

Microsoft® Lync™ Server 2013

Enhanced Gateway

Mediant Gateway family

# Configuration Note

## AudioCodes Enhanced Gateway for Microsoft Lync Server 2013



**Microsoft Partner**  
Gold Communications



February 2014

Document #: LTRT-40134



---

## Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
<b>2</b>	<b>Component Information.....</b>	<b>9</b>
2.1	AudioCodes Gateway Version .....	9
2.2	Microsoft Lync Server 2013 Version .....	9
<b>3</b>	<b>Assigning IP Address to PSTN Gateway.....</b>	<b>11</b>
3.1	Initial Access to the PSTN Gateway .....	11
3.1.1	Assigning IP Address to the Device .....	13
<b>4</b>	<b>Configuring the Enhanced Gateway.....</b>	<b>15</b>
4.1	Step 1: Configuring the Mediation Server as a Proxy .....	17
4.2	Step 2: Restricting Communication to Mediation Server Only .....	20
4.3	Step 3: Configuring TLS.....	21
4.3.1	Enabling TLS and Defining TLS Port.....	21
4.3.2	Configuring the NTP Server .....	22
4.3.3	Configuring the DNS Server .....	23
4.3.4	Configuring a Certificate .....	23
4.4	Step 4: Configuring TCP Transport Type.....	30
4.5	Step 5: Configuring Secure Real-Time Transport Protocol.....	31
4.6	Step 6: Configuring Voice Coders (with Silence Suppression) .....	33
4.7	Step 7: Configuring Comfort Noise and Gain Control .....	34
4.8	Step 8: Configuring Early Media .....	36
4.9	Step 9: Configuring PSTN Trunks.....	39
4.9.1	Enabling Trunks.....	39
4.9.2	Configuring the Channel Select Method.....	40
4.9.3	Configuring IP-to-Trunk Group Routing.....	41
4.9.4	Configuring the Trunk .....	42
4.9.5	Configuring the TDM Bus .....	44
4.10	Step 10: Configuring Normalization Rules for E.164 Format for PBX/PSTN Connectivity.....	45
4.10.1	Number Normalization Examples .....	49
4.11	Miscellaneous Configuration .....	52
4.11.1	Configuring SRTP Behavior upon Rekey Mode .....	52
<b>A</b>	<b>Configuring Lync Server 2013 .....</b>	<b>53</b>

## List of Figures

Figure 1-1: High-Level Architecture of Enhanced Media Gateway .....	7
Figure 3-1: Login Screen .....	12
Figure 3-2: IP Settings Screen (Single Network Interface) .....	12
Figure 3-3: IP Settings Screen (Multiple Network Interface) .....	13
Figure 3-4: Maintenance Actions: Reset Gateway .....	13
Figure 4-1: Summary of Steps for Configuring Enhanced Gateway for PSTN-Only .....	16
Figure 4-2: Proxy & Registration Page .....	17
Figure 4-3: Proxy Sets Table Page .....	18
Figure 4-4: Reasons for Alternative Routing Page .....	19
Figure 4-5: SIP General Parameters Page .....	19
Figure 4-6: Advanced Parameters Page .....	20
Figure 4-7: SIP General Parameters Page .....	21
Figure 4-8: Application Settings Page .....	22
Figure 4-9: DNS Server Settings .....	23
Figure 4-10: Certificates Page .....	24
Figure 4-11: Microsoft Certificate Services Web Page .....	25
Figure 4-12: Request a Certificate Page .....	26
Figure 4-13: Advanced Certificate Request Page .....	26
Figure 4-14: Submit a Certificate Request or Renewal Request Page .....	27
Figure 4-15: Certificate Issued Page .....	27
Figure 4-16: Download a CA Certificate, Certificate Chain, or CRL Page .....	28
Figure 4-17: Certificates Page (Uploading Certificate) .....	29
Figure 4-18: SIP General Parameters Page .....	30
Figure 4-19: Media Security Page .....	32
Figure 4-20: Coders Table Page .....	33
Figure 4-21: RTP/RTCP Settings Page .....	34
Figure 4-22: IPMedia Settings Page .....	35
Figure 4-23: SIP General Parameters Page (1) .....	36
Figure 4-24: SIP General Parameters Page (2) .....	37
Figure 4-25: Advanced Parameters Page .....	38
Figure 4-26: Trunk Group Table Page .....	39
Figure 4-27: Trunk Group Settings Page .....	40
Figure 4-28: Inbound IP Routing Table Page .....	41
Figure 4-29: Trunk Settings Page .....	42
Figure 4-30: TDM Bus Settings Page .....	44
Figure 4-31: Number Manipulation Table - Add Dialog Box .....	45
Figure 4-32: Destination Phone Number Manipulation Table for IP→Tel Calls .....	50
Figure 4-33: Destination Phone Number Manipulation Table for Tel→IP Calls .....	51
Figure 4-34: AdminPage .....	52
Figure A-1: Starting the Lync Server Topology Builder .....	53
Figure A-2: Topology Builder Options .....	54
Figure A-3: Save Topology .....	54
Figure A-4: Downloaded Topology .....	55
Figure A-5: Choosing New IP/PSTN Gateway .....	55
Figure A-6: Define New IP/PSTN Gateway .....	56
Figure A-7: Define the IP Address .....	56
Figure A-8: Define the Root Trunk .....	57
Figure A-9: Gateway Added as an IP/PSTN Gateway and Trunk created .....	58
Figure A-10: Choosing Publish Topology .....	58
Figure A-11: Publish Topology Screen .....	59
Figure A-12: Publish Topology Progress Screen .....	59
Figure A-13: Publish Topology Successfully Completed .....	60

## Notice

This document describes the installation and configuration of AudioCodes Mediant Gateway family as Enhanced Gateway deployed in the Microsoft Lync Server 2013 environment.

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 the 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: February-03-2014

## Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI<sup>2</sup>, 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](http://www.audiocodes.com/support).

## Abbreviations and Terminology

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

## Documentation Feedback

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

## Related Documentation

Manual Name
Mediant 500 MSBR Hardware Installation Manual
Mediant 500 MSBR SIP User's Manual
Mediant 800 Gateway and E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 2000 User's Manual
Mediant 3000 User's Manual
Mediant 800 Gateway and E-SBC Hardware Installation Manual
Mediant 1000B Gateway and E-SBC Hardware Installation Manual
Mediant 2000 SIP Hardware Installation Manual
Mediant 3000 SIP Installation Manual

# 1 Introduction

This document describes the installation and configuration of Enhanced Gateway (hereafter referred to as *gateway*), deployed in the Microsoft Lync Server 2013 environment.

The Enhanced Gateway is typically co-located with Microsoft Mediation server at the enterprise's headquarters. The Mediation server is the Lync Server entity that is responsible for interfacing the Lync Server network with the gateway, which provides legacy connections to the public switched telephone network (PSTN) or private branch exchange (PBX).



**Note:** AudioCodes' SBA located at the remote branch office, can also provide Enhanced gateway functionality. For information on how to configure the SBA, refer to the relevant *SBA Installation Manual*.

AudioCodes gateways can also provide the Lync Server environment with a connection to analog devices (such as fax machines and telephones) with AudioCodes MediaPack™ 1xx series as an Analog Telephone Adapter (ATA).



**Note:** This document doesn't describe how to configure the gateway for communication with Analog Devices. For information on how to configure the Gateway with Analog Devices, refer to the *Enhanced Gateway and Analog Devices Configuration Note*.

Figure 1-1: High-Level Architecture of Enhanced Media Gateway



## Reader's Notes



## 2 Component Information

### 2.1 AudioCodes Gateway Version

**AudioCodes Gateway Version**

<b>GW Vendor</b>	AudioCodes
<b>Models</b>	<ul style="list-style-type: none"><li>▪ Mediant 500 MSBR</li><li>▪ Mediant 800 Gateway &amp; E-SBC</li><li>▪ Mediant 1000B Gateway &amp; E-SBC</li><li>▪ Mediant 2000 Gateway</li><li>▪ Mediant 3000 Gateway &amp; E-SBC</li></ul>
<b>Software Version</b>	SIP_6.60A or later
<b>Protocol</b>	<ul style="list-style-type: none"><li>▪ PRI /BRI (to PSTN)</li><li>▪ SIP/TCP or TLS (to Lync Server)</li></ul>
<b>Additional Notes</b>	None

### 2.2 Microsoft Lync Server 2013 Version

**Microsoft Lync Server 2013 Version**

<b>Vendor</b>	Microsoft
<b>Model</b>	Microsoft Lync
<b>Software Version</b>	Release 2013 5.0.8308.0
<b>Protocol</b>	SIP
<b>Additional Notes</b>	None

## Reader's Notes

## 3 Assigning IP Address to PSTN Gateway

The gateway includes an embedded Web server (*Web interface*), providing a user-friendly graphical user interface (GUI) for configuration. The IP address used for accessing this Web interface must be changed to suit the networking scheme in which your Enhanced Gateway is deployed.

Before you can configure the PSTN gateway, you need to first access it with the default VoIP / Management LAN IP address, as described below.

### 3.1 Initial Access to the PSTN Gateway

Before you can configure the PSTN gateway, you need to access its Web interface using the default VoIP / Management LAN IP address as shown in the table below.

**PSTN Gateway Default IP Addresses**

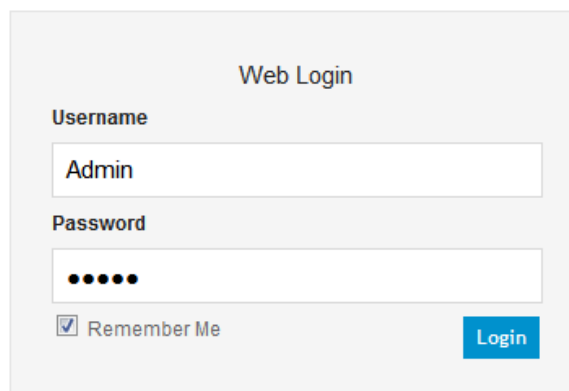
Device Name	IP Address	Subnet Mask
Mediant 3000	<ul style="list-style-type: none"><li>TP-6310 or TP-8410 blade in Slot 1: 10.1.10.10</li><li>TP-6310 or TP-8410 blade in Slot 3: 10.1.10.11 (HA mode)</li></ul>	255.255.0.0
Mediant 2000	<ul style="list-style-type: none"><li>Device with single module (trunks 1-8): 10.1.10.10</li><li>Device's second module (trunks 9-16): 10.1.10.11</li></ul>	255.255.0.0
Mediant 1000B	192.168.0.2	255.255.255.0
Mediant 800	192.168.0.2	255.255.255.0
Mediant 500	192.168.0.2	255.255.255.0

➤ **To initially access the PSTN gateway:**

1. Connect to the **first** LAN port on the device directly to a PC, using a straight-through Ethernet cable.
2. Ensure that your PC is configured with an IP address in the same subnet as the gateway.
3. Open a standard Web browser, and then in the URL address field, enter the default VoIP / Management LAN IP address (e.g., "10.1.10.10").

The following login screen appears, prompting you to log in with your login credentials:

**Figure 3-1: Login Screen**



Web Login

Username

Admin

Password

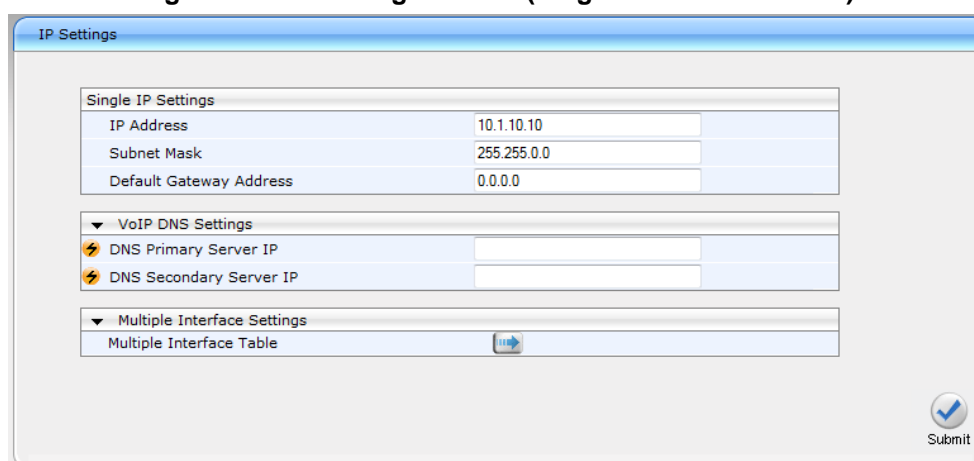
•••••

☒ Remember Me

Login

4. Log in with the default, case-sensitive user name ("Admin") and password ("Admin"), and then click **OK**; the Web interface appears, displaying the Home page.
5. Do one of the following:
  - a. For the Mediant 500, Mediant 800, and Mediant 1000B devices:
    - ◆ Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**) and proceed to Section 3.1.1.
  - b. For the Mediant 2000 and Mediant 3000 devices:
    - ◆ Open the IP Settings page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table** ), as shown below:

**Figure 3-2: IP Settings Screen (Single Network Interface)**



IP Settings


Single IP Settings

IP Address	10.1.10.10
Subnet Mask	255.255.0.0
Default Gateway Address	0.0.0.0

VoIP DNS Settings

DNS Primary Server IP	
DNS Secondary Server IP	

Multiple Interface Settings

Multiple Interface Table	
--------------------------	---

Submit

- ◆ Click the **Multiple Interface Table**  button, located under the Multiple Interface Settings group; a confirmation message box appears.
- ◆ Click **OK**; the Multiple Interface Table page appears; proceed to Section 3.1.1.

### 3.1.1 Assigning IP Address to the Device

This section describes how to assign an IP address to the device.

➤ **To assign an IP address to the device:**

1. Select the **Index** radio button corresponding to the Application Type **OAMP + Media + Control** (i.e., the VoIP and Management LAN interface), and then click **Edit**.

**Figure 3-3: IP Settings Screen (Multiple Network Interface)**

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS S IP Address
0	OAMP + Media + Control	IPv4 Manual	192.168.0.2	24	192.168.0.1	1	Voice		

2. Configure a LAN network address so that it corresponds to your network IP addressing scheme.
3. Click **Apply**, and then click **Done** to apply and validate your settings.
4. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the Maintenance Actions page, click the **Reset** button; the gateway resets and your settings are saved to the flash memory.

**Figure 3-4: Maintenance Actions: Reset Gateway**

5. Maintain the cabled connection between the gateway's LAN port and the computer.

## Reader's Notes

## 4 Configuring the Enhanced Gateway

This section provides step-by-step procedures for configuring the Enhanced Gateway for scenarios where it is used **only** for connecting the Microsoft Lync environment to the PSTN network.

The configuration steps described in this section are performed through the embedded Web server (*Web interface*) of the Enhanced Gateway.



### Notes:

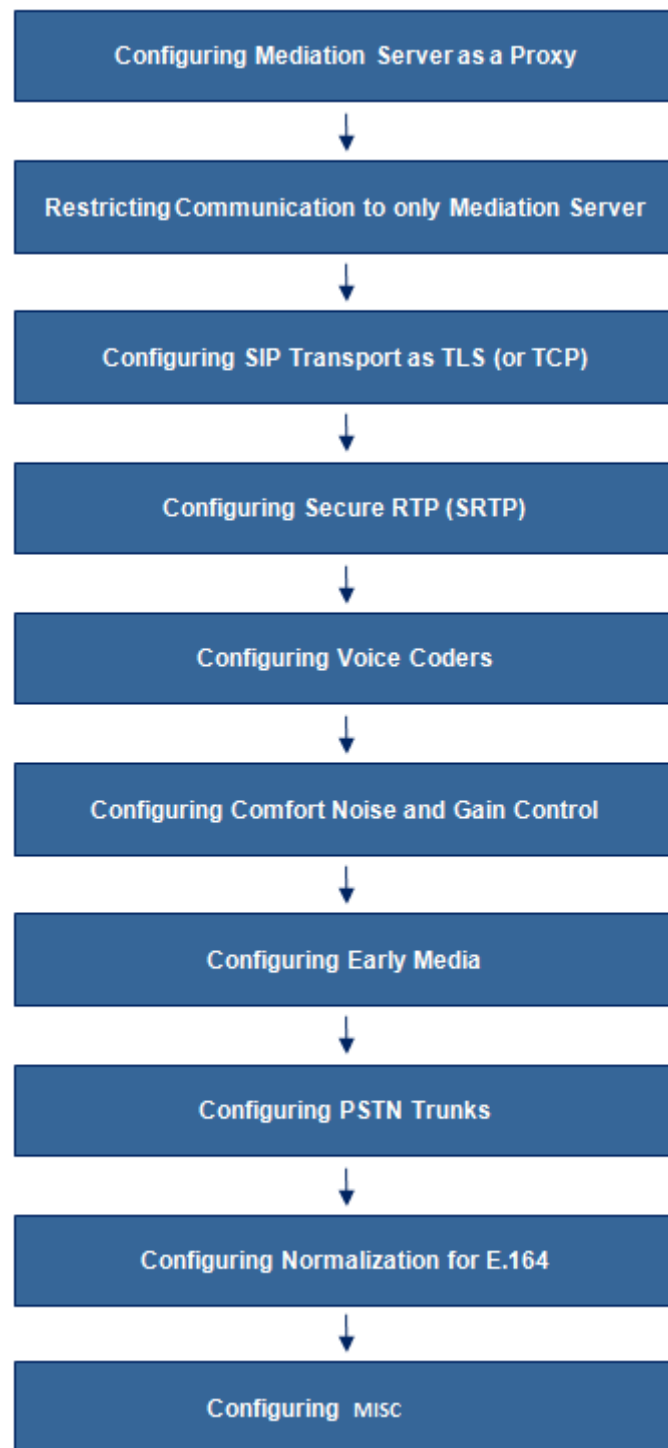
- The gateway must be installed with a Software License that includes the following items:
  - ♦ Microsoft
  - ♦ Security
  - ♦ RTP
  - ♦ SIP

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

- The Gateway must be installed with SIP firmware version 6.6 or later.
- This configuration of the Enhanced Gateway is relevant for both Microsoft Lync 2013 and Microsoft Lync 2010.

The steps for configuring the Enhanced Gateway are summarized in the flowchart below:

**Figure 4-1: Summary of Steps for Configuring Enhanced Gateway for PSTN-Only**





## 4.1 Step 1: Configuring the Mediation Server as a Proxy

The procedure below describes how to configure the address (IP address or FQDN) of the Mediation server through which the Enhanced Gateway communicates with Microsoft Lync. The Enhanced Gateway forwards all telephone calls (PBX/PSTN) to the Mediation server using this configured address. This address is configured in the Enhanced Gateway as a proxy server. In other words, the Mediation server acts as a proxy server (without registration) for the Enhanced Gateway.

➤ **To configure the Mediation server as a proxy server:**

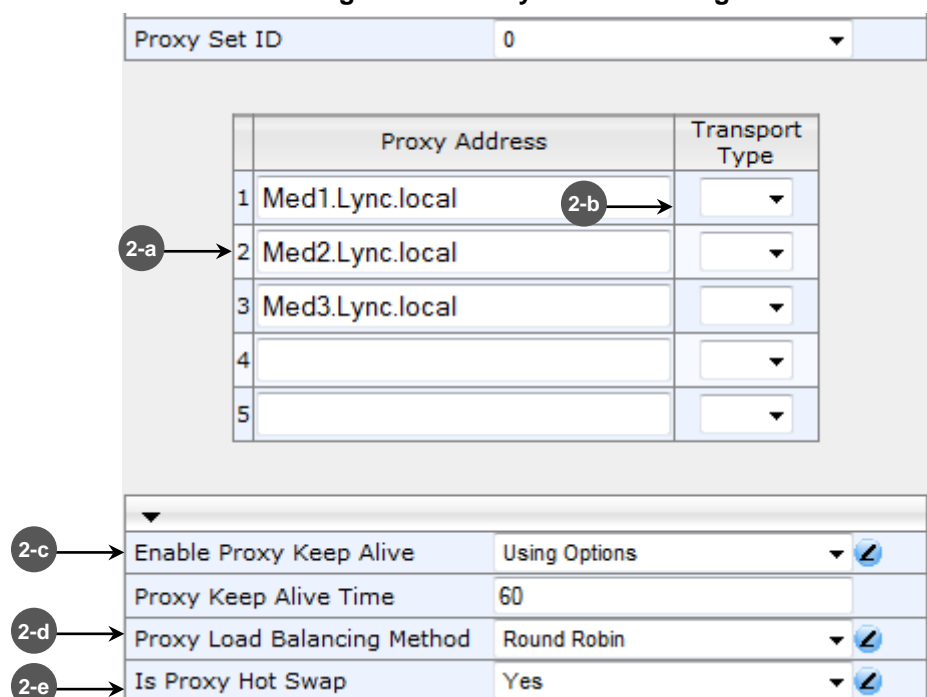
1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).

**Figure 4-2: Proxy & Registration Page**

- a. From the 'Use Default Proxy' drop-down list, select **Yes** to enable the Mediation server to serve as a proxy server.
- b. From the 'Redundant Routing Mode' drop-down list, select **Proxy**.  
This setting ensures that if a SIP 5xx message is received in response to an INVITE message sent to the primary proxy (i.e., Mediation server), the Enhanced Gateway re-sends it to the redundant proxy (i.e., next Mediation server). To configure alternative routing upon receipt of a SIP 503 response (as required by Microsoft Lync), see Step 3.
- c. Click **Submit**.
- d. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

2. Click the **Proxy Set Table** button to open the Proxy Sets Table page:

**Figure 4-3: Proxy Sets Table Page**



	Proxy Address	Transport Type
1	Med1.Lync.local	2-b →
2	Med2.Lync.local	2-a →
3	Med3.Lync.local	
4		
5		

2-c →	Enable Proxy Keep Alive	Using Options	
	Proxy Keep Alive Time	60	
2-d →	Proxy Load Balancing Method	Round Robin	
2-e →	Is Proxy Hot Swap	Yes	

- a. In the 'Proxy Address' fields, configure all Mediation server IP addresses or FQDN's with which the Enhanced Gateway is required to work.



**Note:** If you configured the Mediation server address as an FQDN, ensure that you configure the DNS server (see Section 4.3.2 on page 23).

- b. In the 'Transport Type' drop-down list, select the transport type (**TLS** or **TCP**) for these proxies. For more information on the TLS and TCP transport type configuration, see Section 4.3 on page 21.
- c. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options** to discover whether a particular Mediation server in the cluster is available.
- d. From the 'Proxy Load Balancing Method' drop-down list, select **Round Robin** to enable the round robin proxy load-balancing mechanism.
- e. From the 'Is Proxy Hot Swap' drop-down list, select **Yes**.  
If there is no response from the first Mediation server after a user-defined number of retransmissions, the INVITE message is sent to the redundant Mediation server.
- f. Click **Submit** to apply your settings.

3. When the Enhanced Gateway receives a SIP 503 response from the Mediation server in response to an INVITE, it re-sends the INVITE to the redundant Mediation server (located at the datacenter). To achieve this, you need to configure the receipt of a SIP 503 response as a reason for IP alternative routing:
  - a. Open the Reasons for Alternative Routing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Alternative Routing Reasons**).

Figure 4-4: Reasons for Alternative Routing Page

IP to Tel Reasons	
Reason 1	
Reason 2	
Reason 3	
Reason 4	
Reason 5	

Tel to IP Reasons	
Reason 1	503
Reason 2	
Reason 3	
Reason 4	
Reason 5	

Submit

- b. Under the **Tel to IP Reasons** group, from the 'Reason 1' drop-down list, select **503**.
- c. Click **Submit**.
- d. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 4-5: SIP General Parameters Page

Enable Voicemail URI	Disable
Retry-After Time	0
Enable P-Associated-URI Header	Disable
Source Number Preference	
Forking Handling Mode	Parallel handling
Enable Comfort Tone	Disable
Add Trunk Group ID as Prefix to Source	No
Fake Retry After	60
Enable Reason Header	Enable

Basic Parameter List  
Submit

- e. In 'Fake Retry After' field, enter the time **60** (in seconds). When the Enhanced Gateway receives a SIP 503 response (from the Mediation server) without a Retry-After header, the Enhanced Gateway behaves as if the 503 response includes a Retry-After header with this user-defined period.
- f. Click **Submit**.
- g. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

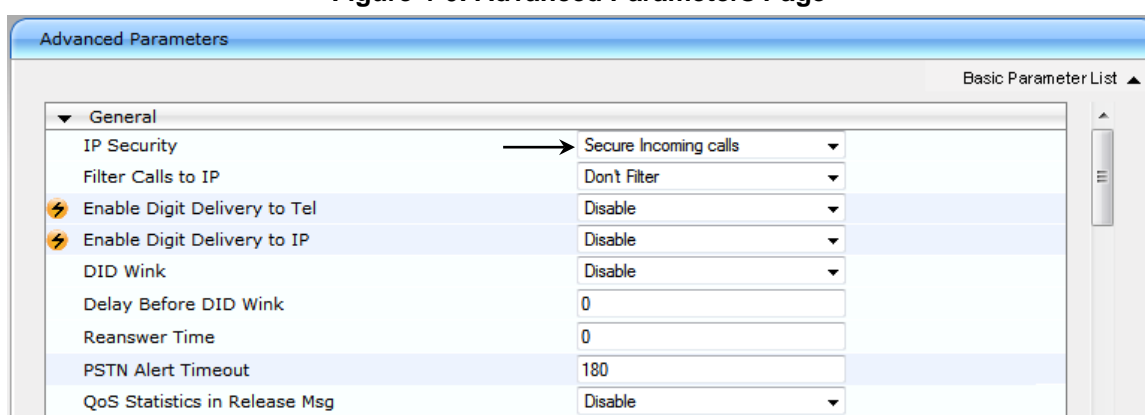
## 4.2 Step 2: Restricting Communication to Mediation Server Only

The procedure below describes how to restrict IP communication, by allowing communication only between the Enhanced Gateway and the Mediation server. This ensures that the Enhanced Gateway accepts and sends SIP calls **only** to and from the Mediation server (as required by Microsoft). This is done by enabling the IP Security feature and then defining the allowed ("administrative" list) IP addresses (or FQDNs) in the Proxy Set table.

➤ **To allow IP communication only between the Enhanced Gateway and Mediation server:**

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

Figure 4-6: Advanced Parameters Page



Advanced Parameters	
Basic Parameter List ▲	
▼ General	
IP Security	Secure Incoming calls
Filter Calls to IP	Don't Filter
⚡ Enable Digit Delivery to Tel	Disable
⚡ Enable Digit Delivery to IP	Disable
DID Wink	Disable
Delay Before DID Wink	0
Reanswer Time	0
PSTN Alert Timeout	180
QoS Statistics in Release Msg	Disable

2. From the 'IP Security' drop-down list, select **Secure Incoming calls** to enable the security feature to accept and send SIP calls only from and to user-defined IP addresses or FQDN (i.e., Mediation server) configured in the Proxy Set table (see Step 4.1 on page 17).
3. Click **Submit** to apply your settings.
4. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

## 4.3 Step 3: Configuring TLS

Transport Layer Security (TLS) is the recommended transport type (enabled by default on Lync environment) for communication between the Enhanced Gateway and the Mediation server. However, if you require TCP instead, then skip this section and proceed to Step 4 (Section 4.4 on page 30).

TLS provides encrypted SIP signaling between the Enhanced Gateway and the Mediation server. When using TLS, you also need to configure the Enhanced Gateway with a certificate for authentication during the TLS handshake with the Mediation server.

### 4.3.1 Enabling TLS and Defining TLS Port

The procedure below describes how to enable TLS and configure the Enhanced Gateway ports used for TLS.

➤ **To enable TLS and configure TLS ports:**

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

**Figure 4-7: SIP General Parameters Page**

SIP General Parameters	
Detect Fax on Answer Tone	Initiate T.38 on Preamble
2 → SIP Transport Type	TLS
SIP UDP Local Port	5060
SIP TCP Local Port	5060
3 → SIP TLS Local Port	5067
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
4 → SIP Destination Port	5067
Use user=phone in SIP URL	Yes
Use user=phone in From Header	No

Submit

2. From the 'SIP Transport Type' drop-down list, select **TLS**.
3. In the 'SIP TLS Local Port', enter **5067**. This port corresponds to the Mediation server TLS transmitting port configuration.
4. In the 'SIP Destination Port', enter **5067**. This port corresponds to the Mediation server TLS listening port configuration.
5. Click **Submit** to apply your settings.
6. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

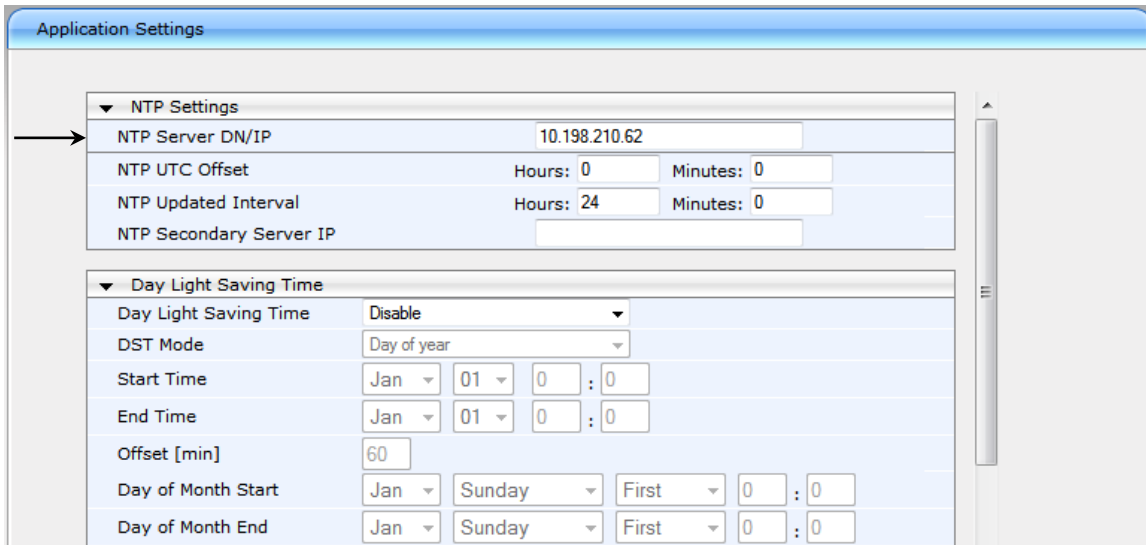
### 4.3.2 Configuring the NTP Server

The procedure below describes how to configure the Network Time Protocol (NTP) server. This is important for maintaining the correct time and date on the Enhanced Gateway, by synchronizing it with a third-party NTP server. This ensures that the Enhanced Gateway has the same date and time as the Certification Authority (CA), discussed later in Section 4.3.4 on page 21.

➤ **To configure the NTP server:**

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

**Figure 4-8: Application Settings Page**



The screenshot shows the 'Application Settings' window. On the left, a tree view has 'NTP Settings' selected, indicated by a black arrow. The main area contains two sections: 'NTP Settings' and 'Day Light Saving Time'.

**NTP Settings:**

- NTP Server DN/IP: 10.198.210.62
- NTP UTC Offset: Hours: 0, Minutes: 0
- NTP Updated Interval: Hours: 24, Minutes: 0
- NTP Secondary Server IP: (empty field)

**Day Light Saving Time:**

- Day Light Saving Time: Disable (dropdown)
- DST Mode: Day of year (dropdown)
- Start Time: Jan, 01, 0 : 0
- End Time: Jan, 01, 0 : 0
- Offset [min]: 60
- Day of Month Start: Jan, Sunday, First, 0 : 0
- Day of Month End: Jan, Sunday, First, 0 : 0

2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

### 4.3.3 Configuring the DNS Server

The procedure below describes how to configure the IP address of the Domain Name System (DNS) servers. This is required if the Mediation server is configured with an FQDN, in which case, the DNS is used to resolve it into an IP address.

➤ **To configure the DNS servers:**

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

**Figure 4-9: DNS Server Settings**

The screenshot shows a web-based configuration interface titled "IP Interfaces Table". It features a toolbar with "Add Index", "Delete", and "Apply" buttons. Below the toolbar is a table with the following data:

IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS IP Address
10.8.6.86	16	10.8.0.1	1	Voice	10.8.7.80	10.8.8.70

Below the table, there is a section for "WAN Interface Name" with a dropdown menu currently set to "Not Configured".

2. In the 'DNS Primary Server IP' and 'DNS Secondary Server IP' fields, enter the IP address of the primary and secondary DNS server, respectively.
3. Click **Submit** to apply your changes and then click **Done**.
4. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.
5. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the 'Maintenance Actions' page, click the **Reset** button; the Enhanced Gateway resets and your settings are saved to the flash memory.

### 4.3.4 Configuring a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). It is composed of the following steps:

1. Generating a certificate signing request (CSR)
2. Obtaining CA and Trusted Root certificates from Microsoft
3. Installing Microsoft CA and Trusted Root certificates on the Enhanced Gateway

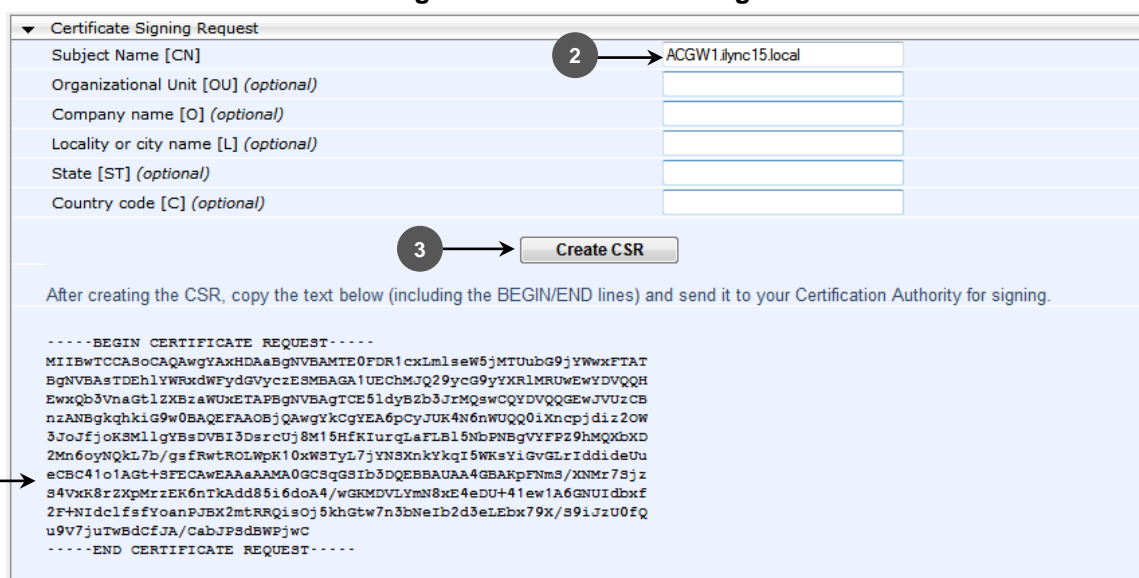
### 4.3.4.1 Generating a Certificate Signing Request

The procedure below describes how to generate a CSR by the Enhanced Gateway. This CSR is later sent to the Microsoft CA.

➤ **To generate a CSR:**

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

**Figure 4-10: Certificates Page**



The screenshot shows the 'Certificate Signing Request' form. Callout 2 points to the 'Subject Name [CN]' field, which contains 'ACGW1.ilync15.local'. Callout 3 points to the 'Create CSR' button. Callout 4 points to the 'BEGIN CERTIFICATE REQUEST' text block.

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-----
MIIBwTCCAsCAQAwgYwHDAaBgNVBAMTE0FDR1cxLmlsew5jMTUubG9jYVwwFTAT
BgNVBAsTDEhlYWVWYXNjaWVycyESMBAGA1UEChMJQ29ycG9yYXR1MRUwEwYDVQ
EhEwQ3VnaGt1ZXBzaWUxETAPBgNVBAGTCE5ldyB2b3JrMQswCQYDVQQGEwJVUzCB
n2ANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA6pCyJUK4N6nWUQ0iXncpjdiz2OW
3JoJfjoRSM1lgYBsDVBI3DsUj8M15HfKIurqlaFLB15NbPnBgVYFP29hMQXbXD
2Mn6oyNQKL7b/gsfRwtrROLWpK10xWSTyL7jYN3XnkYkqI5WksYiGvGLrIddideUu
eCBC41o1AGt+sFECAWEAAAMA0GCSqGSIb3DQEBAUAA4GBAKpFNmS/XNMr7Sjz
S4VxK8r2XpMrzEK6nTkAdd85i6doA4/wGKMDVLYmN8xE4eDU+41ew1A6GNUIdbxf
2F+NidclfsfVoanPJBX2mtRRQisOj5khGtw7n3bNeib2d3eLEbx79X/s9iJzU0fq
u9v7juTwBdcfJA/CabJpsdBWPjwc
-----END CERTIFICATE REQUEST-----

```

2. In the Subject Name field, enter the media gateway name (e.g., "ACGW1.ilync15.local"). This name must be equivalent to the gateway name configured in the Topology Builder for Lync Server 2013.
3. Click **Create CSR**; a Certificate request is generated and displayed on the page.
4. Copy the certificate 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 PC with the file name *certreq.txt*.



#### 4.3.4.2 Obtaining the Microsoft CA and Trusted Root Certificates

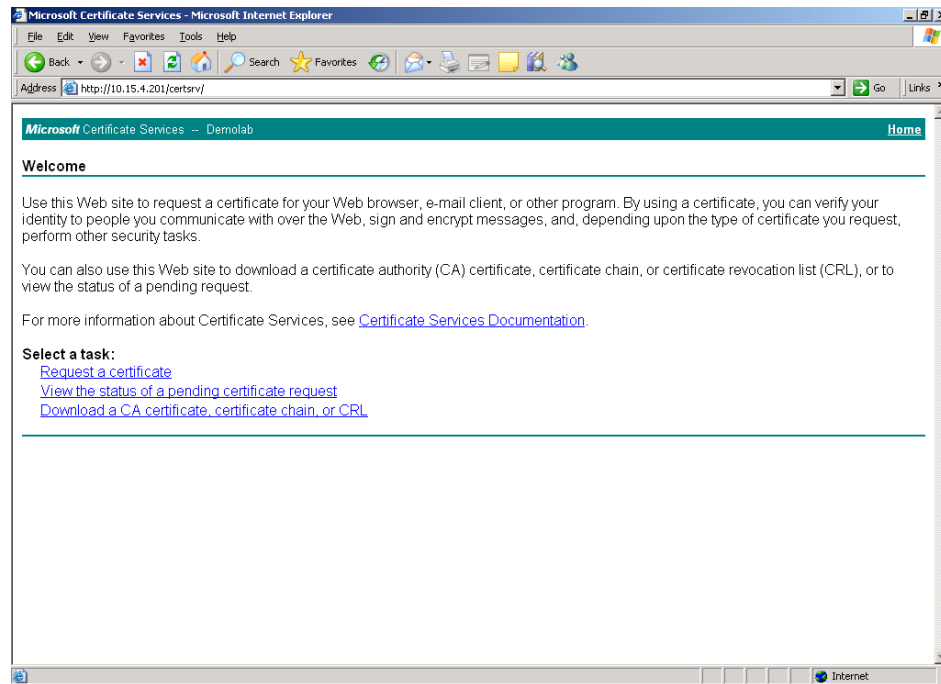
Once you have generated a CSR (described in the previous section), you need to upload it to Microsoft Certificate server and request a CA and trusted root certificates.

➤ **To obtain Microsoft CA and trusted root certificates:**

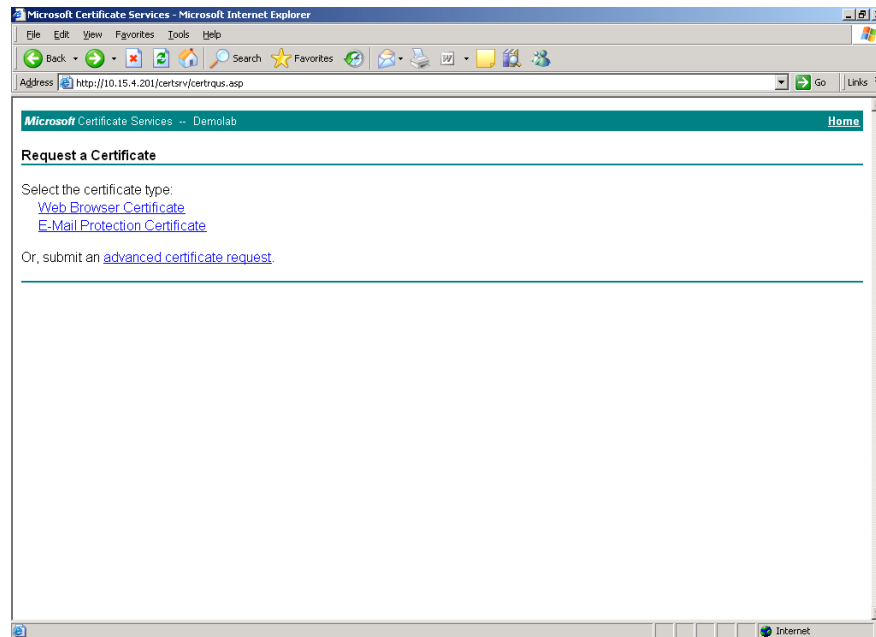
1. Open a Web browser and then navigate to Microsoft Certificate Services at the following link:

http://< certificate server address >/certsrv

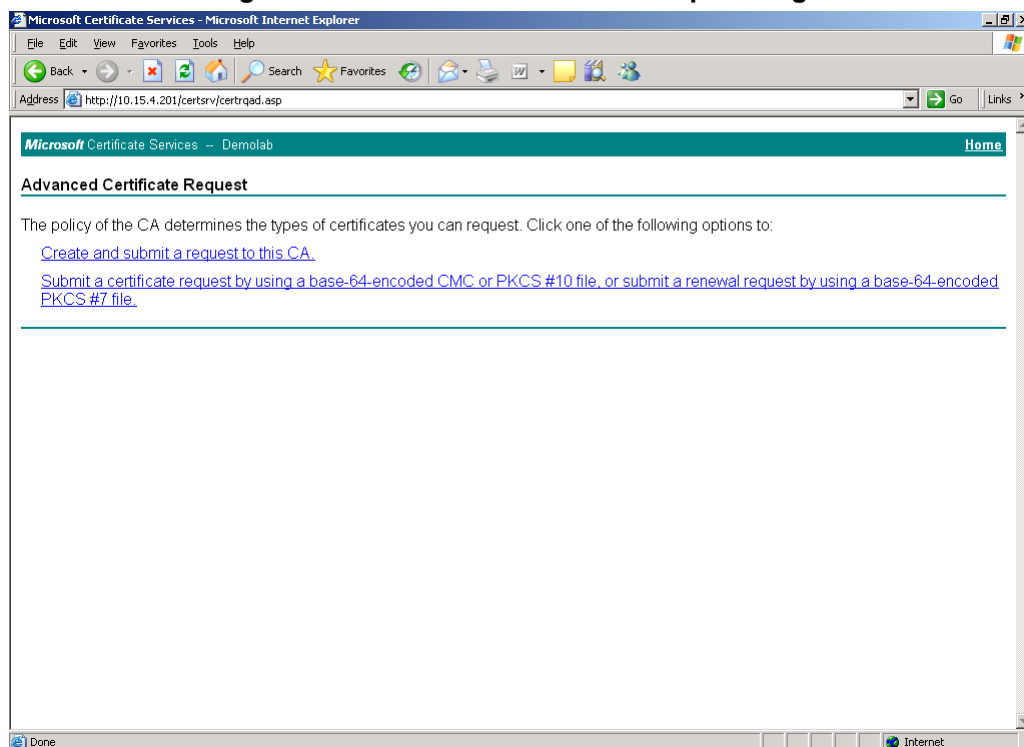
**Figure 4-11: Microsoft Certificate Services Web Page**



2. Click the **Request a certificate** link; the Request a Certificate page appears:

**Figure 4-12: Request a Certificate Page**


3. Click the **advanced certificate request** link; the Advanced Certificate Request page appears:

**Figure 4-13: Advanced Certificate Request Page**


- Click the **Submit a Certificate request by using base-64-encoded...** link; the Submit a Certificate Request or Renewal Request page appears:

**Figure 4-14: Submit a Certificate Request or Renewal Request Page**

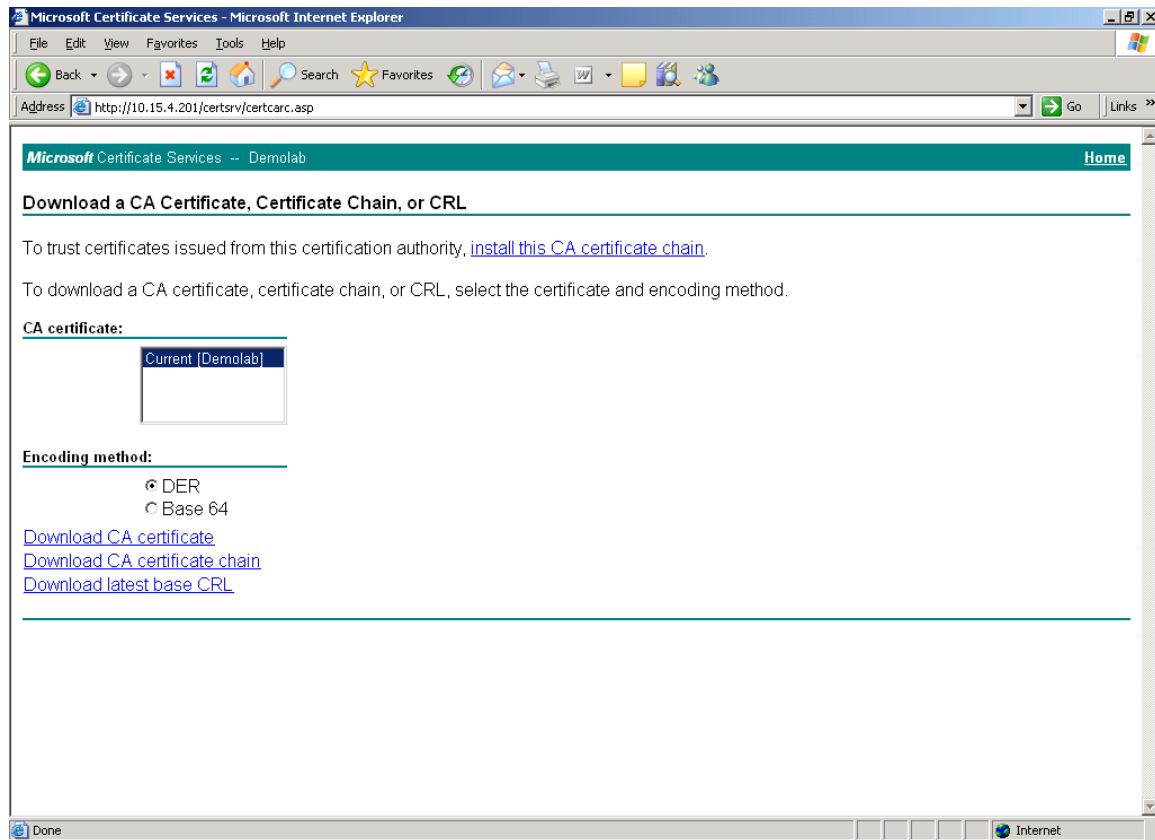
- Open the CSR file (*certreq.txt*) that you created and saved in Section 4.3.4.1 on page 24, and then copy its contents to the **Saved Request** text box.
- From the **Certificate Template** drop-down list, select **Web Server**.
- Click **Submit**; the Certificate Issued Page is displayed:

**Figure 4-15: Certificate Issued Page**

- Select the **Base 64 encoded** option.
- Click the **Download CA certificate** link, and then save the file with the name, *gateway.cer* in a folder on your PC.
- Navigate once again to the certificate server at **http://< certificate server address >/certsrv**.

11. Click the **Download a CA certificate, certificate chain or CRL** link; the Download a CA Certificate, Certificate Chain, or CRL page appears:

**Figure 4-16: Download a CA Certificate, Certificate Chain, or CRL Page**



12. Under the **Encoding method** group, select the **Base 64** option.
13. Click the **Download CA certificate** link, and then save the file with the name *certroot.cer* in a folder on your PC.

### 4.3.4.3 Loading Microsoft CA and Trusted Root Certificates to Enhanced Gateway

Once you have obtained the CA and trusted root certificates from Microsoft, you need to load these two certificates to the Enhanced Gateway.

➤ **To load certificates to the Enhanced Gateway:**

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

**Figure 4-17: Certificates Page (Uploading Certificate)**

▼ Upload certificate files from your computer

Private key pass-phrase (optional)

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

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

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

3 → Send **"Trusted Root Certificate Store"** file from your computer to the device.  
The file must be in textual PEM format.

2. In the 'Device Certificate' field, click **Browse**, select the *gateway.cer* certificate file that you saved on your local disk (see Step 9 in the previous section), and then click **Send File** to upload the certificate to the Enhanced Gateway.
3. In the 'Trusted Root Certificate Store' field, click **Browse** to select the *certroot.cer* certificate file that you saved on your local disk (see Step 13 in the previous section), and then click **Send File** to upload the certificate.
4. On the toolbar, click **Burn** to save the certificates to the Enhanced Gateway flash memory.
5. On the toolbar, from the **Device Actions** drop-down list, choose **Reset**, and then in the Maintenance Actions page, click the **Reset** button; the Enhanced Gateway resets and your settings are saved to the flash memory.

## 4.4 Step 4: Configuring TCP Transport Type

TCP provides unencrypted SIP signaling between the Enhanced Gateway and Mediation server. The procedure below describes how to configure the SIP TCP transport type.

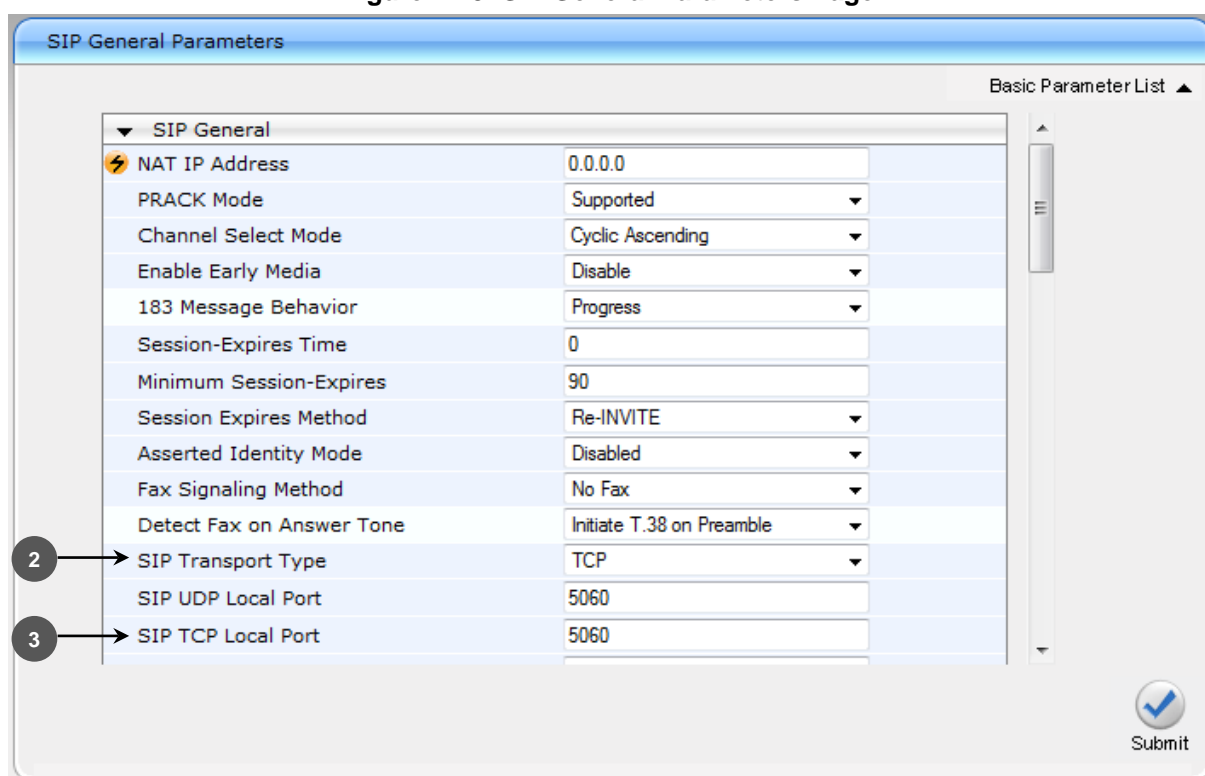


**Note:** Microsoft does not recommend implementing TCP for the SIP transport type between the Enhanced Gateway and the Mediation server.

➤ **To set SIP transport type to TCP:**

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

**Figure 4-18: SIP General Parameters Page**



SIP General Parameters	
Basic Parameter List ▲	
▼ SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported ▼
Channel Select Mode	Cyclic Ascending ▼
Enable Early Media	Disable ▼
183 Message Behavior	Progress ▼
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE ▼
Asserted Identity Mode	Disabled ▼
Fax Signaling Method	No Fax ▼
Detect Fax on Answer Tone	Initiate T.38 on Preamble ▼
2 → SIP Transport Type	TCP ▼
3 → SIP UDP Local Port	5060
SIP TCP Local Port	5060
Submit	

2. From the 'SIP Transport Type' drop-down list, select **TCP**.
3. In the 'SIP TCP Local Port' field, enter the same Gateway TCP listening port number that was configured on the Topology Builder for the gateway.
4. Click **Submit** to apply your changes.
5. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

## 4.5 Step 5: Configuring Secure Real-Time Transport Protocol

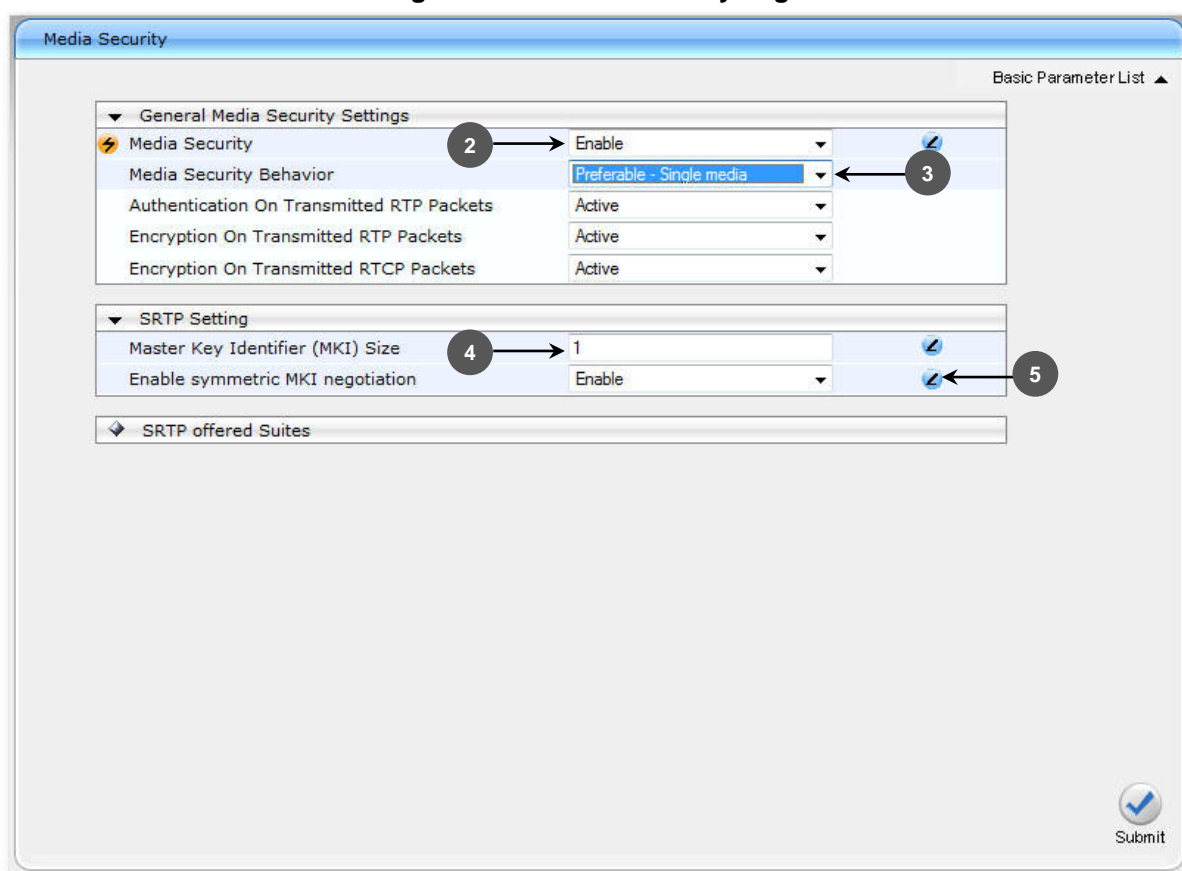
If you configure TLS as the SIP transport type between the Enhanced Gateway and Mediation server, it is recommended to enable Secure RTP (SRTP) encryption and set its mode of operation to one of the following (and that which matches the SRTP supported at the Mediation server):

- **Preferable** (default): The Enhanced Gateway initiates encrypted calls. However, if negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted – **This option is not supported by the Mediation server.**
- **Mandatory**: The Enhanced Gateway initiates encrypted calls, however if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.
- **Preferable - Single Media**: The PSTN Gateway sends SDP with a single media ('m=') line only (e.g., m=audio 6000 RTP/AVP 8 0 101) with RTP/AVP and crypto keys. The remote SIP user agent (UA) can respond with SRTP or RTP parameters:
  - If the Mediation Server does not support SRTP, it uses RTP and ignores the crypto lines.
  - If the PSTN Gateway receives an SDP offer with a single media, it responds with SRTP (RTP/SAVP) if the 'Media Security' parameter is set to **Enable**. If SRTP is not supported (i.e., 'Media Security' is set to **Disabled**), it responds with RTP.

➤ **To configure SRTP:**

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

**Figure 4-19: Media Security Page**



2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
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 the Mediation server is configured to 'SRTP Optional' or 'Disable'.
4. In the 'Master Key Identifier (MKI) Size' field, enter **1**. This configures the size (in bytes) of the MKI in SRTP Tx packets.
5. From the 'Enable Symmetric MKI Negotiation' drop-down list, select **Enable**.
6. Click **Submit** to apply your changes.
7. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.
8. On the toolbar, from the 'Device Actions' drop-down list, choose **Reset**, and then in the Maintenance Actions page, click the **Reset** button; the Enhanced Gateway resets and your settings are saved to the flash memory.



## 4.6 Step 6: Configuring Voice Coders (with Silence Suppression)

The Enhanced Gateway communicates with the Mediation server using either the G.711 A-law or G.711  $\mu$ -law (Mu-Law) voice coder. In addition, silence suppression can be enabled per coder, which is recommended for improving the performance of the Mediation server. The procedure below shows how you can change the default coder.

➤ **To configure the voice coder and silence suppression:**

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

**Figure 4-20: Coders Table Page**

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

Submit

2. From the 'Coder Name' drop-down list, select the required coder.
3. From the 'Silence Suppression' drop-down list, select **Enable**.
4. Click **Submit**.
5. On the toolbar, click **Burn** to save the certificates to the Enhanced Gateway flash memory.

## 4.7 Step 7: Configuring Comfort Noise and Gain Control

The Microsoft Lync network provides high voice quality by implementing suppression of typing noise during calls and improved generation of “comfort noise,” which reduces hissing and smoothes over the discontinuous flow of audio packets. You may need to configure the Enhanced Gateway to match these voice quality features, by enabling silence suppression, comfort noise generation, automatic gain control (AGC), and echo canceller (enabled by default).

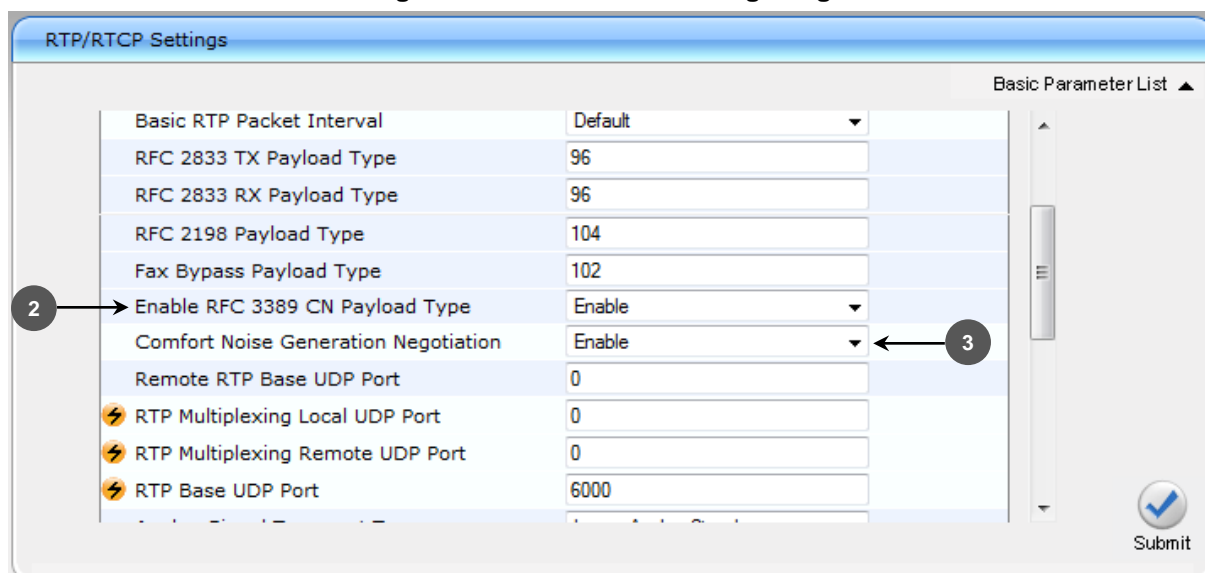


**Note:** Silence suppression is configured per coder type, as described in Step 6 (See Section 4.6 on page 33).

➤ **To configure voice quality:**

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** > **RTP/RTCP Settings**).

**Figure 4-21: RTP/RTCP Settings Page**



RTP/RTCP Settings	
Basic RTP Packet Interval	Default
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
2 → Enable RFC 3389 CN Payload Type	Enable
Comfort Noise Generation Negotiation	3 → Enable
Remote RTP Base UDP Port	0
⚡ RTP Multiplexing Local UDP Port	0
⚡ RTP Multiplexing Remote UDP Port	0
⚡ RTP Base UDP Port	6000

Submit

2. Verify that the 'Enable RFC 3389 CN payload Type' parameter is set to **Enable**.
3. From the 'Comfort Noise Generation Negotiation' drop-down list, select **Enable** to enable comfort noise generation.
4. Click **Submit**.
5. Open the IPMedia Settings page (**Configuration** tab > **VoIP** menu > **Media** > **IPMedia Settings**).

Figure 4-22: IPMedia Settings Page

IPMedia Settings		
IPMedia Detectors	Enable	
Enable Answer Detector	Disable	
Answer Detector Activity Delay	0	
Answer Detector Silence Time	10	
Answer Detector Redirection	0	
Answer Detector Sensitivity	0	
Answer Machine Detector Sensitivity Parameter Suit	0	
Answer Machine Detector Sensitivity	3	
Answer Machine Detector Beep Detection Timeout	200	
Answer Machine Detector Beep Detection Sensitivity	0	
Enable AGC	Enable	
AGC Class	2	

Submit

6. From the 'IPMedia Detectors' drop-down list, select **Enable**. This parameter requires an Enhanced Gateway reset (see below).
7. From the 'Enable AGC' drop-down list, select **Enable**.
8. Click **Submit** to apply your changes.
9. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.
10. On the toolbar, from the 'Device Actions' drop-down list, choose **Reset**, and then in the Maintenance Actions page, click the **Reset** button; the Enhanced Gateway resets and your settings are saved to the flash memory.

## 4.8 Step 8: Configuring Early Media

Early media refers to audio and video that is exchanged before a call is accepted by the recipient. Early media generated by the caller includes voice commands or dual-tone multi frequency (DTMF) tones to activate interactive voice response (IVR) systems. Early media generated by the call recipient include ringback tones, announcements, and requests for input.

Enhanced early media support in Microsoft Lync 2013 enables a caller to hear a ringback tone generated by the call recipient's mobile phone. This is also the case in team-call scenarios, where a call is routed to two team members, one of whom has configured simultaneous ringing for their mobile device.

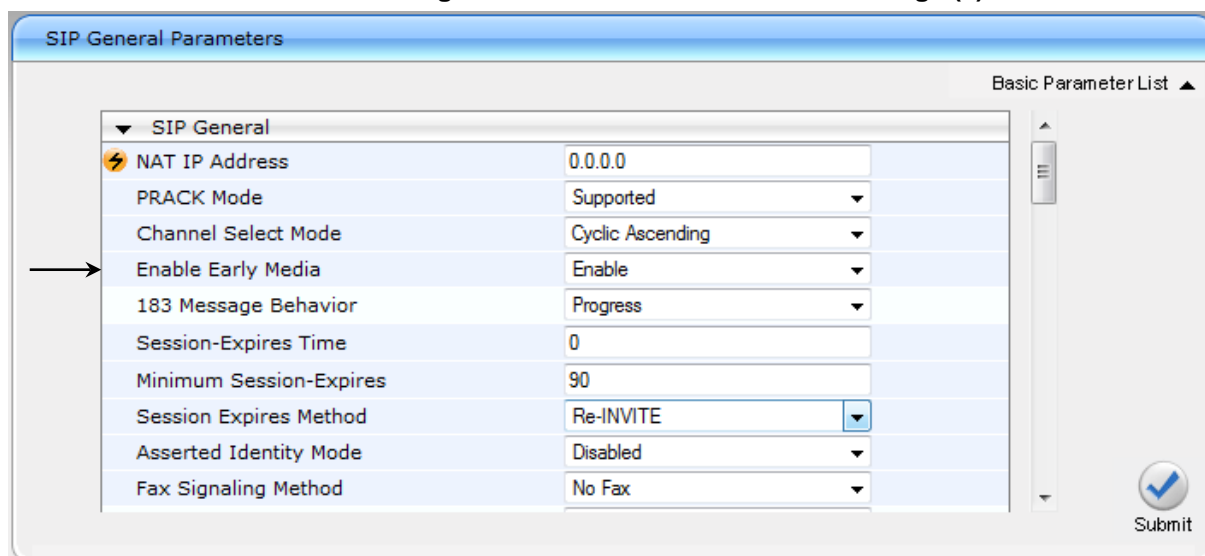
According to Microsoft Lync 2013 requirements, the Enhanced Gateway must send a SIP 183 with SDP response immediately after it receives an INVITE. The RTP packets however, will not be sent until the Enhanced Gateway receives an ISDN Progress, Alerting and Progress Indicator or Connect message. For example, if the Enhanced Gateway receives ISDN Progress, it starts sending RTP packets according to initial negotiation; however there is no need to re-send the 183 response.

You may optionally configure the Enhanced Gateway's early media feature to support the Microsoft Lync 2013 enhanced early media feature.

➤ **To configure the Early Media feature:**

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

**Figure 4-23: SIP General Parameters Page (1)**



SIP General Parameters	
▼ SIP General	
⚡ NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
→ Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax

Basic Parameter List ▲

Submit

2. From the 'Enable Early Media' drop-down list, select **Enable**.

Figure 4-24: SIP General Parameters Page (2)

SIP General Parameters		Basic Parameter List ▲
Play Ringback Tone to IP	Don't Play	
Play Ringback Tone to Tel	Play Local Until Remote Media Arrive	
Use Tgrp information	Disable	
Enable GRUU	Disable	
User-Agent Information		
SDP Session Owner	AudiocodesGW	
Play Busy Tone to Tel	Don't Play	
Subject		
Multiple Packetization Time Format	None	
Enable Semi-Attended Transfer	Disable	
3xx Behavior	Forward	
Enable P-Charging Vector	Disable	
Enable VoiceMail URI	Disable	
Retry-After Time	0	
Enable P-Associated-URI Header	Disable	
Source Number Preference		
Forking Handling Mode	Sequential handling	
Enable Comfort Tone	Disable	

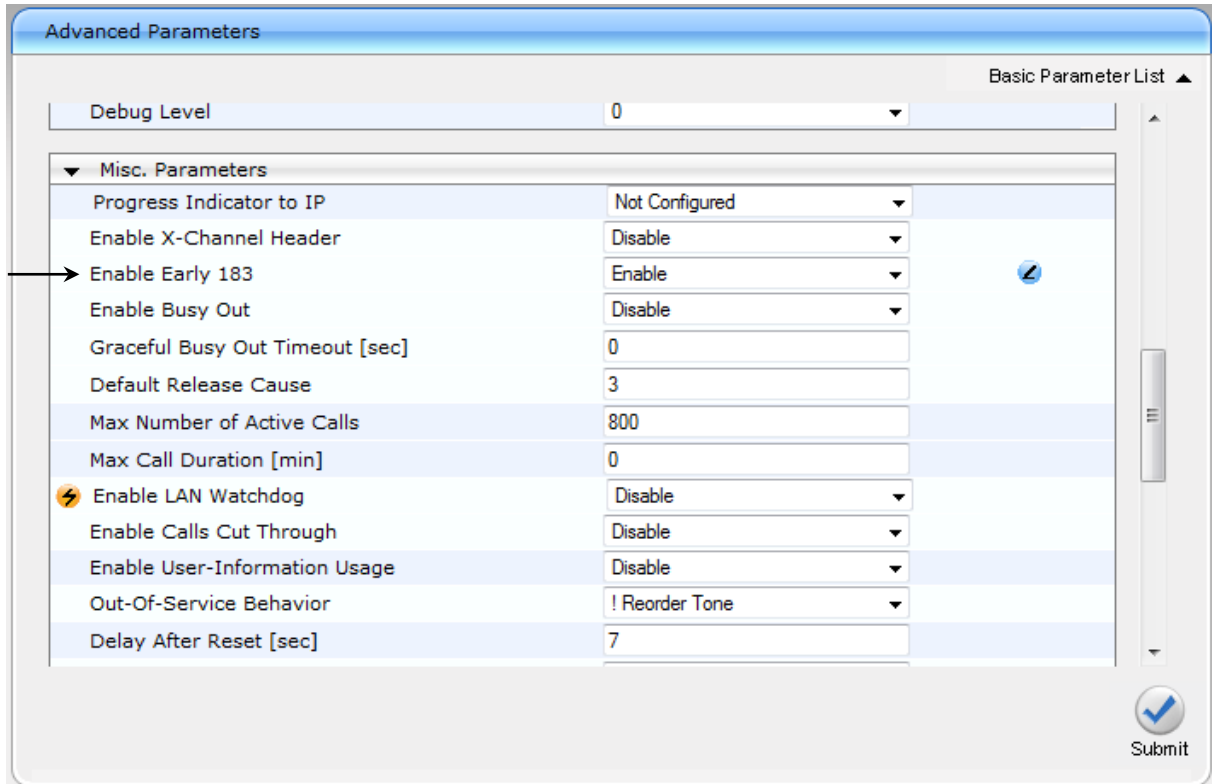
Submit

3. From the 'Play Ringback Tone to Tel' drop-down list, select **Play Local Until Remote Media Arrive**.

If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the Enhanced Gateway plays a local ringback tone if there are no prior received RTP packets. The Enhanced Gateway stops playing the local ringback tone as soon as it starts receiving RTP packets. At this stage, if the Enhanced Gateway receives additional 18x responses, it does not resume playing the local ringback tone.

4. From the 'Forking Handling Mode' drop-down list, select **Sequential handling**. The PSTN Gateway re-opens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if 180 response without SDP is received.
5. Click **Submit** to apply your changes.
6. Open the Advanced Parameters page (**Configuration tab > VoIP menu > SIP Definitions > Advanced Parameters**).

Figure 4-25: Advanced Parameters Page



Advanced Parameters		Basic Parameter List ▲
Debug Level		0
▼ Misc. Parameters		
Progress Indicator to IP	Not Configured	
Enable X-Channel Header	Disable	
→ Enable Early 183	Enable	
Enable Busy Out	Disable	
Graceful Busy Out Timeout [sec]	0	
Default Release Cause	3	
Max Number of Active Calls	800	
Max Call Duration [min]	0	
⚡ Enable LAN Watchdog	Disable	
Enable Calls Cut Through	Disable	
Enable User-Information Usage	Disable	
Out-Of-Service Behavior	! Reorder Tone	
Delay After Reset [sec]	7	
		Submit

- From the 'Enable Early 183' drop-down list, select **Enable**.



**Note:** If the 'B-Channel Negotiation' parameter is set to **Preferred** or **Any**, the 'Enable Early 183' parameter is ignored and a SIP 183 is not sent upon receipt of an INVITE. In such a case, you can set the 'Progress Indicator to IP' (ProgressIndicator2IP) parameter to 1 (PI = 1) for the device to send a SIP 183 upon receipt of an ISDN Call Proceeding message.

- Click **Submit** to apply your changes.
- On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

## 4.9 Step 9: Configuring PSTN Trunks

This section describes how to configure PRI (i.e., E1/T1) or BRI trunks connected to the Enhanced Gateway.

### 4.9.1 Enabling Trunks

To enable trunks, you need to assign them to Trunk Groups, as described below.

➤ **To enable trunks:**

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

**Figure 4-26: Trunk Group Table Page**

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-31	1000	1	
2							

2. In the 'Module' column, select the module number and type (e.g., PRI) on which the trunks are located.
3. In the 'From Trunk' and 'To Trunk' columns, select the physical trunk range.
4. In the 'Channel(s)' column, enter the B-channels (e.g., 1-31) that you want to enable.
5. In the 'Phone Number' column, enter the phone number (e.g., 1000) for the first channel; phone numbers 1001, 1002, 1003, and so on are sequentially assigned to subsequent channels. Note that these numbers are used internally.
6. In the 'Trunk Group ID' column, enter the ID for the Trunk Group.
7. Click **Submit** to apply your changes.
8. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

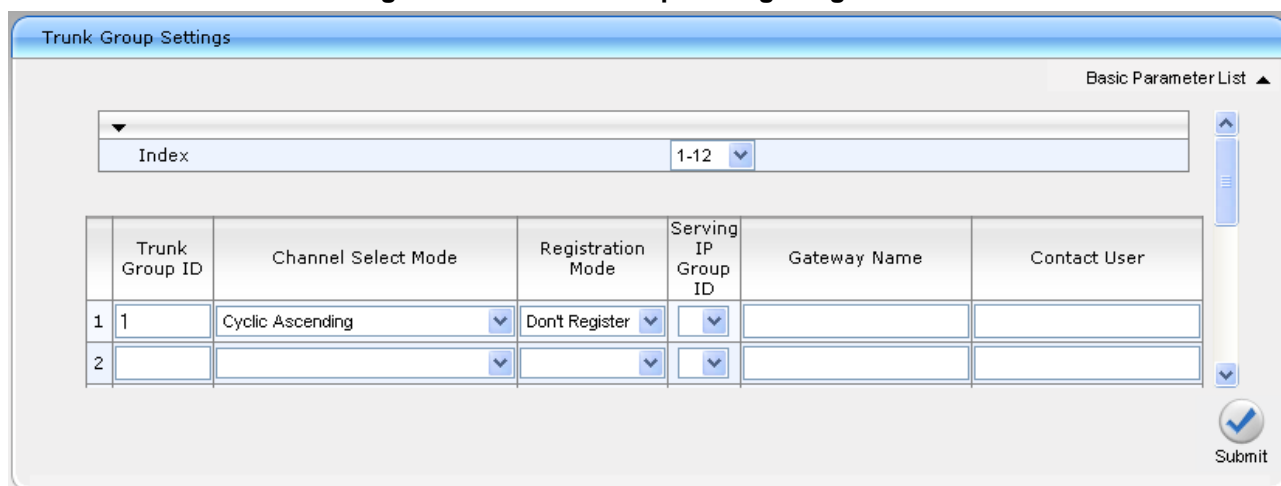
## 4.9.2 Configuring the Channel Select Method

Once you have enabled the trunks and assigned them to Trunk Groups, you need to configure the method for which IP-to-Tel calls are assigned to channels within the Trunk Group.

➤ **To configure the channel select mode:**

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

**Figure 4-27: Trunk Group Settings Page**



Index	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending	Don't Register			
2						

Submit

2. In the 'Trunk Group ID' column, enter the Trunk Group ID that you want to configure.
3. From the 'Channel Select Mode' drop-down list, select the method for which IP-to-Tel calls are assigned to channels pertaining to the Trunk Group (i.e. Cyclic Ascending).
4. From the 'Registration Mode' drop-down list, select **Don't Register**.
5. Click **Submit** to apply your changes.
6. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.



### 4.9.3 Configuring IP-to-Trunk Group Routing

The procedure below describes how to configure an IP-to-Trunk Group routing rule, whereby all calls from the Mediation server to any destination phone number is routed to Trunk Group 1 (that you configured in Section 4.9.1 on page 39).

➤ **To configure an IP-to-Trunk Group routing rule:**

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

**Figure 4-28: Inbound IP Routing Table Page**

	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			*	*	192.168.0.1	1	0	-1
2								
3								
4								

2. In the first table entry row, enter the asterisk (\*) sign in the 'Dest. Phone Prefix' and 'Source Phone Prefix' fields.
3. In the 'Source IP Address' field, enter the IP address of the Mediation server.
4. In the 'Trunk Group ID' field, enter the Trunk Group to where the calls must be routed.
5. Click **Submit** to apply your changes.
6. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

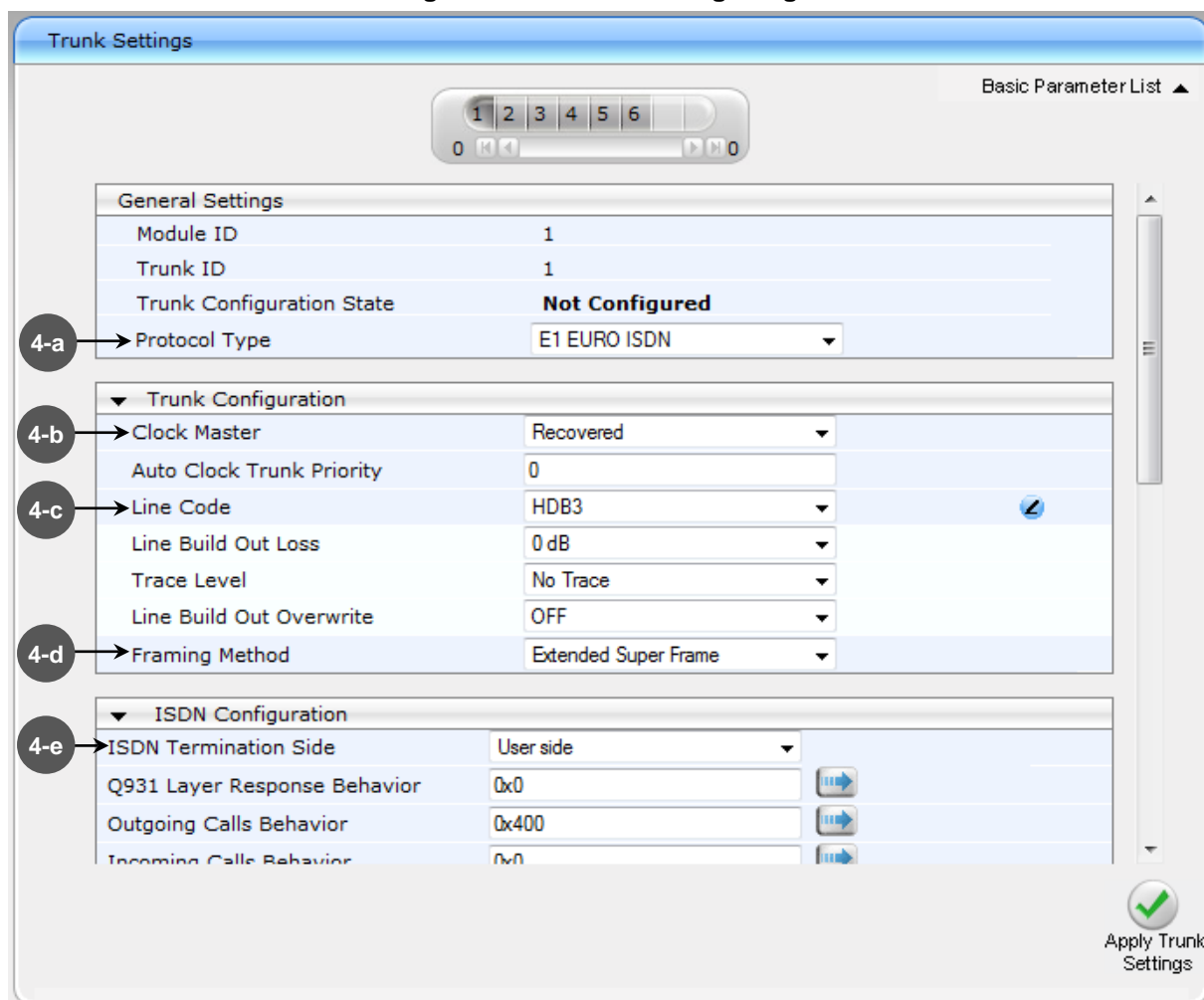
## 4.9.4 Configuring the Trunk

The procedure below describes basic configuration of the physical trunk.

➤ **To configure the physical trunk:**

1. Open the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Trunk Settings**).

**Figure 4-29: Trunk Settings Page**



Trunk Settings

Basic Parameter List ▲

1 2 3 4 5 6

0 0 0

General Settings

Module ID 1

Trunk ID 1

Trunk Configuration State **Not Configured**

4-a → Protocol Type E1 EURO ISDN ▼

▼ Trunk Configuration

4-b → Clock Master Recovered ▼

Auto Clock Trunk Priority 0

4-c → Line Code HDB3 ▼

Line Build Out Loss 0 dB ▼

Trace Level No Trace ▼

Line Build Out Overwrite OFF ▼

4-d → Framing Method Extended Super Frame ▼

▼ ISDN Configuration

4-e → ISDN Termination Side User side ▼


Q931 Layer Response Behavior 0x0 [Apply]

Outgoing Calls Behavior 0x400 [Apply]

Incoming Calls Behavior 0x0 [Apply]

Apply Trunk Settings

2. On the top of the page, a bar with trunk number icons displays the status of each trunk:
  - Grey - disabled
  - Green - active
  - Yellow - RAI alarm
  - Red - LOS / LOF alarm
  - Blue - AIS alarm
  - Orange - D-channel alarm (ISDN only)


Select the Trunk that you want to configure, by clicking the desired trunk number icon.
3. If the trunk is new, configure the trunk as required. If the trunk was previously configured, click the **Stop Trunk**  button to de-activate the trunk.

## 4. Basic trunk configuration:

- a. From the 'Protocol Type' drop-down list, select the required trunk protocol.

**Notes:**

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the Enhanced Gateway.
- All PRI trunks of the Enhanced Gateway must be of the same line type - E1 or T1. However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the Release Notes).
- BRI trunks can operate with E1 or T1 trunks.
- If the trunk can't be stopped because it provides the clock (assuming the Enhanced Gateway is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' page (see Section 4.9.5 on page 44).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to **None**.

- b. From the 'Clock Master' drop-down list, select the trunk's clock source:
    - ◆ **Recovered:** clock source is recovered from the trunk.
    - ◆ **Generated:** clock source is provided by the internal TDM bus clock source (according to the parameter 'TDM Bus Clock Source' – see Section 4.9.5 on page 44).
  - c. From the 'Line Code' drop-down list, select the line code:
    - ◆ **B8ZS** (bipolar 8-zero substitution) for T1 trunks only
    - ◆ **HDB3** (high-density bipolar 3) for E1 trunks only
    - ◆ **AMI** (for E1 and T1)
  - d. From the 'Framing Method' drop-down list, select the required framing method. For E1 trunks always set this parameter to **Extended Super Frame**.
  - e. To configure whether the trunk is connected to the PBX is User or Network side, from the 'ISDN Termination' drop-down list, select **User side** or **Network side**.
5. Continue configuring the trunk according to your requirements.
  6. When you have completed configuration, click the **Apply Trunk Settings**  button to apply the changes to the selected trunk.
  7. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.
  8. On the toolbar, from the 'Device Actions' drop-down list, choose **Reset**, and then in the Maintenance Actions page, click the **Reset** button; the Enhanced Gateway resets and your settings are saved to the flash memory.

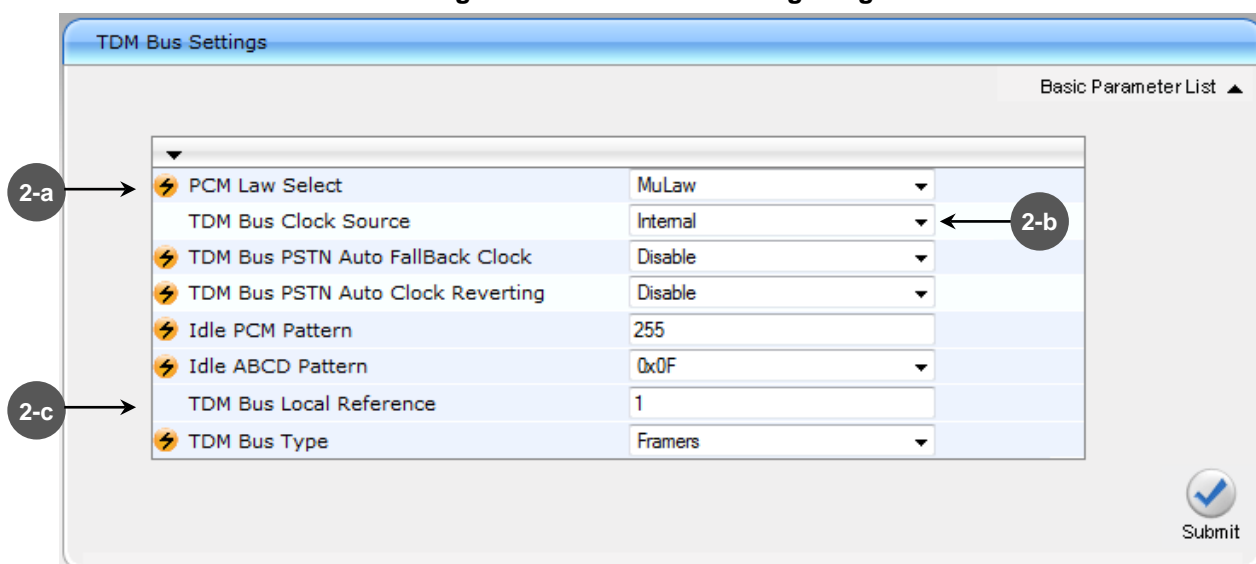
## 4.9.5 Configuring the TDM Bus

The procedure below describes how to configure the TDM bus of the Enhanced Gateway.

➤ **To configure the TDM bus:**

1. Open the TDM Bus Settings page (**Configuration** tab > **VoIP** menu > **TDM** > **TDM Bus Settings**).

**Figure 4-30: TDM Bus Settings Page**



Setting	Value
PCM Law Select	MuLaw
TDM Bus Clock Source	Internal
TDM Bus PSTN Auto FallBack Clock	Disable
TDM Bus PSTN Auto Clock Reverting	Disable
Idle PCM Pattern	255
Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1
TDM Bus Type	Framers

Submit

2. Configure the TDM bus parameters according to your deployment requirements. Below is a description of some of the main TDM parameters:
  - PCM Law Select:** defines the type of PCM companding law in the input/output TDM bus. Typically, A-Law is used for E1 and Mu-Law for T1/J1.
  - TDM Bus Clock Source:** defines the clock source to which the Enhanced Gateway synchronizes - generate clock from local source (Internal) or recover clock from PSTN line (Network).
  - TDM Bus Local Reference:** defines the physical trunk ID from which the Enhanced Gateway recovers (receives) its clock synchronization when the TDM Bus Clock Source is configured to recover the clock from the PSTN line.
3. Click **Submit** to apply your changes.
4. On the toolbar, click **Burn** to save the settings to the Enhanced Gateway flash memory.
5. On the toolbar, from the 'Device Actions' drop-down list, choose **Reset**, and then in the Maintenance Actions page, click the **Reset** button; the Enhanced Gateway resets and your settings are saved to the flash memory.

## 4.10 Step 10: Configuring Normalization Rules for E.164 Format for PBX/PSTN Connectivity

Microsoft Lync 2013 implements the standard E.164 format, while the PBX or PSTN implements other number formats for dialing. If the Enhanced Gateway is connected to a PBX or directly to the PSTN, the Enhanced Gateway may need to perform number manipulations for the called and/or calling number to match the PBX or PSTN dialing rules or to match Microsoft Lync 2013 E.164 format.

Therefore, the Enhanced Gateway must be configured with manipulation rules to translate (i.e., normalize) numbers dialed in standard E.164 format to various formats, and vice versa. Manipulation needs to be done for outbound calls (i.e., calls received from Microsoft Lync clients through Microsoft Lync 2013) and inbound calls (i.e., calls destined to Lync clients).

Number manipulation (and mapping of NPI/TON to SIP messages) rules are configured in the following Manipulation tables:

■ **For Tel-to-IP calls:**

- Destination Phone Number Manipulation Table for Tel-to-IP Calls
- Source Phone Number Manipulation Table for Tel-to-IP Calls

■ **For IP-to-Tel calls:**

- Destination Phone Number Manipulation Table for IP-to-Tel Calls
- Source Phone Number Manipulation Table for IP-to-Tel Calls

Number manipulation configuration examples are provided for inbound and outbound calls in Section 4.10.1.

➤ **To configure number manipulation rules:**

1. Open the required Number Manipulation page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Manipulations** > **Dest Number IP -> Tel** or **Dest Number Tel -> IP**, **Source Number IP -> Tel**, or **Source Number Tel -> IP**); the relevant Manipulation table page is displayed.
2. Click the **Add** button; the following dialog box is displayed:

**Figure 4-31: Number Manipulation Table - Add Dialog Box**

Rule	Action
Index	0
Destination Prefix	*
Source Prefix	*
Source IP Address	*
Source Host Prefix	*
Destination Host Prefix	*

3. Click the **Rule** tab, and then configure the matching characteristics. For a description of the parameters, see the table below.
4. Click the **Action** tab, and then configure the manipulation operation. For a description of the parameters, see the table below.

5. Click **Submit** to apply your changes.
6. On the toolbar, click **Burn** to save the changes to the Enhanced Gateway flash memory.

**Table 4-1: Number Manipulation Parameters Description**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Destination Prefix	Defines the destination (called) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the \$ sign to denote calls without a called number.
Source Prefix	Defines the source (calling) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the \$ sign to denote calls without a calling number.
Source IP Address	<p>Defines the source IP address of the caller. This is obtained from the Contact header in the INVITE message.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the number manipulation tables for IP-to-Tel calls.</li> <li>▪ The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99.</li> <li>▪ The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all IP addresses between 10.8.8.0 and 10.8.8.255.</li> </ul>
Source Host Prefix	<p>Defines the URI host name prefix of the incoming SIP INVITE message in the From header.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the number manipulation tables for IP-to-Tel calls.</li> <li>▪ The asterisk (*) wildcard can be used to denote any prefix.</li> <li>▪ If the P-Asserted-Identity header is present in the incoming INVITE message, then the value of this parameter is compared to the P-Asserted-Identity URI host name (instead of the From header).</li> </ul>
Destination Host Prefix	<p>Defines the Request-URI host name prefix of the incoming SIP INVITE message.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the number manipulation tables for IP-to-Tel calls.</li> <li>▪ The asterisk (*) wildcard can be used to denote any prefix.</li> </ul>

Parameter	Description
Source Trunk Group	<p>Defines the source Trunk Group ID for Tel-to-IP calls. To denote all Trunk Groups, leave this field empty.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The value -1 indicates that this field is ignored in the rule.</li> <li>This parameter is applicable only to the number manipulation tables for Tel-to-IP calls.</li> <li>For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).</li> </ul>
Source IP Group	<p>Defines the IP Group from where the IP call originated. Typically, the IP Group of an incoming INVITE is determined or classified using the Inbound IP Routing Table. If not used (i.e., any IP Group), leave the field empty.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The value -1 indicates that this field is ignored.</li> <li>This parameter is applicable only to the number manipulation tables for Tel-to-IP calls.</li> <li>If this Source IP Group has a Serving IP Group, then all calls from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if the 'PreferRouteTable' parameter is set to 1.</li> </ul>
Destination IP Group	<p>Defines the IP Group to where the call is sent.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The value -1 indicates that this field is ignored.</li> <li>This parameter is applicable only to the Destination Phone Number Manipulation Table for Tel -&gt; IP Calls.</li> </ul>
<b>Operation (Action)</b>	
Stripped Digits From Left	<p>Defines the number of digits to remove from the left of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234.</p>
Stripped Digits From Right	<p>Defines the number of digits to remove from the right of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 5551.</p>
Prefix to Add	<p>Defines the number or string that you want added to the front of the telephone number. For example, if you enter 9 and the phone number is 1234, the new number is 91234.</p>
Suffix to Add	<p>Defines the number or string that you want added to the end of the telephone number. For example, if you enter 00 and the phone number is 1234, the new number is 123400.</p>
Number of Digits to Leave	<p>Defines the number of digits that you want to keep from the right of the phone number. For example, if you enter 4 and the phone number is 00165751234, then the new number is 1234.</p>

Parameter	Description
NPI	<p>Defines the Numbering Plan Indicator (NPI).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Unknown (default)</li> <li>▪ <b>[9]</b> Private</li> <li>▪ <b>[1]</b> E.164 Public</li> <li>▪ <b>[-1]</b> Not Configured = value received from PSTN/IP is used</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to number manipulation tables for IP-to-Tel calls.</li> <li>▪ NPI can be used in the SIP Remote-Party-ID header by using the 'EnableRPIHeader' and 'AddTON2RPI' parameters.</li> <li>▪ For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 49.</li> </ul>
TON	<p>Defines the Type of Number (TON).</p> <ul style="list-style-type: none"> <li>▪ If you selected 'Unknown' for the NPI, you can select Unknown <b>[0]</b>.</li> <li>▪ If you selected 'Private' for the NPI, you can select Unknown <b>[0]</b>, Level 2 Regional <b>[1]</b>, Level 1 Regional <b>[2]</b>, PISN Specific <b>[3]</b> or Level 0 Regional (Local) <b>[4]</b>.</li> <li>▪ If you selected 'E.164 Public' for the NPI, you can select Unknown <b>[0]</b>, International <b>[1]</b>, National <b>[2]</b>, Network Specific <b>[3]</b>, Subscriber <b>[4]</b> or Abbreviated <b>[6]</b>.</li> </ul> <p>The default is 'Unknown'.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to number manipulation tables for IP-to-Tel calls.</li> <li>▪ TON can be used in the SIP Remote-Party-ID header by using the 'EnableRPIHeader' and 'AddTON2RPI' parameters.</li> <li>▪ For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 49.</li> </ul>
Presentation	<p>Enables caller ID.</p> <ul style="list-style-type: none"> <li>▪ Not Configured = Privacy is determined according to the Caller ID table.</li> <li>▪ <b>[0]</b> Allowed = Sends Caller ID information when a call is made using these destination/source prefixes.</li> <li>▪ <b>[1]</b> Restricted = Restricts Caller ID information for these prefixes.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This field is applicable only to number manipulation tables for source phone number manipulation.</li> <li>▪ If this field is set to <b>Restricted</b> and the 'Asserted Identity Mode' (AssertedIdMode) parameter is set to <b>P-Asserted</b>, the From header in the INVITE message includes the following: From: 'anonymous' &lt;sip:anonymous@anonymous.invalid&gt; and 'privacy: id' header.</li> </ul>



## 4.10.1 Number Normalization Examples

Two examples are provided below for number normalization. The examples are based on the following assumptions:

- PBX with prefix (local) number 333
- 4-digit extension numbers that begin with the digit 1 (i.e., 1xxx)
- National area code is 206
- Country code is 1

### 4.10.1.1 Modifying E.164 Numbers to PBX / PSTN Format for Outbound Calls

Outbound calls refer to calls made by Lync clients to a PBX / PSTN number:

1. **Local Calls within PBX:** The caller dials only the last four digits (e.g., 1212). Lync translates (normalizes) the phone number into an E.164 number format: +12063331212 (where +1 is the country code, 206 the local area code, and 333 the PBX prefix number). The Manipulation table is configured to send only the last four digits to the PBX (i.e., 1212).
2. **National Calls to the Same Area Code:** The caller dials 9 for an external line, and then dials a 7-digit telephone number (e.g., 9-555-4321). Lync translates (normalizes) the phone number into an E.164 number format: +12065554321 (where +1 is the country code, 206 the local area code, 5554321 the phone number). The Manipulation table is configured to remove (strip) the first five digits and add 9 as a prefix to the remaining number. Therefore, the Enhanced Gateway sends the number 95554321 to the PBX, and then the PBX sends the number 5554321 to the PSTN.
3. **National Calls to a Different Area Code:** The caller dials 9 for an external line, the out-of-area code, and then a 7-digit telephone number (e.g., 9-503-331-1425). Lync translates (normalizes) the phone number into an E.164 number format: +15033311425 (where +1 is the international code, 503 the out-of area code, 3311425 the phone number). The Manipulation table is configured to remove (strip) the first two digits (i.e., +1), then add 9 as a prefix to the remaining number. Therefore, the Enhanced Gateway sends the number 95033311425 to the PBX, and then the PBX sends the number 5033311425 to the PSTN.
4. **Dialing International Calls:** The caller dials 9 for an external line, the access code for international calls (e.g., 011 for the US), the country code (e.g., +44 for the UK), the area code (e.g., 1483), and then a 6-digit telephone number (e.g., 829827). Lync translates (normalizes) the phone number into an E.164 number format: +441483829827 (where +44 is the country code, 1483 the area code, 829827 the phone number). The Manipulation table is configured to remove the first digit (e.g., +), and add the external line digit (e.g., 9) and the access code for international calls (e.g., 011 for the US) as the prefix. Therefore, the Enhanced Gateway sends the number 9011441483829827 to the PBX and the PBX, in turn, sends the number 011441483829827 to the PSTN.

The configuration of the above scenarios is shown in the [Figure 4-32](#).

**Figure 4-32: Destination Phone Number Manipulation Table for IP→Tel Calls**

Destination Phone Number Manipulation Table for IP -> Tel Calls							
Add +		Insert +					
Index	Destination Prefix	Source Prefix	Source IP Address	Source Host Prefix	Destination Host Prefix	Prefix to Add	Suffix to Add
1	+1206333	*	*	*	*		
2	+206	*	*	*	*	9	
3	+1	*	*	*	*	9	
4	+	*	*	*	*	9011	

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

#### 4.10.1.2 Modifying PBX, Local, and National Calls to E.164 Format for Inbound Calls

Inbound calls refer to calls received by Lync clients from the PBX / PSTN:

- 1. Local Calls from the PBX / PSTN:** The PBX user only dials a 4-digit extension number of the Lync client (e.g., 1220). The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206333 to the extension number. Therefore, the Enhanced Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
- 2. National Calls with the Same Area Code:** The PSTN user dials a 7-digit phone number (e.g., 333-1220), which is received by the Enhanced Gateway. The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1206 to the number. Therefore, the Enhanced Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
- 3. National Calls from a Different Area Code:** The PSTN user dials the national area code and then a 7-digit phone number (e.g., 206-333-1220), which is received by the Enhanced Gateway. The Manipulation table is configured to normalize the number into E.164 format and adds the prefix +1 to the number. Therefore, the Enhanced Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.
- 4. International Calls:** The PSTN international (overseas) caller dials the international access and country code (e.g., 001 for the US), the national area code, and then a 7-digit phone number (e.g., 206-333-1220), which is received by the Enhanced Gateway. The Manipulation table is configured to normalize the number into E.164 format, by removing the first two digits (e.g., 00) and adding the prefix plus sign (+). Therefore, the Enhanced Gateway sends the number +12063331220 to Lync, which relays the call to the Lync client.



**Note:** The international and country codes that are received by the Enhanced Gateway depend on the respective country's PSTN numbering rules.

The configuration of the above scenarios is shown in the figure below:

**Figure 4-33: Destination Phone Number Manipulation Table for Tel→IP Calls**

Destination Phone Number Manipulation Table for Tel -> IP Calls						
<div>Add +</div> <div>Insert +</div>						
Index	Destination Prefix	Source Prefix	Source Trunk Group	Destination IP Group	Prefix to Add	Suffix to Add
1	1xxx	*	-1	-1	+1206333	
2	333	*	-1	-1	+1206	
3	206	*	-1	-1	+1	
4	00	*	-1	-1	+	
<div> <div> <div>1</div> <div>&lt;&gt;</div> </div> <div>Page 1 of 1</div> <div> <div>10</div> <div>▼</div> </div> <div>Show 10 records per page</div> <div>View 1 - 4 of 4</div> </div>						

## 4.11 Miscellaneous Configuration

This step describes the miscellaneous Gateway configuration.

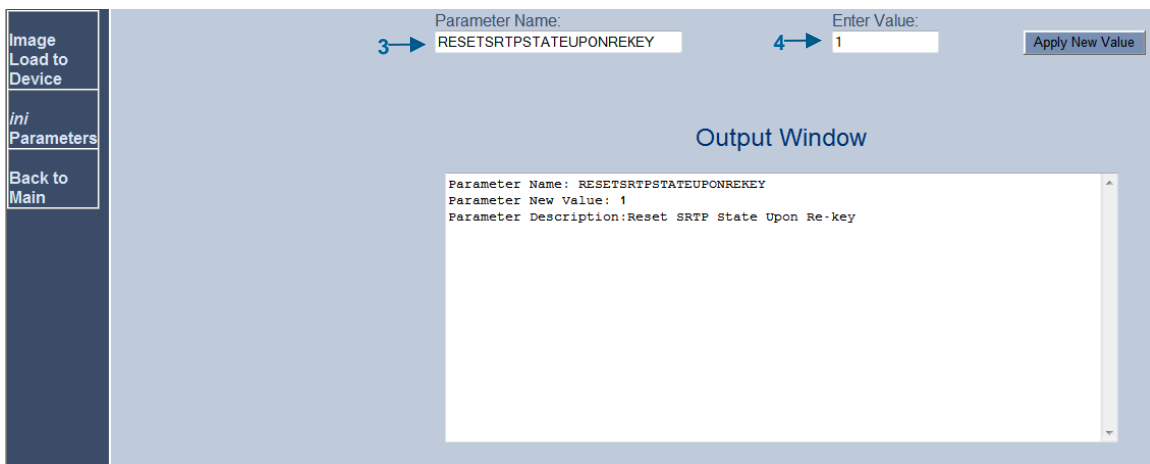
### 4.11.1 Configuring SRTP Behavior upon Rekey Mode

This section describes how to configure SRTP Behavior upon Rekey Mode.

➤ **To configure SRTP Behavior upon Rekey Mode:**

1. Open the Admin page by appending the case-sensitive suffix 'AdminPage' to the Gateway's IP address in your Web browser's URL field (e.g., <http://10.15.4.22/AdminPage>).
2. On the left pane, click **ini** Parameters.

**Figure 4-34: AdminPage**



3. In the 'Parameter Name' field, enter RESETSRTPSTATEUPONREKEY.
4. In the 'Enter Value' field, enter 1.
5. Click the **Apply New Value** button.

## A Configuring Lync Server 2013

This appendix describes how to configure Microsoft Lync Server 2013 topology builder to operate with the AudioCodes Enhanced Gateway.

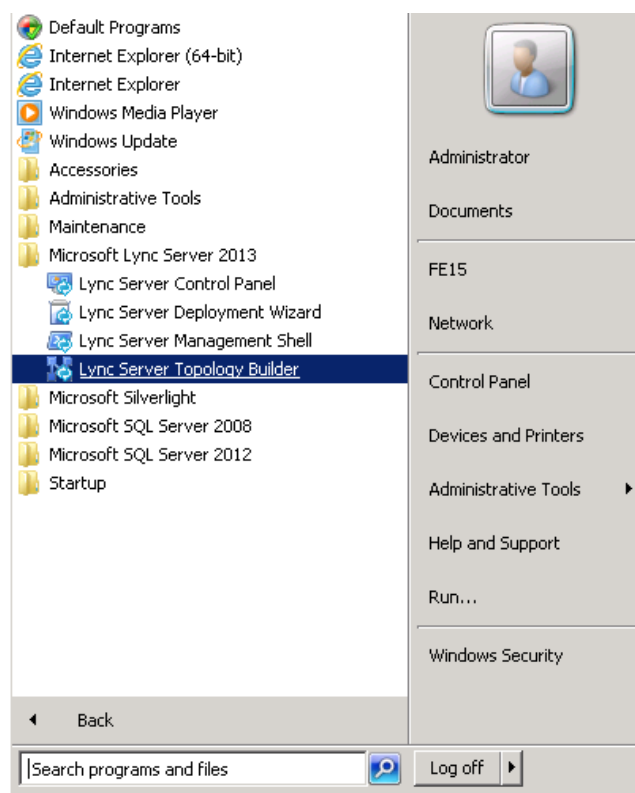


**Note:** Routes, Dial plans, voice policies, and PSTN usages are also necessary for Enterprise voice deployment; however, they are beyond the scope of this document.

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

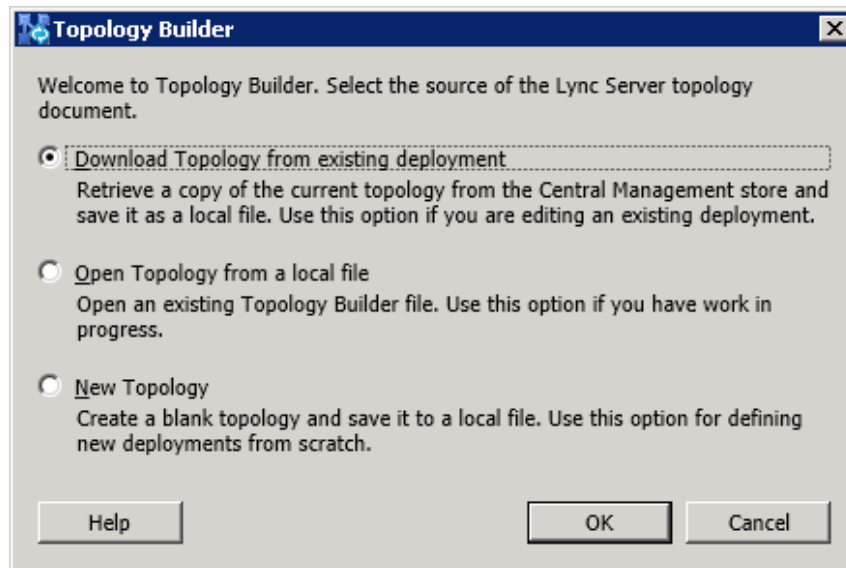
- **To configure the Gateway as an IP/PSTN Gateway and associate it with the Mediation Server:**
- 1. On the Microsoft Lync server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Point to **Start** menu > **All Programs** > **Lync Server Topology Builder**).

**Figure A-1: Starting the Lync Server Topology Builder**



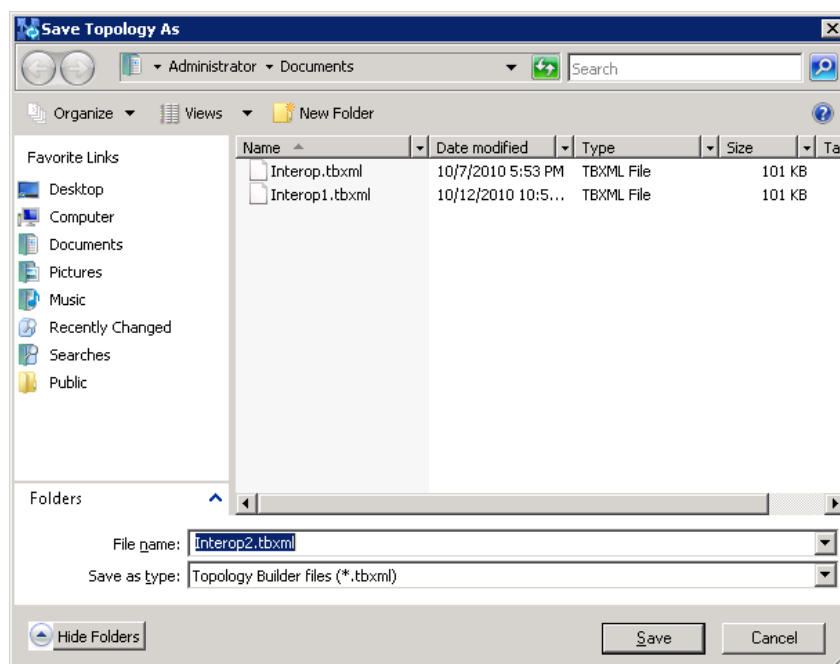
The Topology Builder screen is displayed:

**Figure A-2: Topology Builder Options**



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

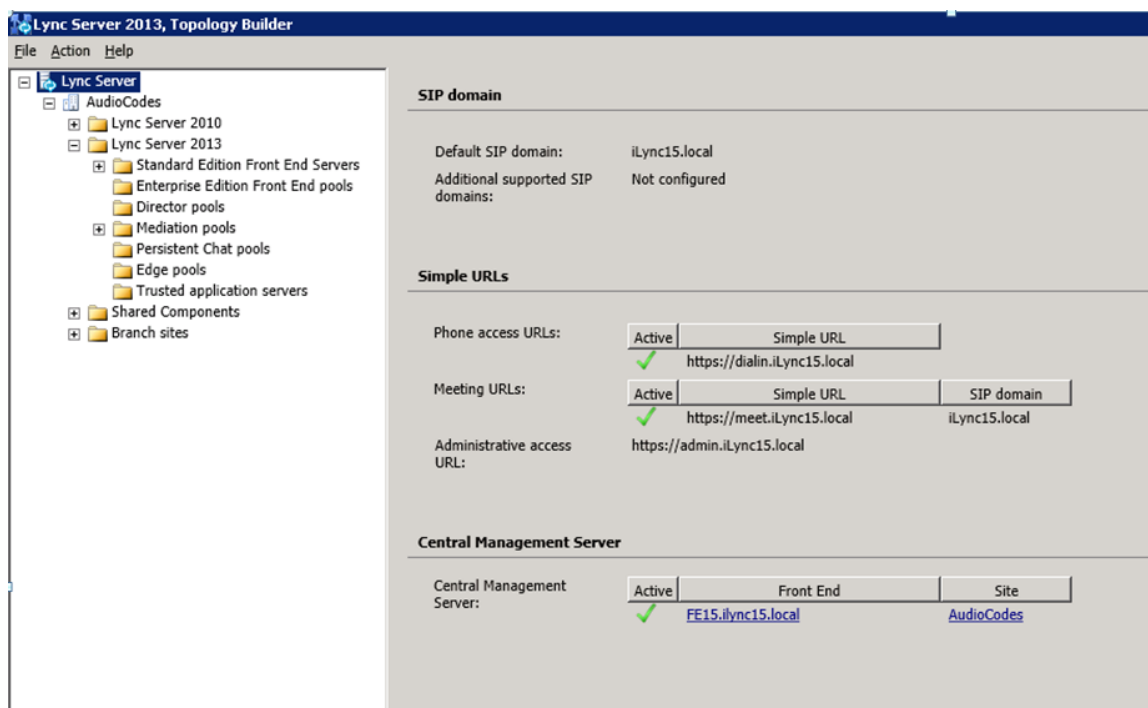
**Figure A-3: Save Topology**



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

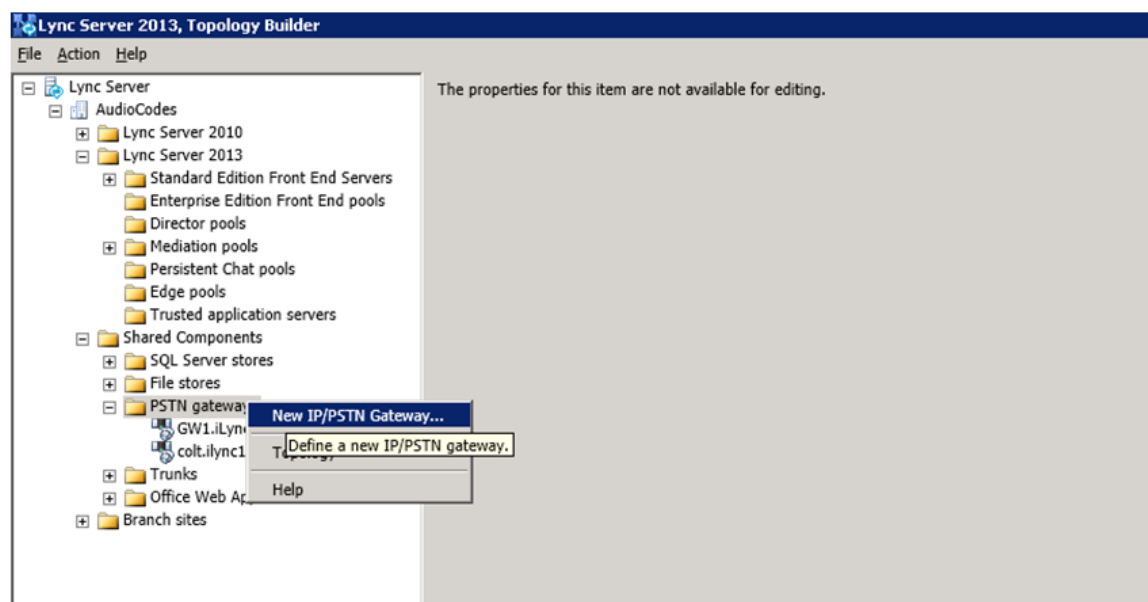
The Topology Builder screen with the downloaded Topology is displayed:

**Figure A-4: Downloaded Topology**



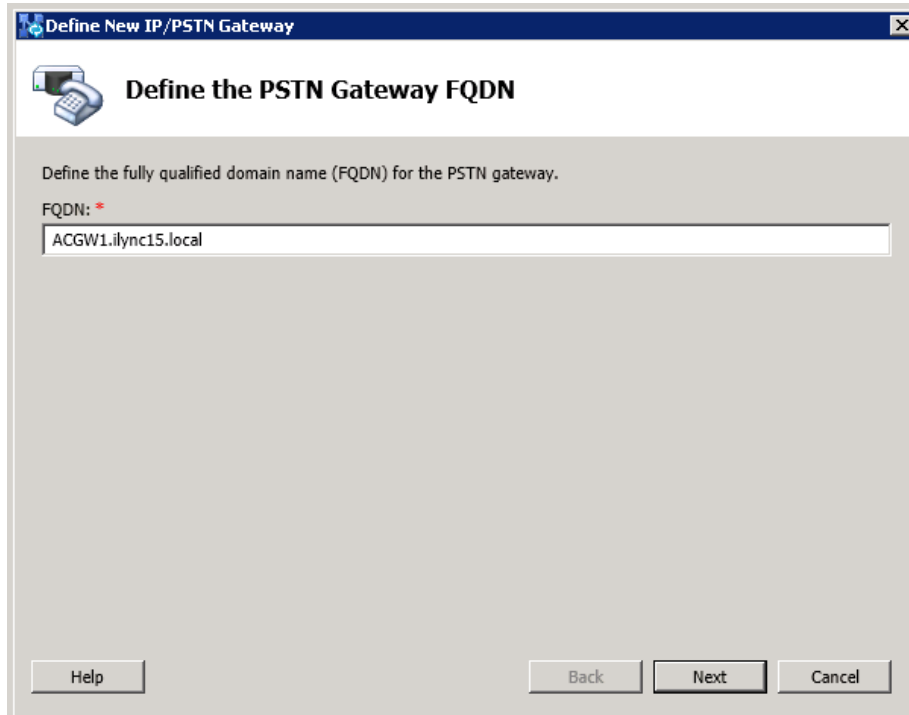
4. In the Navigation tree, select **Lync Server 2013 > Site name i.e. AudioCodes > Shared Components > PSTN Gateways**.
5. Right-click the **PSTN gateways** folder, and then in the pop-up dialog, choose **New IP/PSTN Gateway** as shown below:

**Figure A-5: Choosing New IP/PSTN Gateway**



The following dialog box appears:

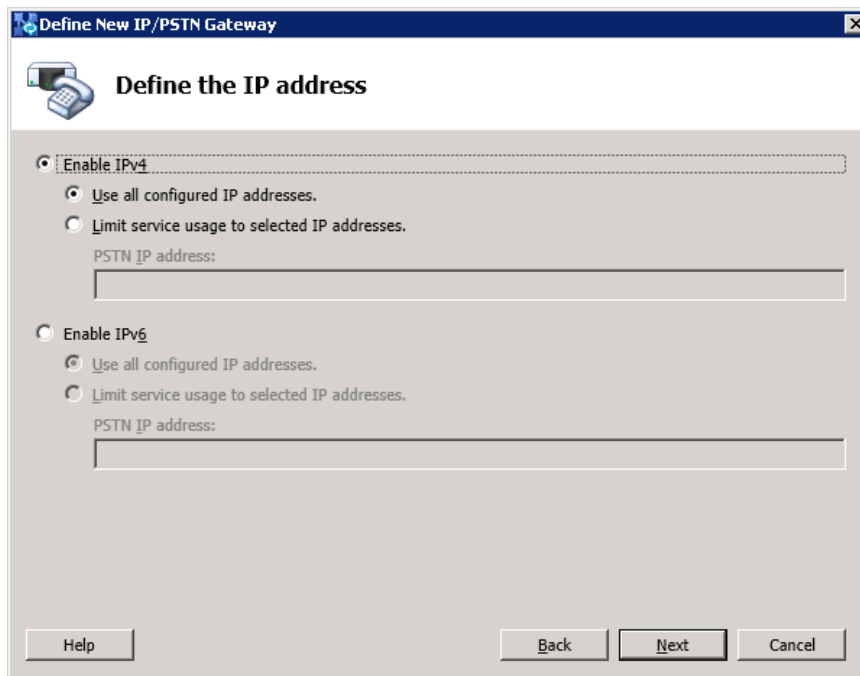
**Figure A-6: Define New IP/PSTN Gateway**



The dialog box is titled "Define New IP/PSTN Gateway". It features a telephone icon and the heading "Define the PSTN Gateway FQDN". Below the heading, it says "Define the fully qualified domain name (FQDN) for the PSTN gateway." There is a label "FQDN: \*" followed by a text input field containing "ACGW1.ilync15.local". At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".

6. In the 'FQDN' field, enter the Fully Qualified Domain Name (FQDN) of the Gateway (e.g., "ACGW1.ilync15.local"); this FQDN should be updated in the relevant DNS record ,and then click **Next**; the Define the IP address screen is displayed:

**Figure A-7: Define the IP Address**

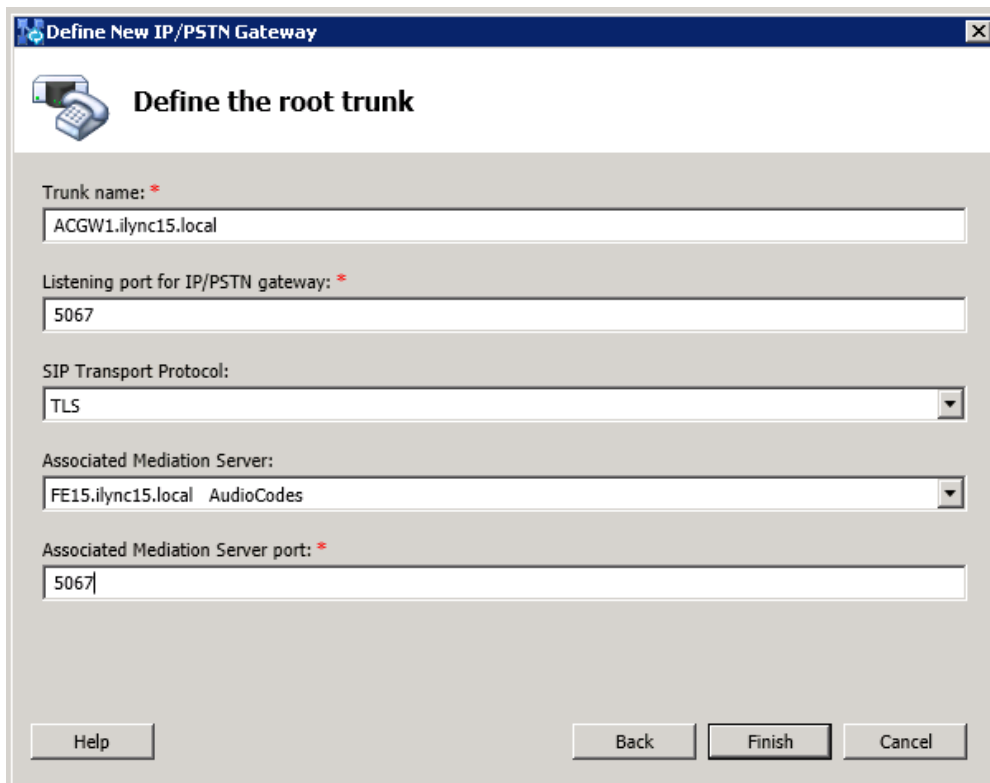


The dialog box is titled "Define New IP/PSTN Gateway". It features a telephone icon and the heading "Define the IP address". Below the heading, there are two main sections. The first section is "Enable IPv4", which is selected with a radio button. It contains two sub-options: "Use all configured IP addresses." (selected) and "Limit service usage to selected IP addresses." (unselected). Below these is a text input field labeled "PSTN IP address:". The second section is "Enable IPv6", which is unselected. It also contains two sub-options: "Use all configured IP addresses." (selected) and "Limit service usage to selected IP addresses." (unselected). Below these is another text input field labeled "PSTN IP address:". At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".



7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and click **Next**; the Define the root trunk screen is displayed:

**Figure A-8: Define the Root Trunk**



**Define New IP/PSTN Gateway**

**Define the root trunk**

Trunk name: \*

ACGW1.ilync15.local

Listening port for IP/PSTN gateway: \*

5067

SIP Transport Protocol:

TLS

Associated Mediation Server:

FE15.ilync15.local AudioCodes

Associated Mediation Server port: \*

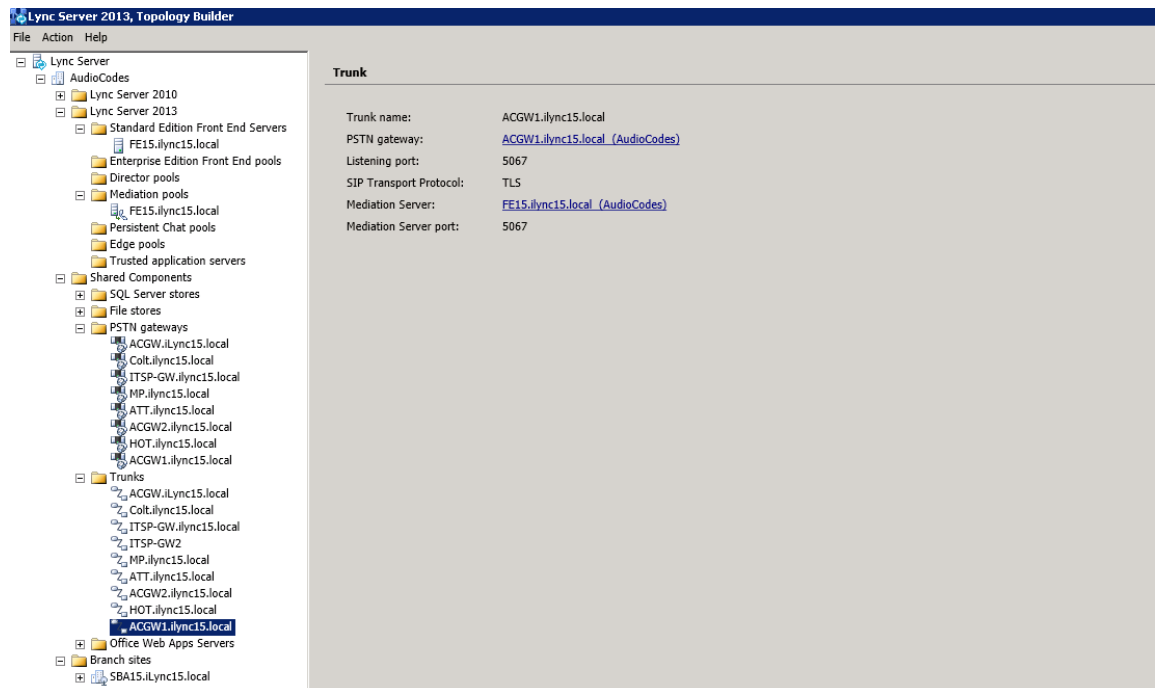
5067

Help Back Finish Cancel

8. In the Trunk name field, define a *root trunk* for the PSTN gateway. A trunk is a logical connection between a Mediation Server and a gateway uniquely identified by the combination (Mediation Server FQDN, Mediation Server listening port (TLS or TCP) : gateway IP and FQDN, gateway listening port):
  - When defining a PSTN gateway in the 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.
9. In the 'Listening Port for IP/PSTN' gateway field, type the listening port that the Gateway uses for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (i.e. 5067).
10. In the 'SIP Transport Protocol' field, select the transport type (i.e. TLS) that the trunk uses.
11. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN Gateway.
12. In the 'Associated Mediation Server port', type the listening port that the Mediation Server will use for SIP messages from the Gateway (i.e. 5067).
13. Click **Finish**.

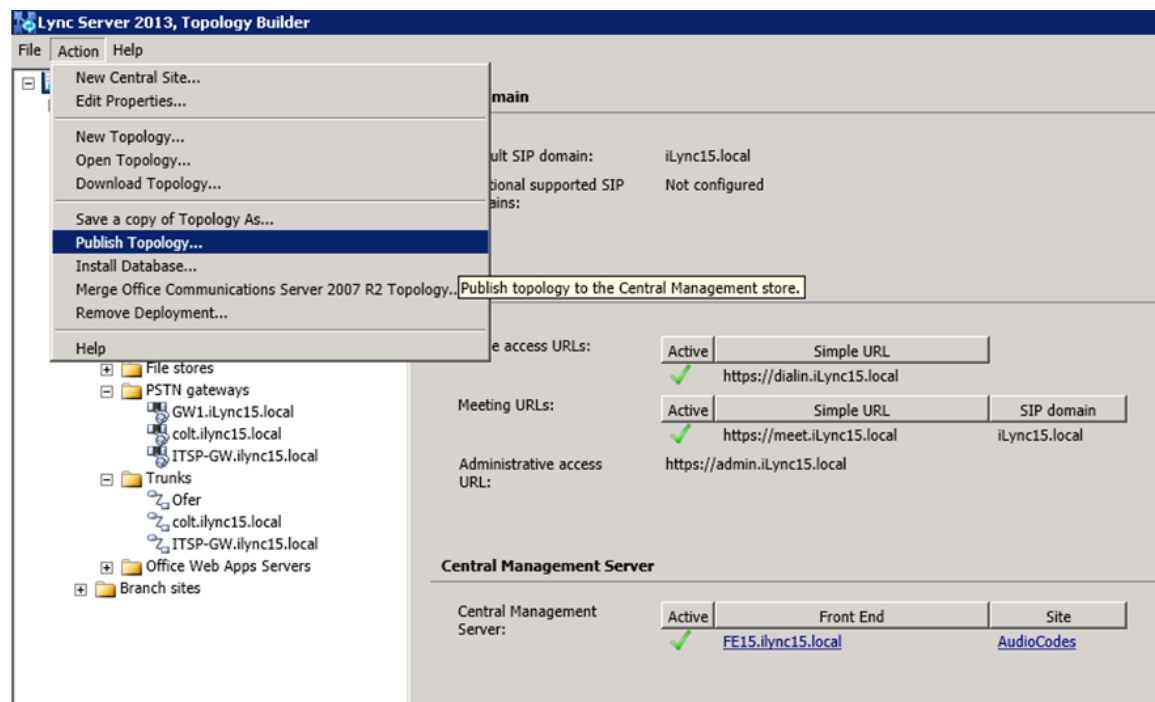
The Gateway is added as a PSTN Gateway and a trunk is created as shown below:

**Figure A-9: Gateway Added as an IP/PSTN Gateway and Trunk created**



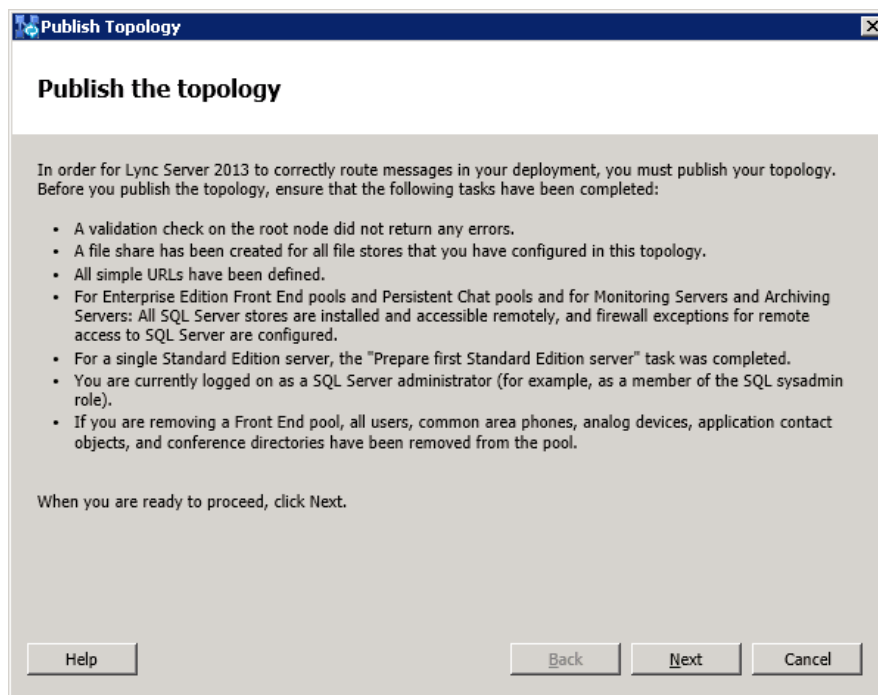
14. Publish the Topology; In the Navigation tree, select the root item **Lync Server**, and then in the Main Menu, choose **Action > Publish Topology**.

**Figure A-10: Choosing Publish Topology**



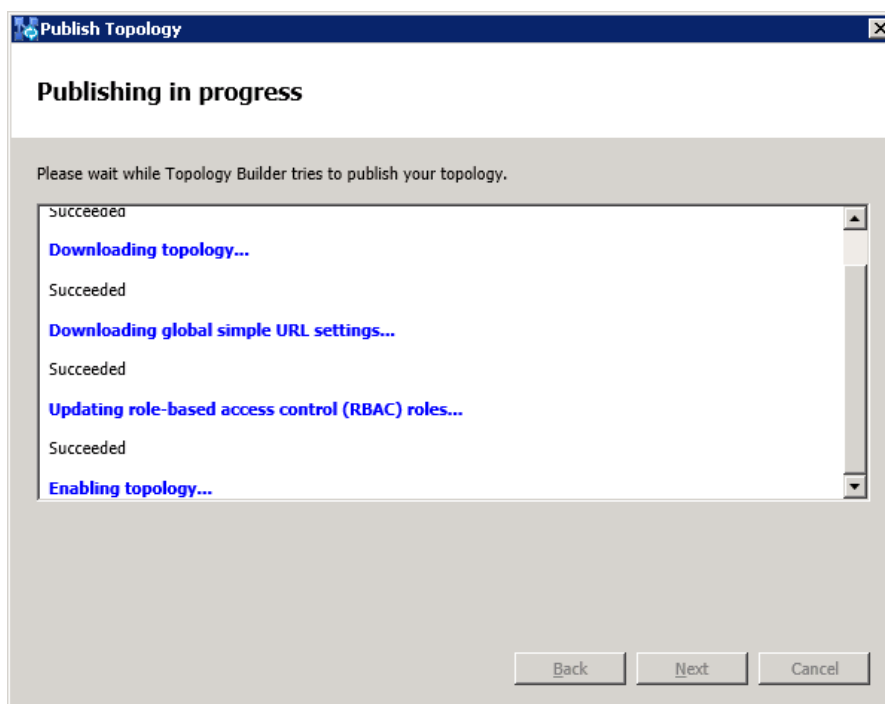
The Publish Topology screen is displayed:

**Figure A-11: Publish Topology Screen**



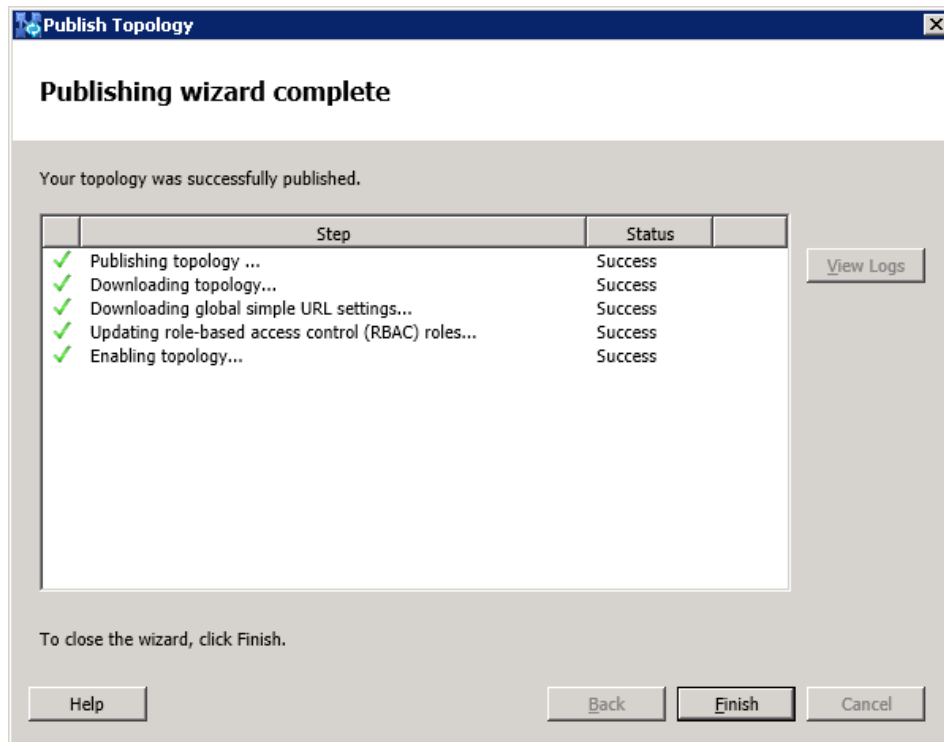
15. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

**Figure A-12: Publish Topology Progress Screen**



16. Wait until the publishing topology process completes successfully:

**Figure A-13: Publish Topology Successfully Completed**



17. Click **Finish**.

## **Reader's Notes**

## Configuration Note