberMapTel2Ip 2 = 32, *, *, 255, 255, 0, 0, 255, +32, , 255, -1, 2;
```

```
[ \NumberMapTel2Ip ]
```

```
;
; *** TABLE SourceNumberMapIp2Tel ***
;
;
```

```
[ SourceNumberMapIp2Tel ]
```

```

FORMAT SourceNumberMapIp2Tel_Index = SourceNumberMapIp2Tel_DestinationPrefix,
SourceNumberMapIp2Tel_SourcePrefix, SourceNumberMapIp2Tel_SourceAddress,
SourceNumberMapIp2Tel_NumberType, SourceNumberMapIp2Tel_NumberPlan,
SourceNumberMapIp2Tel_RemoveFromLeft, SourceNumberMapIp2Tel_RemoveFromRight,
SourceNumberMapIp2Tel_LeaveFromRight, SourceNumberMapIp2Tel_Prefix2Add,
SourceNumberMapIp2Tel_Suffix2Add,
SourceNumberMapIp2Tel_IsPresentationRestricted,
SourceNumberMapIp2Tel_SrcTrunkGroupID, SourceNumberMapIp2Tel_SrcIPGroupID;
SourceNumberMapIp2Tel 1 = *, *, *, 255, 255, 0, 0, 255, , , 255, -1, -1;

```

```
[ \SourceNumberMapIp2Tel ]
```

```

;
; *** TABLE SourceNumberMapTel2Ip ***
;
;

```

```
[ SourceNumberMapTel2Ip ]
```

```

FORMAT SourceNumberMapTel2Ip_Index = SourceNumberMapTel2Ip_DestinationPrefix,
SourceNumberMapTel2Ip_SourcePrefix, SourceNumberMapTel2Ip_SourceAddress,
SourceNumberMapTel2Ip_NumberType, SourceNumberMapTel2Ip_NumberPlan,
SourceNumberMapTel2Ip_RemoveFromLeft, SourceNumberMapTel2Ip_RemoveFromRight,
SourceNumberMapTel2Ip_LeaveFromRight, SourceNumberMapTel2Ip_Prefix2Add,
SourceNumberMapTel2Ip_Suffix2Add,
SourceNumberMapTel2Ip_IsPresentationRestricted,
SourceNumberMapTel2Ip_SrcTrunkGroupID, SourceNumberMapTel2Ip_SrcIPGroupID;
SourceNumberMapTel2Ip 1 = *, +32, *, 255, 255, 3, 0, 255, , , 255, -1, 1;
SourceNumberMapTel2Ip 2 = , , *, 255, 255, 0, 0, 255, +, , 255, -1, 2;

```

```
[ \SourceNumberMapTel2Ip ]
```

```

;
; *** TABLE PstnPrefix ***
;
;

```

```
[ PstnPrefix ]
```

```

FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId,
PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId,
PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix;
PstnPrefix 0 = *, -1, , 10.15.9.11, 1, 1, , ;
PstnPrefix 1 = 32997277, 3, , , 2, 2, , ;
PstnPrefix 2 = *, -1, , 195.130.151.164, 2, 2, , ;

```

```
[ \PstnPrefix ]
```

```

;
; *** TABLE AltRouteCauseTel2Ip ***
;
;

```

```
[ AltRouteCauseTel2Ip ]
```

```
FORMAT AltRouteCauseTel2Ip_Index = AltRouteCauseTel2Ip_ReleaseCause;
```

```
AltRouteCauseTel2Ip 0 = 503;

[ \AltRouteCauseTel2Ip ]

;
; *** TABLE ProxyIp ***
;
;

[ ProxyIp ]
FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = FE-Lync.Lync.local, 2, 1;
ProxyIp 1 = 195.130.151.164:5060, 0, 2;

[ \ProxyIp ]

;
; *** TABLE TxDtmfOption ***
;
;

[ TxDtmfOption ]
FORMAT TxDtmfOption_Index = TxDtmfOption_Type;
TxDtmfOption 0 = 4;

[ \TxDtmfOption ]

;
; *** TABLE TrunkGroupSettings ***
;
;

[ TrunkGroupSettings ]
; ** NOTE: Changes were made to active configuration.
; **      The data below is different from current values.
FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId,
TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode,
TrunkGroupSettings_GatewayName, TrunkGroupSettings_ContactUser,
TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType;
TrunkGroupSettings 0 = 3, 0, 4, , , -1, 255;

[ \TrunkGroupSettings ]

;;

[ 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_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedCodersMode, IpProfile_SBCMediaSecurityBehaviour,
IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversiionMode,
IpProfile_SBCHistoryInfoMode;
IpProfile 1 = Lync, 1, 1, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 1, -1,
1, 0, 3, -1, 1, 4, -1, 1, 1, 0, 0, , -1, 0, 0, -1, 0, 0, 0, 0, -1, 0, 8, 300,
400, -1, -1;
IpProfile 2 = Telenet, 1, 2, 2, 10, 10, 46, 40, 0, 0, 0, 1, 2, 0, 0, 1, 1, -
1, 1, 0, 2, -1, 1, 4, -1, 1, 1, 0, 0, , -1, 0, 0, -1, 0, 0, 0, 0, -1, 0, 8,
300, 400, -1, -1;

[ \IpProfile ]

;
;   *** TABLE ProxySet ***
;
;

[ ProxySet ]
FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput,
ProxySet_ProxyRedundancyMode;
ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;
ProxySet 1 = 1, 60, 1, 1, 0, 0, -1;
ProxySet 2 = 1, 60, 0, 0, 0, 0, -1;

[ \ProxySet ]

;
;   *** TABLE IPGroup ***
;
;

[ 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_ContactName;
IPGroup 1 = 0, Lync, 1, , , 0, -1, 0, 0, -1, 0, , 1, 1, -1, -1, -1, ;
IPGroup 2 = 0, Telenet, 2, , , 0, -1, 0, 0, -1, 0, , 1, 2, -1, -1, 1, ;

```

```
[ \IPGroup ]
```

```
;  
; *** TABLE CodersGroup0 ***  
;  
;
```

```
[ CodersGroup0 ]
```

```
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,  
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;  
CodersGroup0 0 = g711Alaw64k, 20, 0, -1, 0;  
CodersGroup1 1 = g711Ulaw64k, 20, 0, -1, 0;
```

```
[ \CodersGroup0 ]
```

```
;  
; *** TABLE MessageManipulations ***  
;  
;
```

```
[ MessageManipulations ]
```

```
FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,  
MessageManipulations_MessageType, MessageManipulations_Condition,  
MessageManipulations_ActionSubject, MessageManipulations_ActionType,  
MessageManipulations_ActionValue, MessageManipulations_RowRole;  
MessageManipulations 1 = 0, any.Request, "header.referred-by exists",  
header.Diversion, 0, '<'+header.referred-by.URL+'>', 0;  
MessageManipulations 2 = 0, any.Request, , Header.Diversion.URL.user, 6,  
'+32', 0;  
MessageManipulations 3 = 1, any.Request, "header.Diversion exists",  
header.REMOTE-PARTY-ID.screen, 2, '1', 0;
```

```
[ \MessageManipulations ]
```

```
[ \MessageManipulations ]
```

Reader's Notes

Configuration Note