Configuration Note

Connecting Microsoft® Lync™ and Skype SIP Trunk using AudioCodes® Mediant™ 1000 MSBG

Version 6.2

February 2012

Document #: LTRT-41301

Table of Contents

List of Figures

List of Tables

Notice

This document describes how to connect the Microsoft Lync server and Skype SIP Trunking using the Mediant 1000 MSBG SIP device.

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.

Date Published: February-27-2012

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.

Table 1-1: Acronyms

Acronym	Meaning
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 MEDIANT 1000 MSBG device to work with the Skype SIP Trunking and Microsoft Lync Communication platform.

This configuration note is intended for Installation Engineers or AudioCodes and Skype Partners who are installing and configuring the Skype SIP Trunking and Microsoft Lync Communication platform to place VoIP calls using the AudioCodes gateway.

The AudioCodes Mediant 1000 MSBG device was used to implement this solution.

The Mediant 1000 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 MSBG device offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications, as well as flexible PSTN and legacy PBX connectivity.

Note: The scope of this document does not cover security aspects for connecting the SIP Trunk to the Microsoft Lync environment. Security measures should be implemented in accordance with your organization’s security policies. For basic security guidelines, 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 1000 MSBG
Software Version	SIP_6.20A.022.003
Interface Type	SIP/IP
VoIP Protocol	SIP
Additional Notes	None

2.2 Skype SIP Trunking Version

Table 2-2: Skype Version

Gateway Vendor	Skype
Models	
Software Version	
VoIP Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Version

Table 2-3: Microsoft Lync Version

Gateway 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 Microsoft® Lync server 2010 in its private network for enhanced communication within the company.
- The enterprise decides to offer its employees Enterprise voice and to connect the company to the PSTN network using the Skype SIP Trunking service.
- AudioCodes Session Border Controller (SBC) is used to manage the connection between the Enterprise LAN and the Skype 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 Skype SIP trunk in the public network.

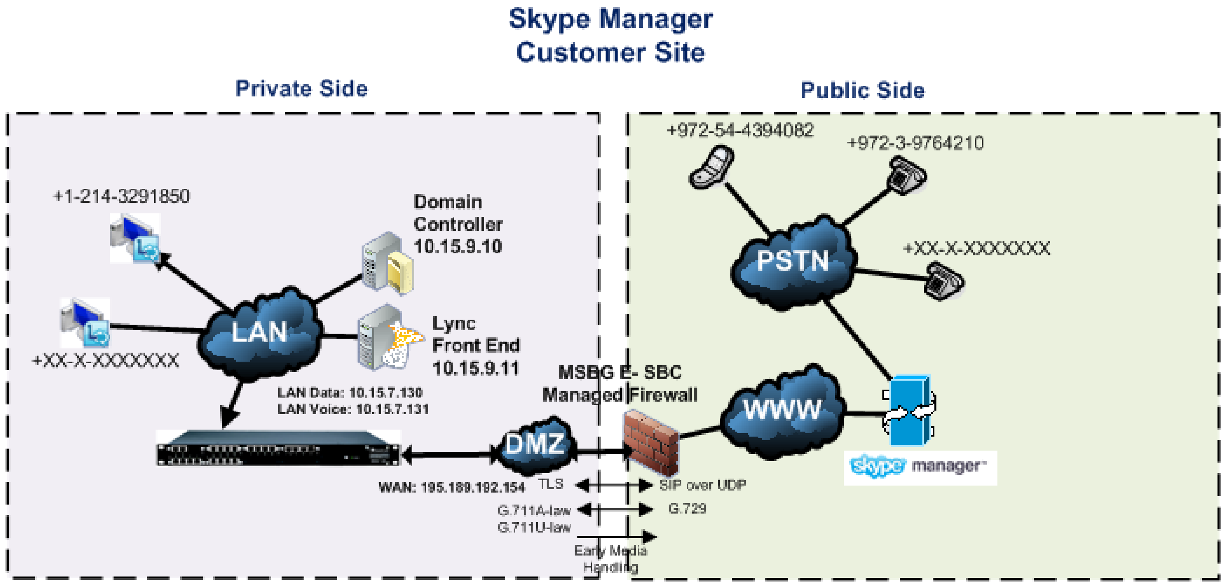
Figure 2-1 below illustrates the interoperability topology between the Microsoft® Lync Server 2010 LAN and the Skype SIP Trunking site.

The setup requirements are characterized as follows:

- While the Microsoft® Lync Server 2010 environment is located on the Enterprise's Local Area Network (LAN), the Skype SIP Trunks are located on the WAN.
- The internal data routing capabilities of the Mediant 1000 MSBG device are used. Consequently, a separate WAN interface is configured in the LAN.
- Microsoft® Lync Server 2010 works with the TLS transport type, while the Skype SIP trunk works on the SIP over UDP transport type.
- Transcoding support: Microsoft® Lync Server 2010 supports G.711A-law and G.711U-law coders, while the Skype SIP Trunk also supports the G.729 coder type.

- Support for early media handling

Figure 2-1: Topology



Reader's Notes

3 Configuring Lync Server 2010

This section describes how to configure the Lync Server 2010 to operate with the Mediant 1000 MSBG. This section describes the following procedures:

1. Configuring the Mediant 1000 MSBG as a 'IP/PSTN Gateway'. See Section 3.1 on page 15.
2. Associating the 'IP/PSTN Gateway' with the Mediation Server. See Section 3.2 on page 20.
3. Configuring a 'Route' to utilize the SIP trunk connected to the Mediant 1000 MSBG. See Section 3.3 on page 26.

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

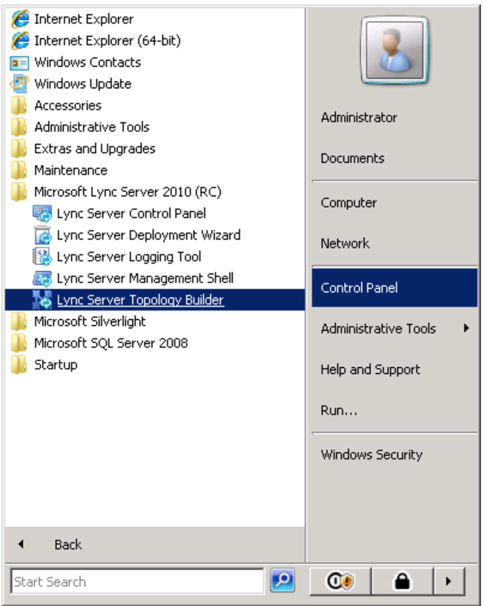
3.1 Configuring the Mediant 1000 MSBG as a 'IP/PSTN Gateway'

This section describes how to configure the Mediant 1000 MSBG as an IP/PSTN Gateway.

➢ **To configure the Mediant 1000 MSBG as a IP/PSTN Gateway and associating it with the Mediation Server:**

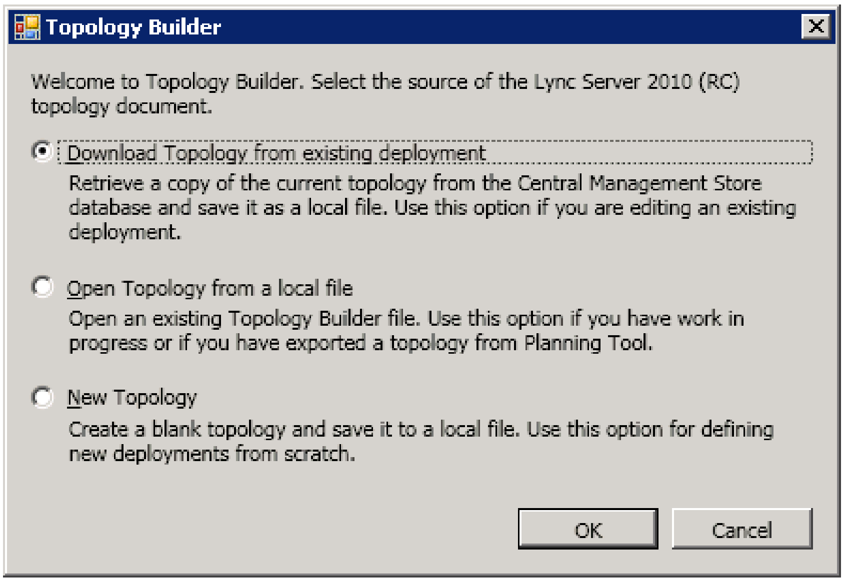
1. On the server where the Topology Builder is located, start the Lync Server 2010 **Topology Builder**: Click **Start**, select **All Programs**, then select **Lync Server Topology Builder**.

Figure 3-1: Starting the Lync Server Topology Builder



The following screen is displayed:

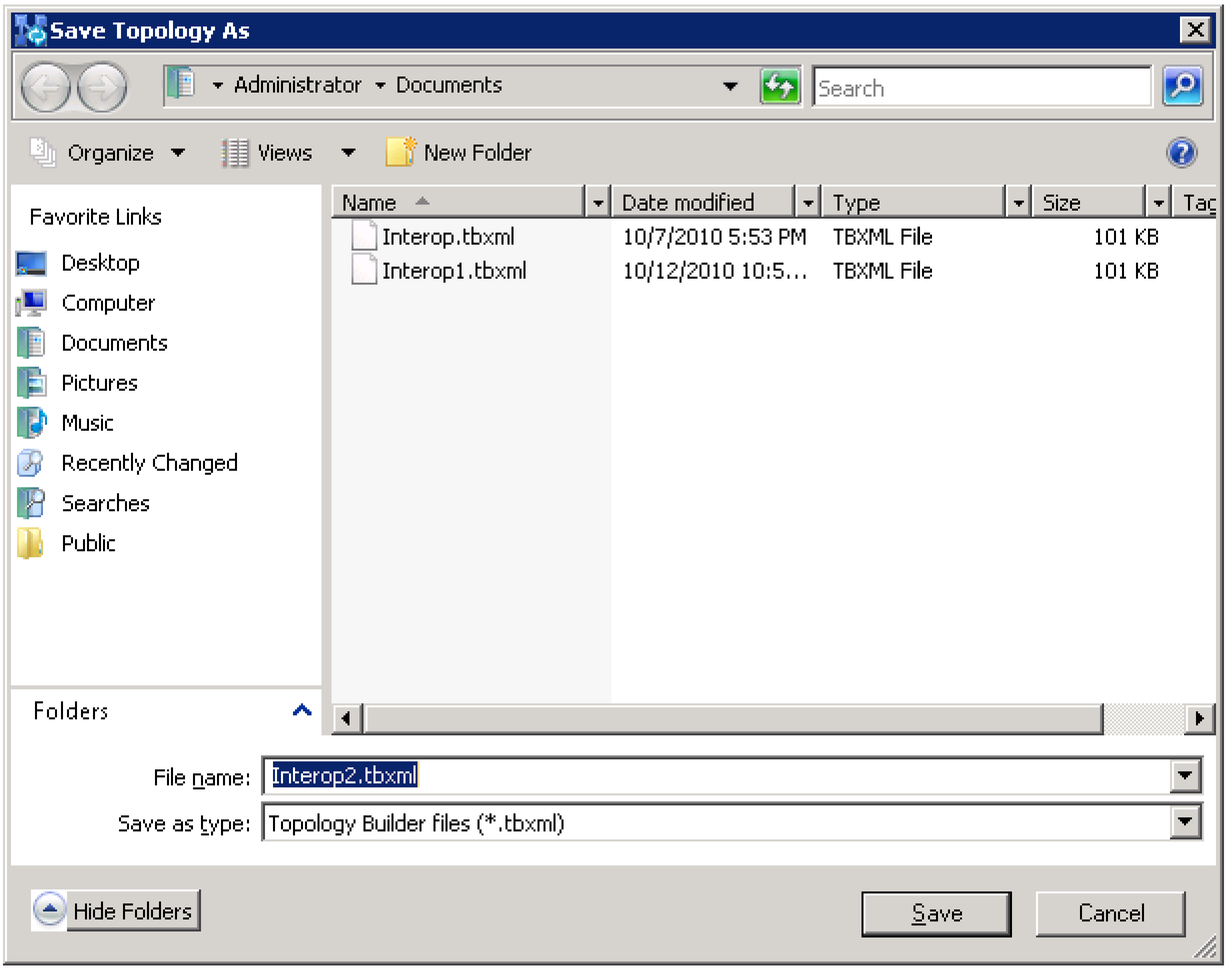
Figure 3-2: Topology Builder Options



2. Choose 'Download Topology from the existing deployment and click **OK**.

   You are prompted to save the Topology which you have downloaded.

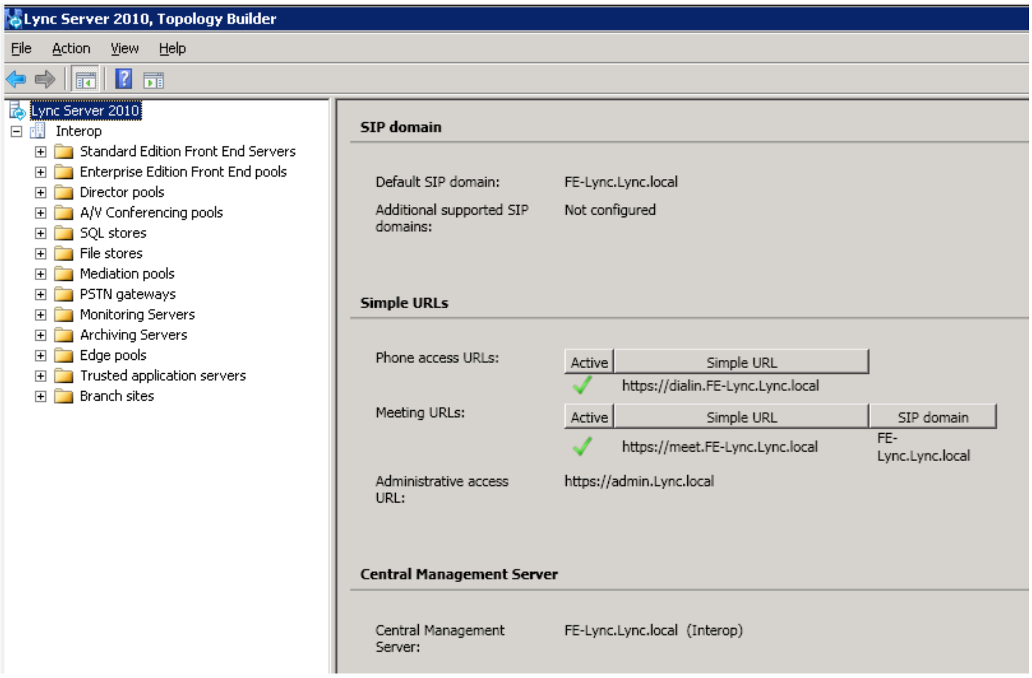
Figure 3-3: Save Topology



3. Enter new **File Name** and **Save** – this action enables you to rollback from any changes you make during the installation.

   The Topology Builder screen with the topology downloaded is displayed.

Figure 3-4: Downloaded Topology



4. Expand the Site; right-click on the IP/PSTN Gateway and choose 'New IP/PSTN Gateway'.

Figure 3-5: New IP/PSTN Gateway

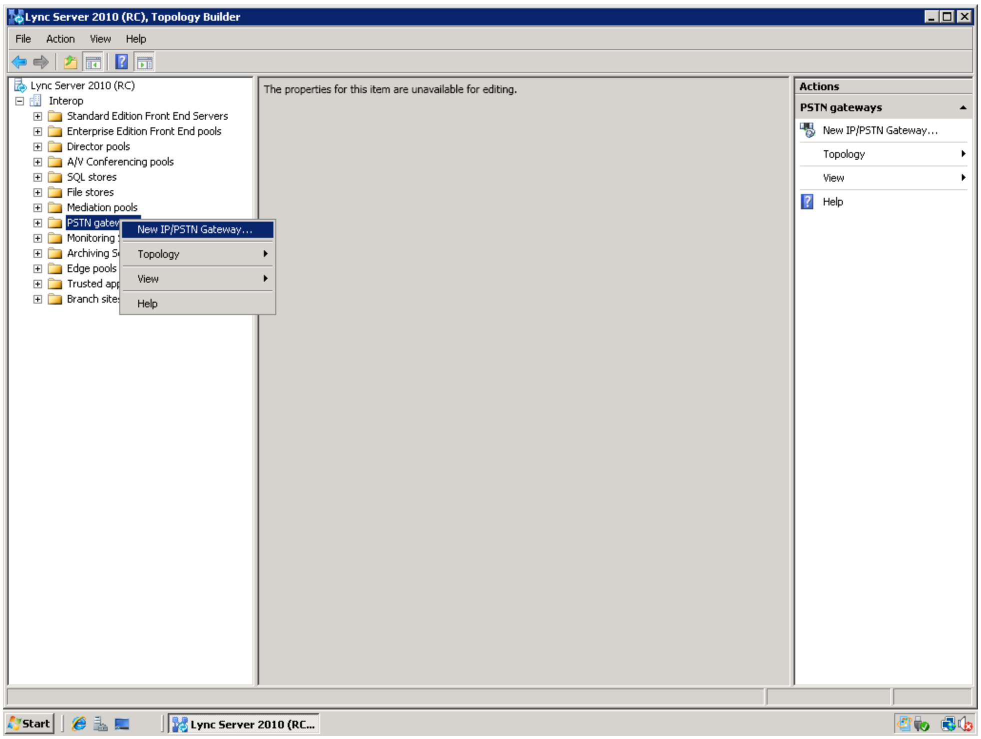
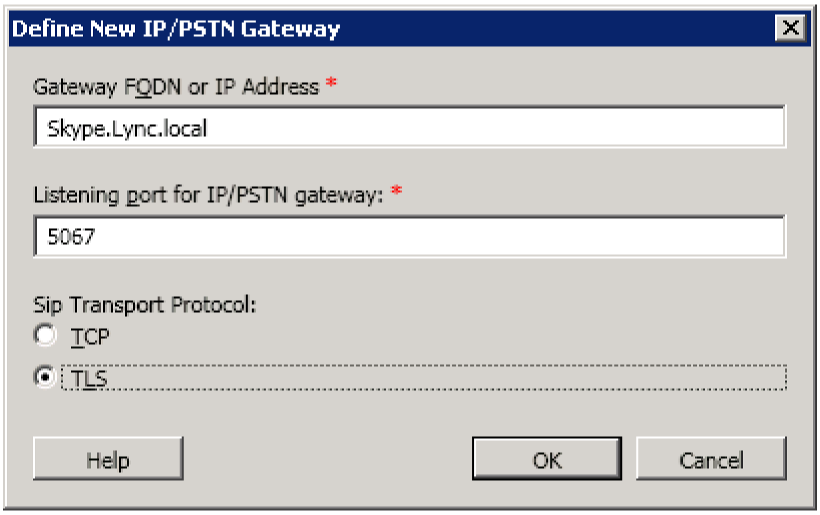


Figure 3-6: Define New IP/PSTN Gateway

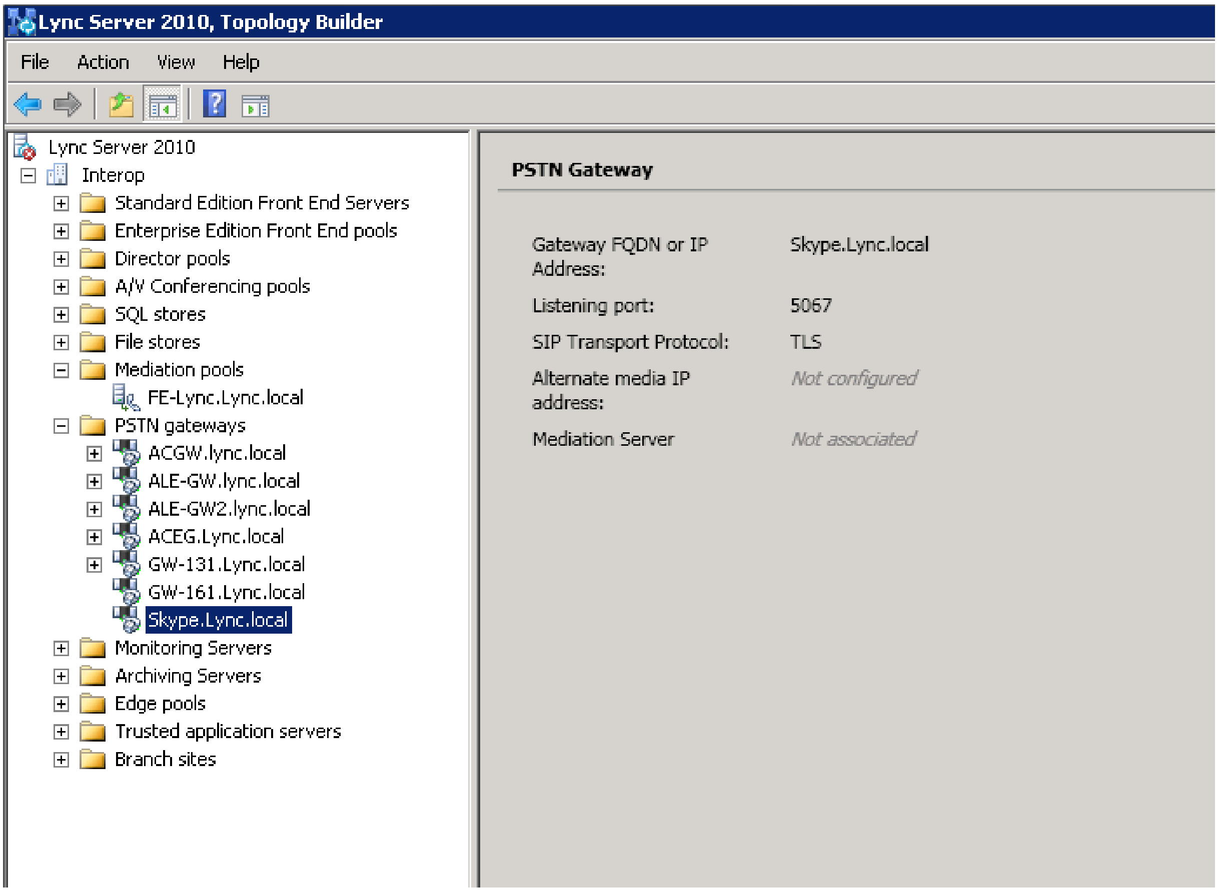


5. Enter the FQDN of the Mediant 1000 MSBG (i.e. 'Skype.lync.local') and click **OK**.

   Note that the listening port for the Gateway is '5067' and the transport type is 'TLS'.

   The Mediant 1000 MSBG is now added as a 'IP/PSTN Gateway'.

Figure 3-7: IP/PSTN Gateway



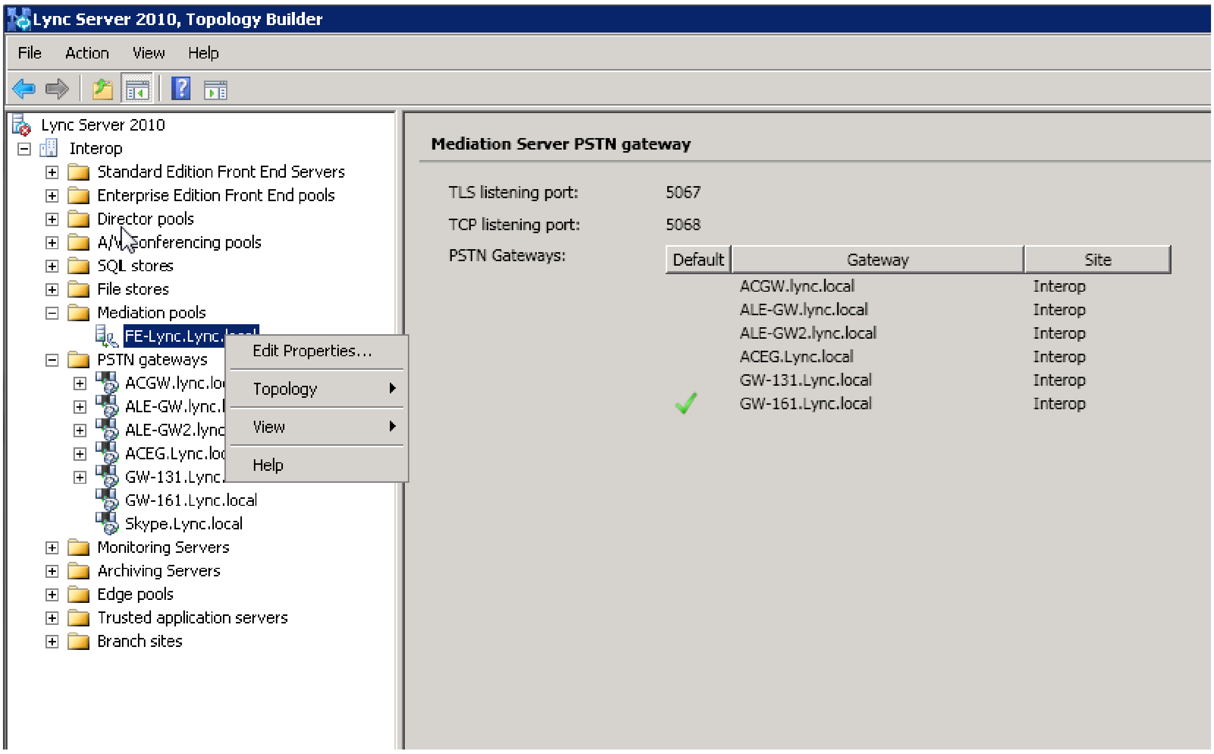
3.2 Associating the ‘IP/PSTN Gateway’ with the Mediation Server

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

➢ **To associate the IP/PSTN Gateway with the Mediation Server:**

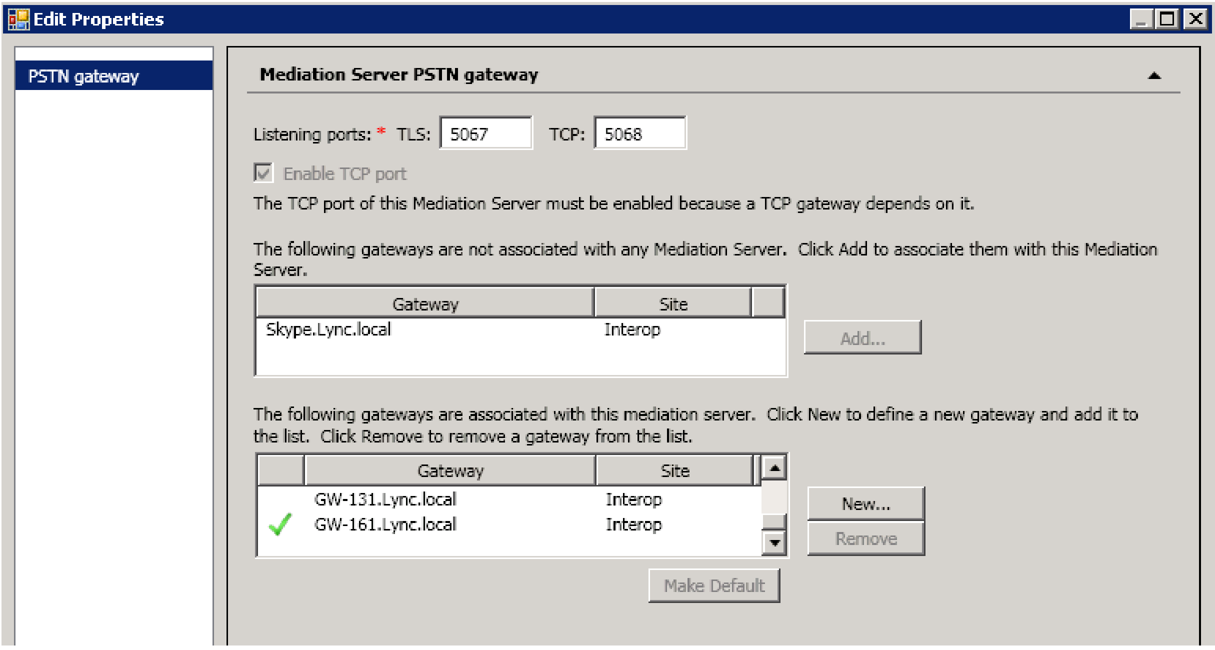
1. Right-click on the **Mediation server** to use with the Mediant 1000 MSBG (i.e. FE-Lync.Lync.local) and choose **Edit Properties**.

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



The following screen is displayed:

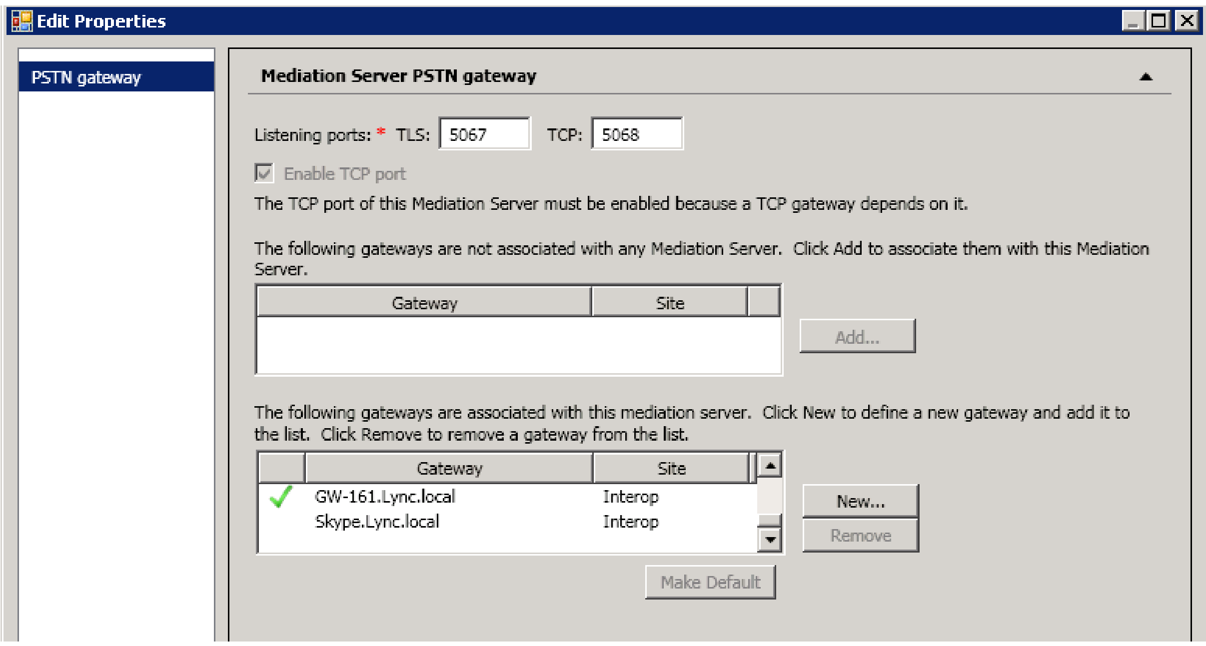
Figure 3-9:Before Associating IP/PSTN Gateway to a Mediation Server Associations



2. In the top-left corner, choose **PSTN gateway** and in the Mediation Server PSTN gateway pane, mark the Mediant 1000 MSBG gateway (i.e. 'Skype.lync.local') and click **Add** to associate it with this Mediation Server.

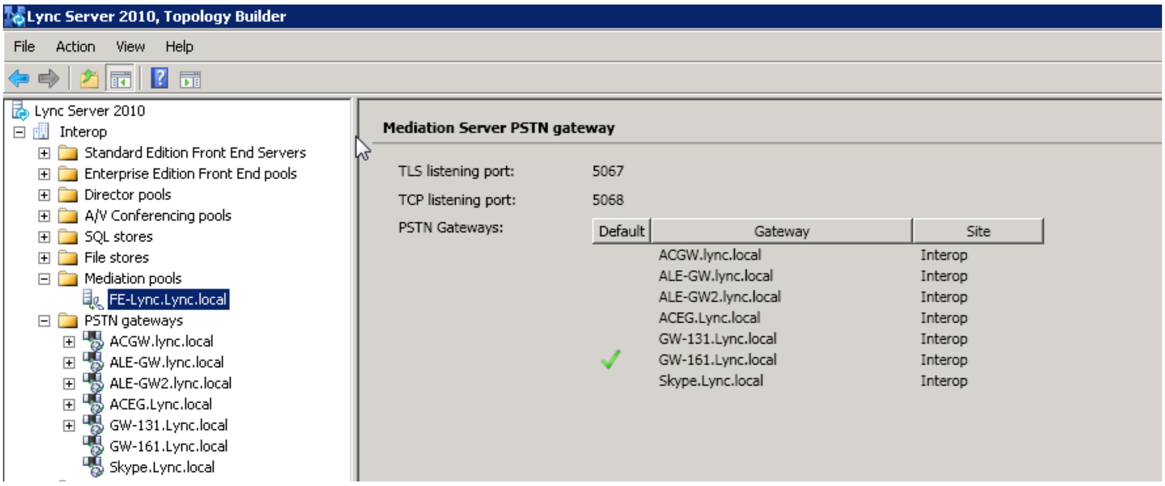
   Note that there are two sub-panes, one including a list of gateways not associated with the Mediation server and one including a list of gateways associated with the Mediation server.

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



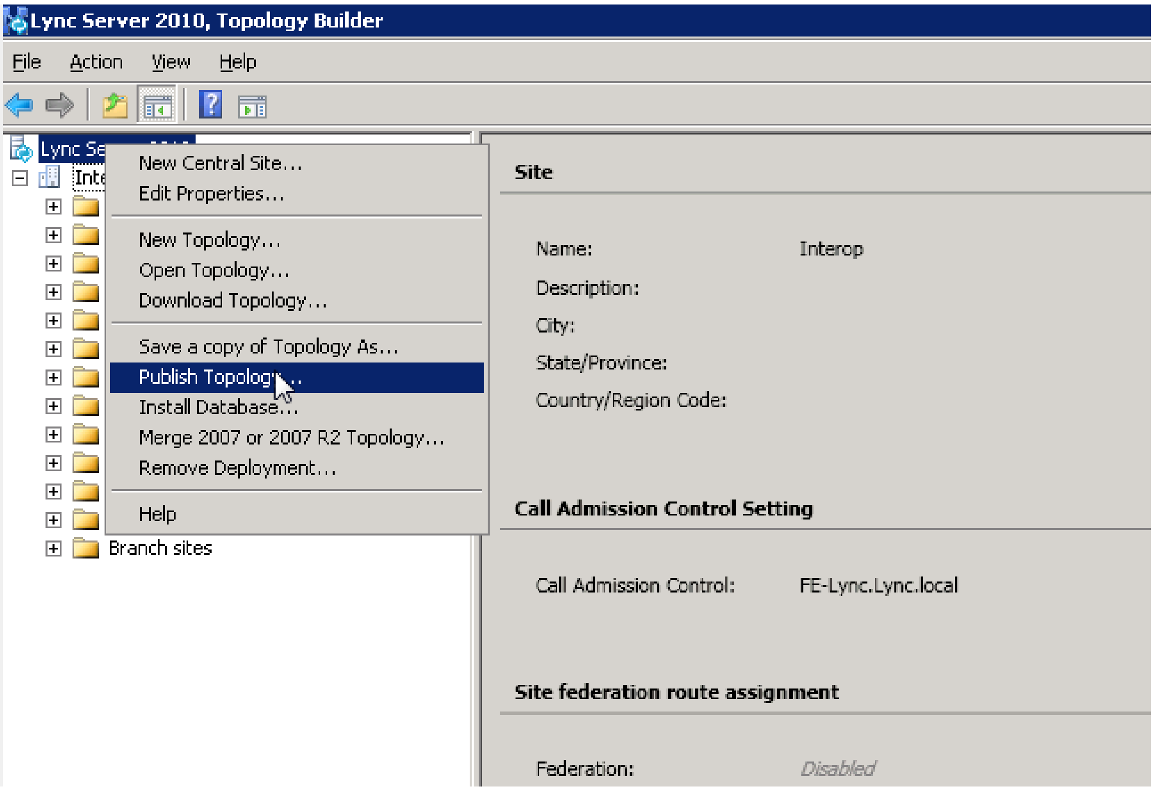
3. Click **OK**.

Figure 3-11: Media Server PSTN Gateway Association Properties



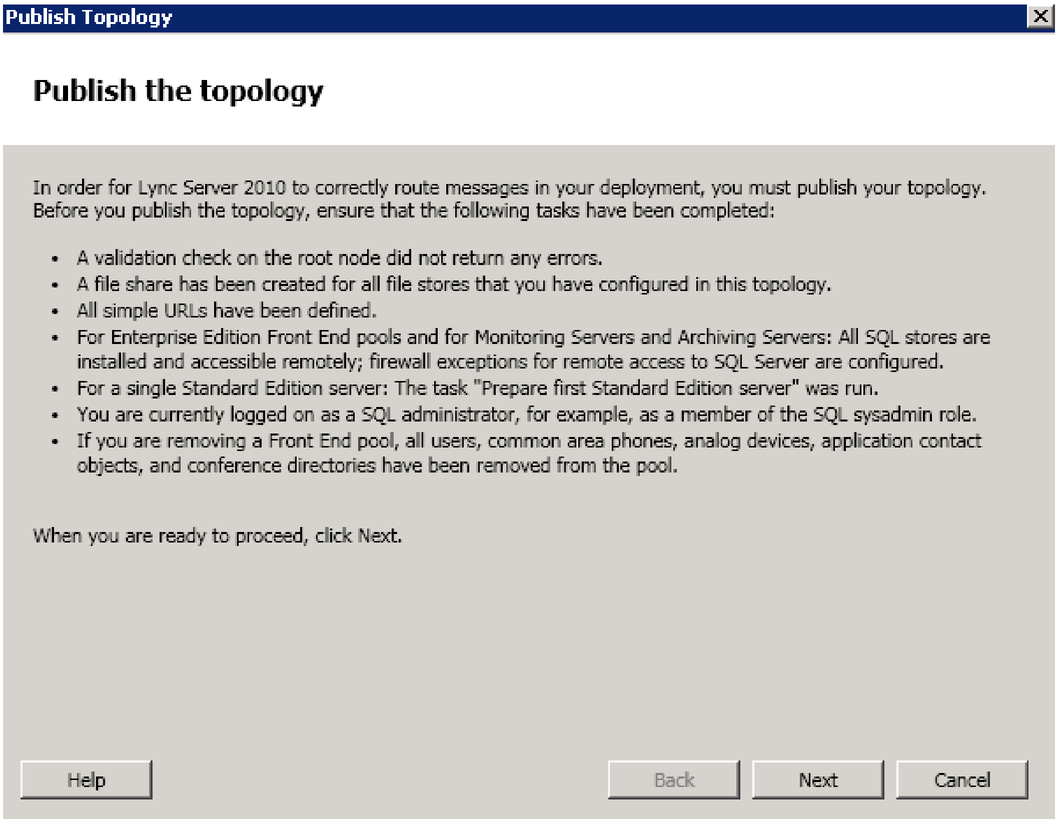
4. In the Lync Server main menu, choose **Action > Publish Topology**.

Figure 3-12: Publishing Topology



The Publish Topology screen is displayed.

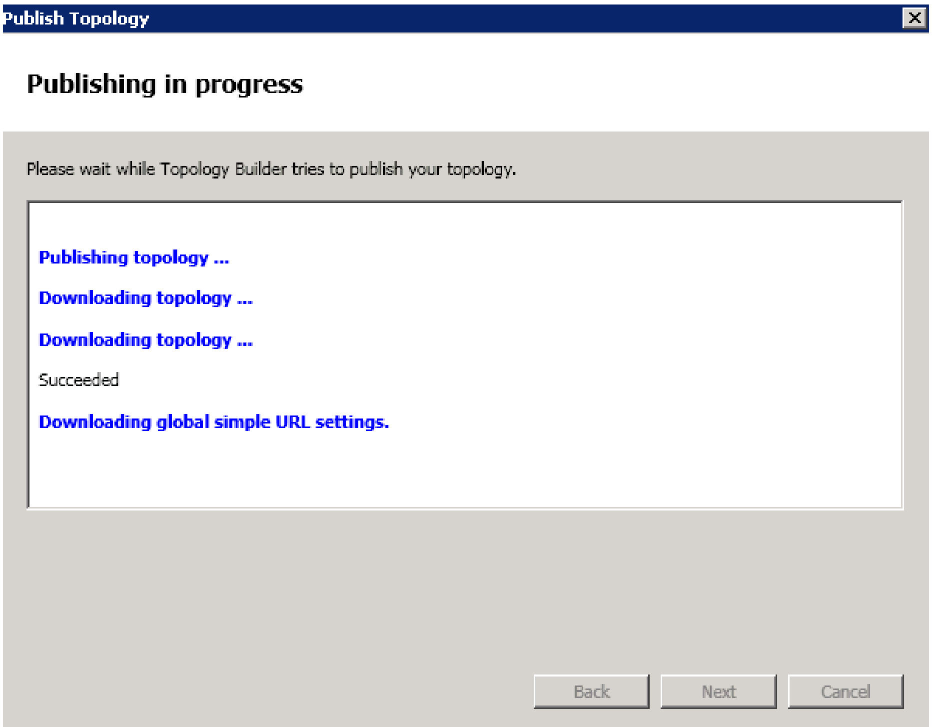
Figure 3-13:Publish Topology Confirmation



5. Click **Next**.

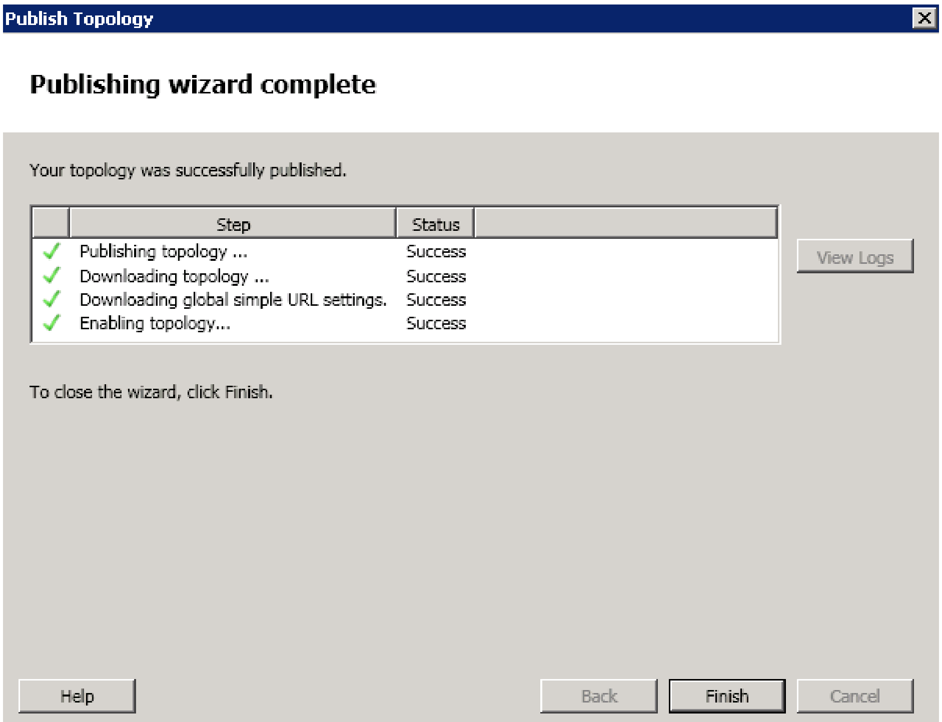
   The Topology Builder attempts to publish your topology.

Figure 3-14: Publish Topology Confirmation screen



Wait until the publish topology process has ended successfully.

Figure 3-15: Publish Topology Successfully Completed



6. Click **Finish**.

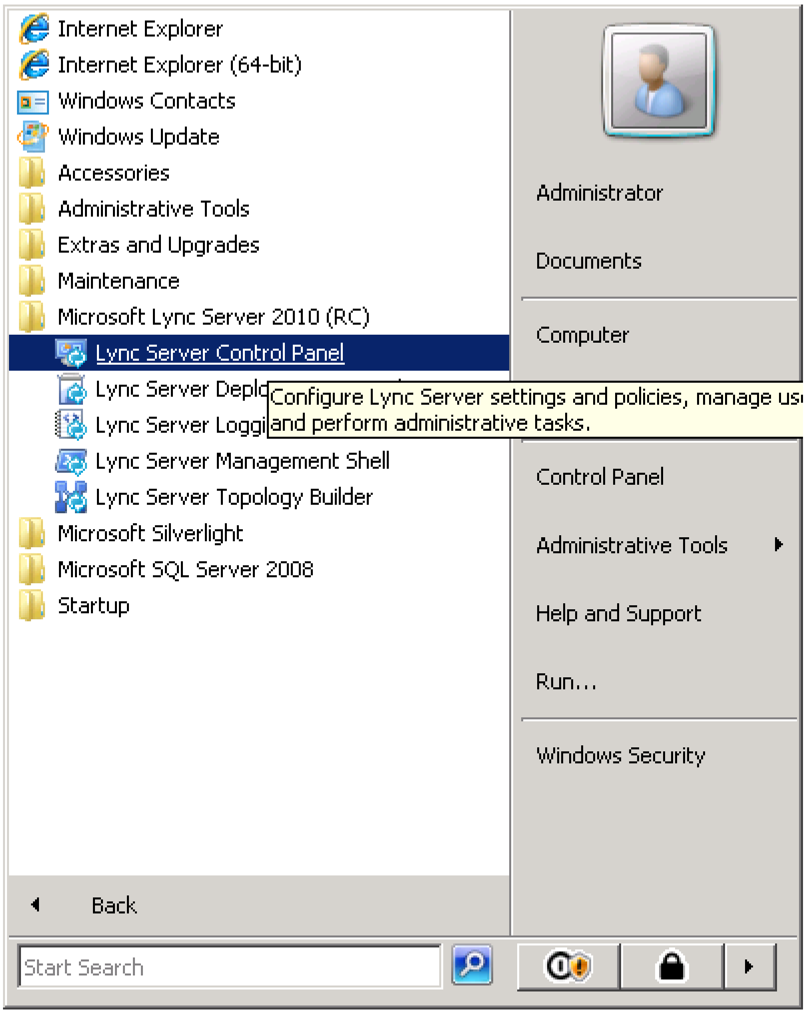
3.3 Configuring the 'Route' on the Lync Server 2010

This section describes how to configure a 'Route' on the Lync server and associate it with the Mediant 1000 MSBG PSTN gateway.

➢ **To configure the 'route' on the Lync server:**

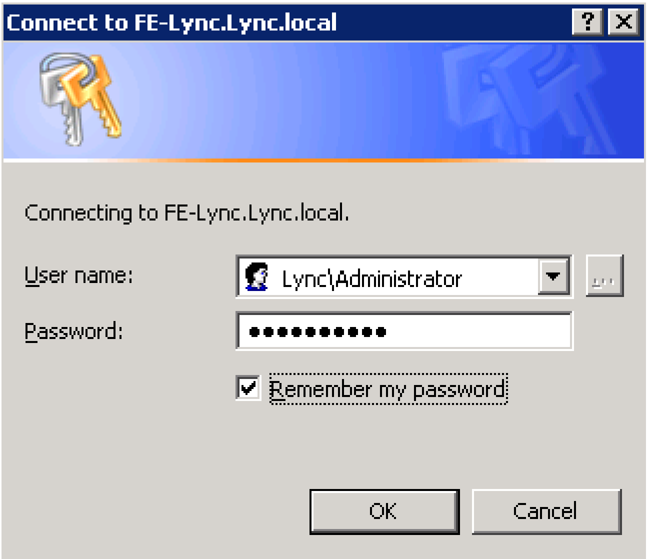
1. Open the Communication Server Control Panel (CSCP), click **Start**, select **All Programs**, and select **Lync Server Control Panel**.

Figure 3-16: Lync Server Control Panel



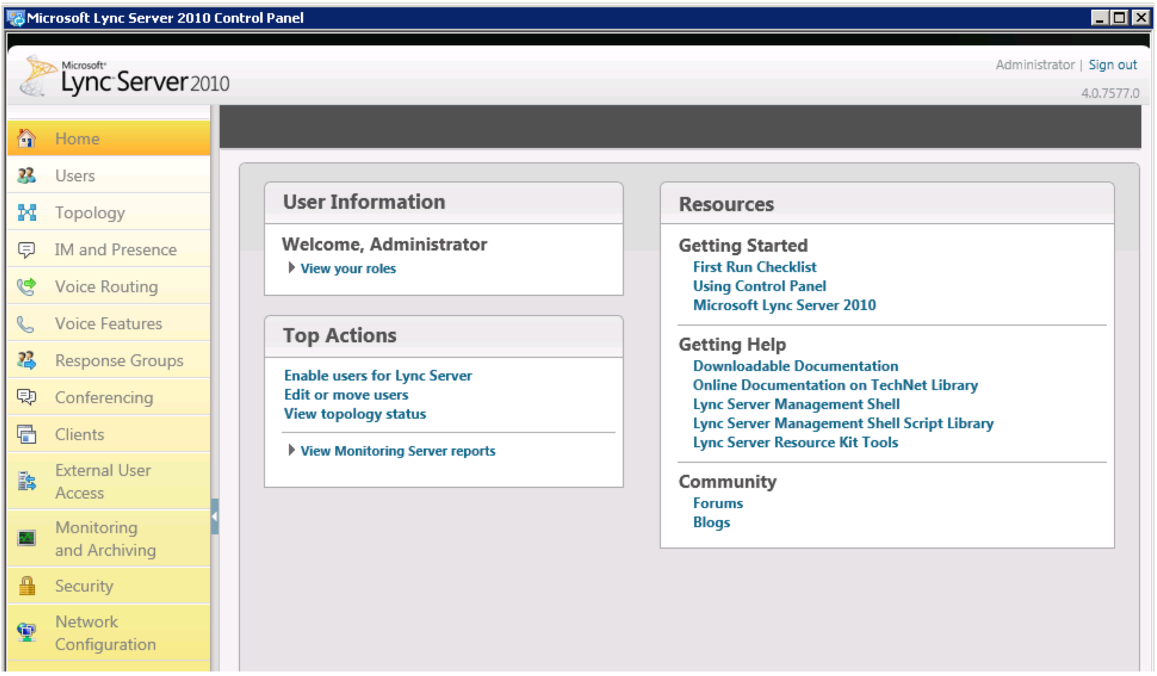
2. You are prompted for credentials; enter your domain username and password.

Figure 3-17: Lync Server Credentials



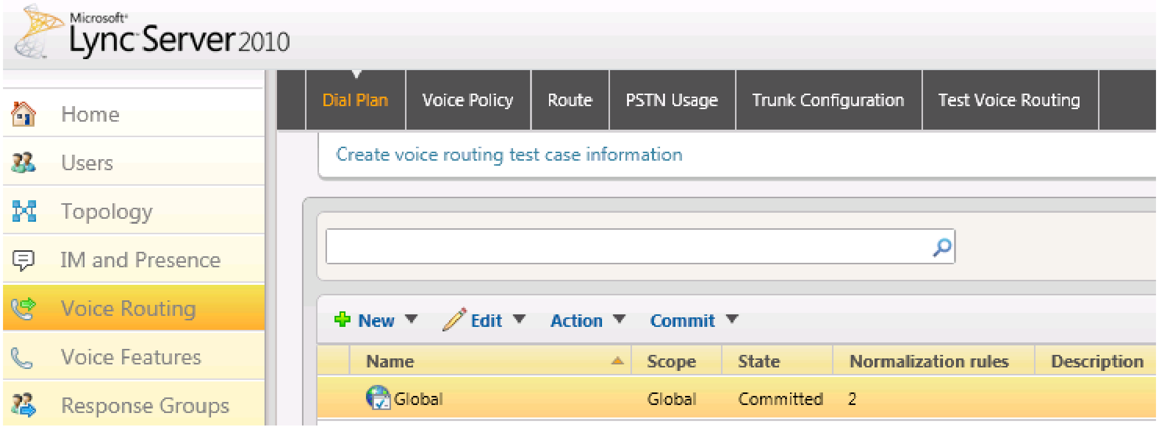
The CSCP Home page is displayed.

Figure 3-18: CSCP Home page



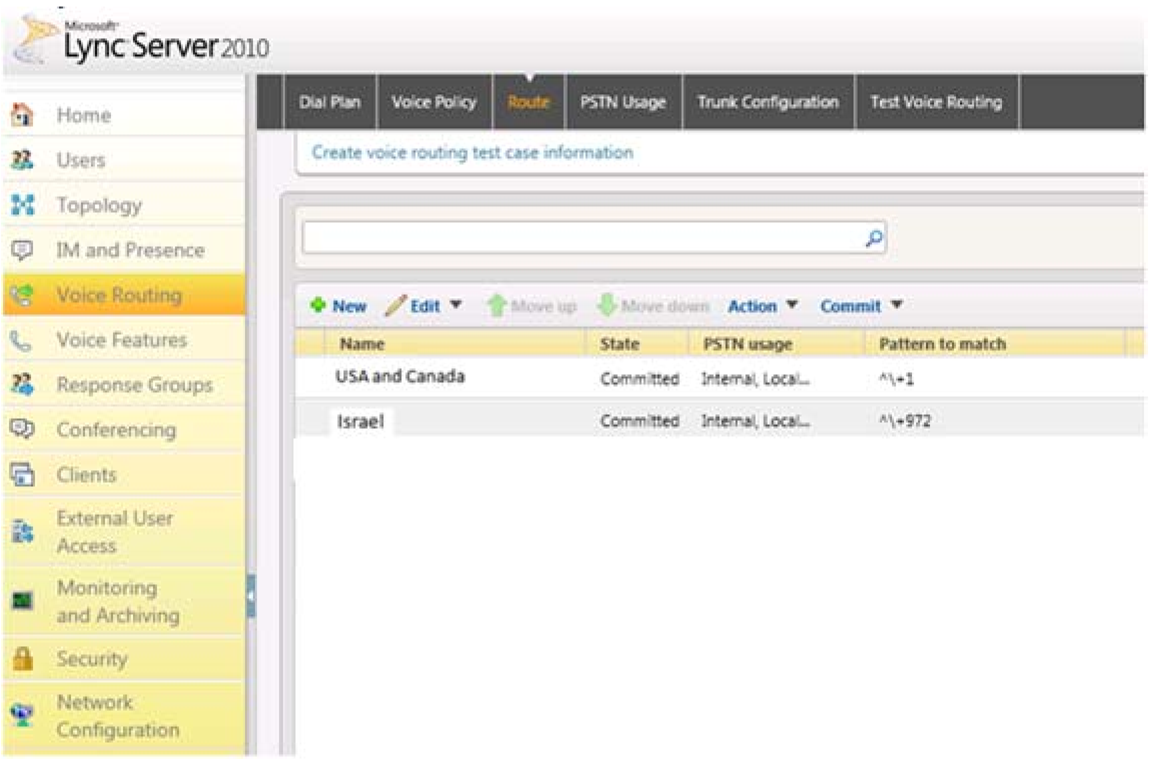
3. In the Navigation pane, select the **'Voice Routing'** option.

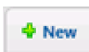
Figure 3-19: Voice Routing Option



4. In the Voice Routing menu at the top of the page, select the **Route** option.

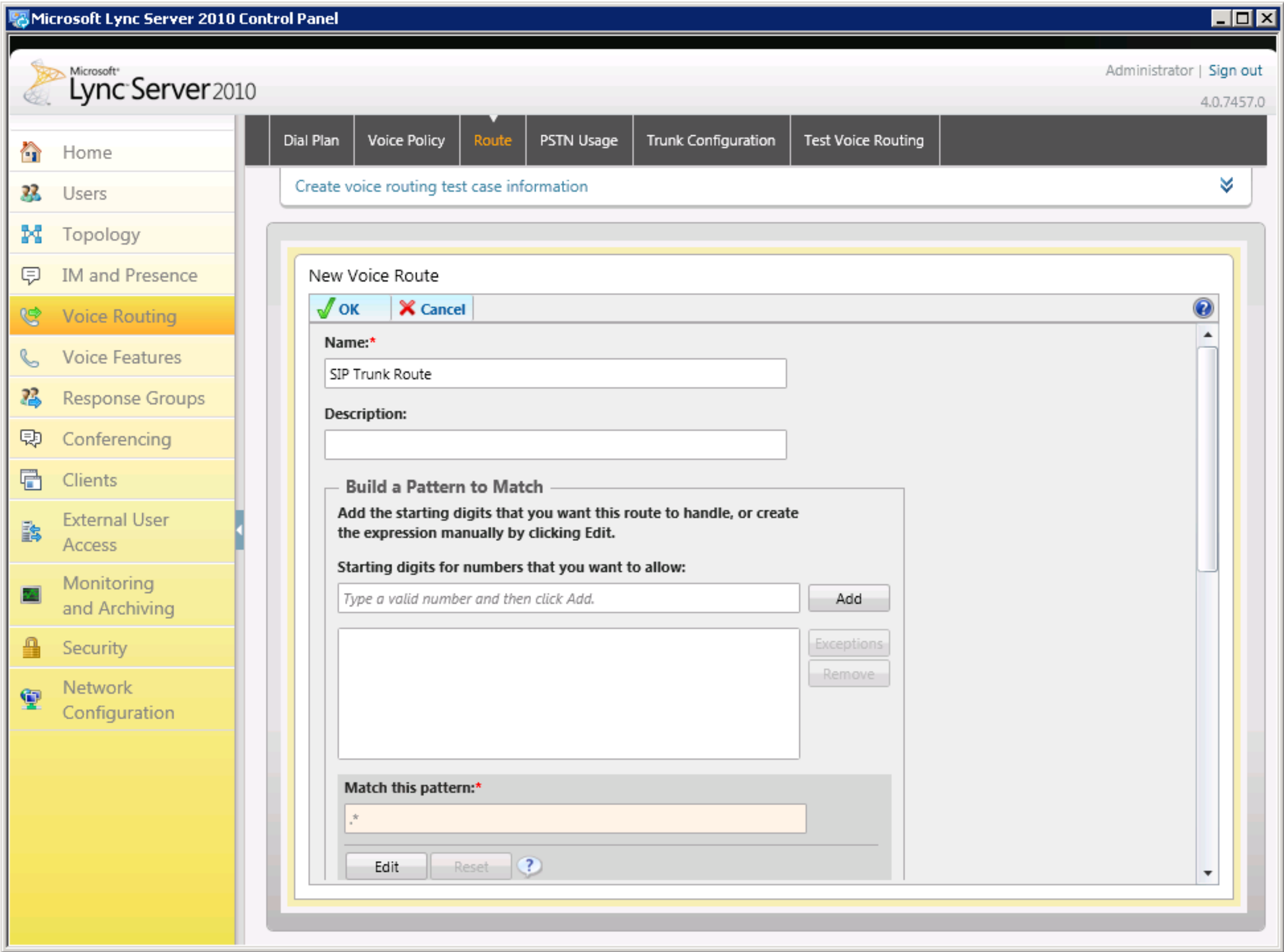
Figure 3-20: Route Option



5. In the content area toolbar, click  .

6. In the Build a Pattern to Match pane, fill in a Name for this route (i.e. SIP Trunk Route) and a Pattern to Match for the phone numbers you wish this route to handle. In this example, the pattern to match is ‘*’, which means “to match all numbers”.
7. Click **Add**.

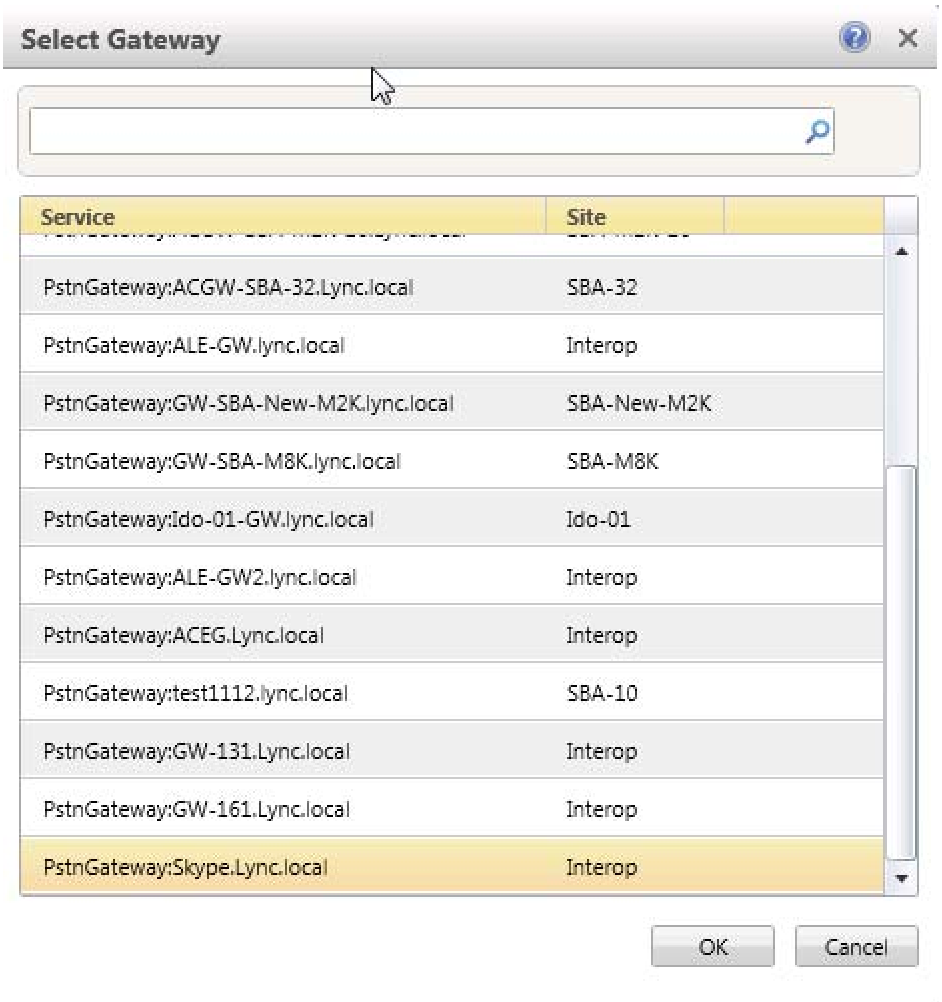
Figure 3-21: Adding New Voice Route



8. Associate the route with the Mediant 1000 MSBG IP/PSTN gateway you created above; scroll down to the Associated Gateways pane and click **Add**.

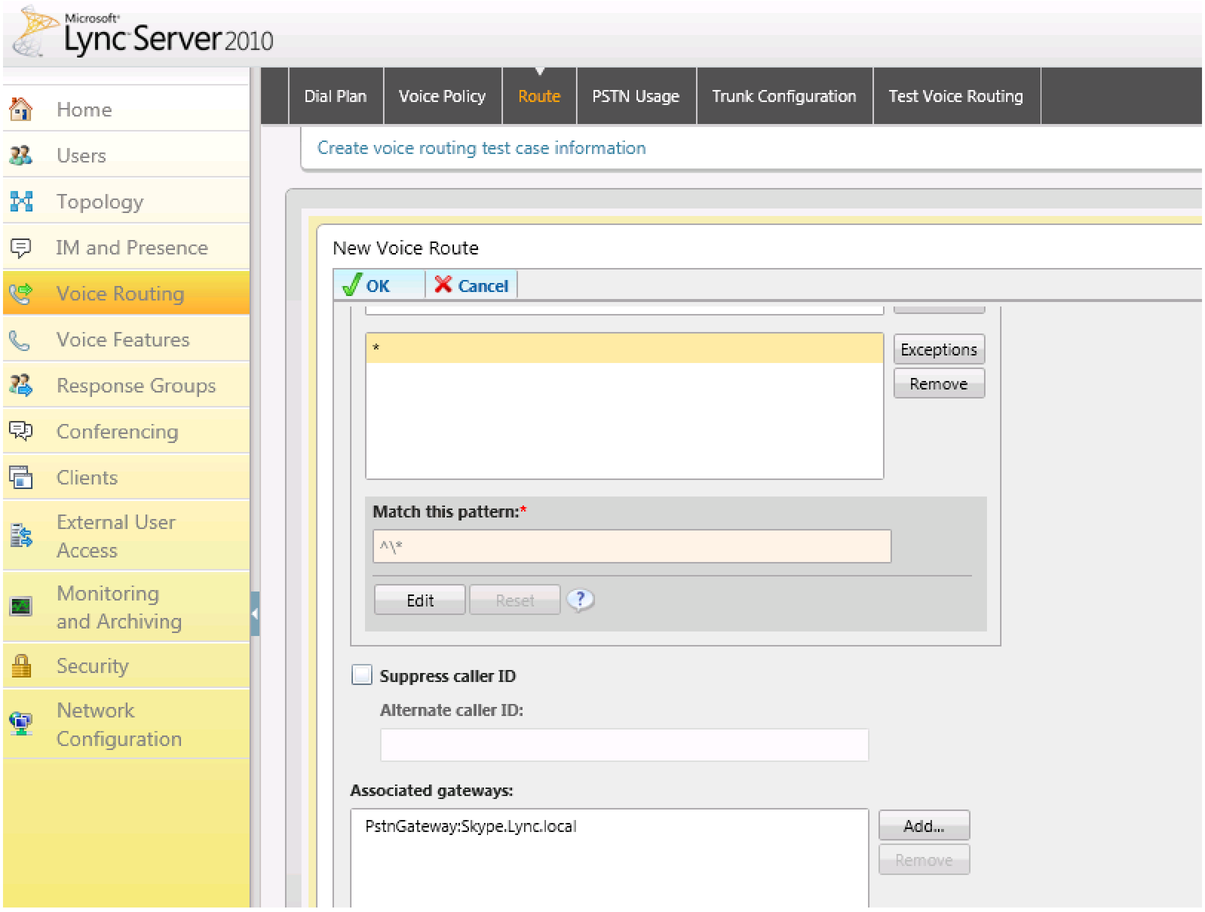
   A list of all the deployed Gateways is displayed.

Figure 3-22: List of Deployed Gateways



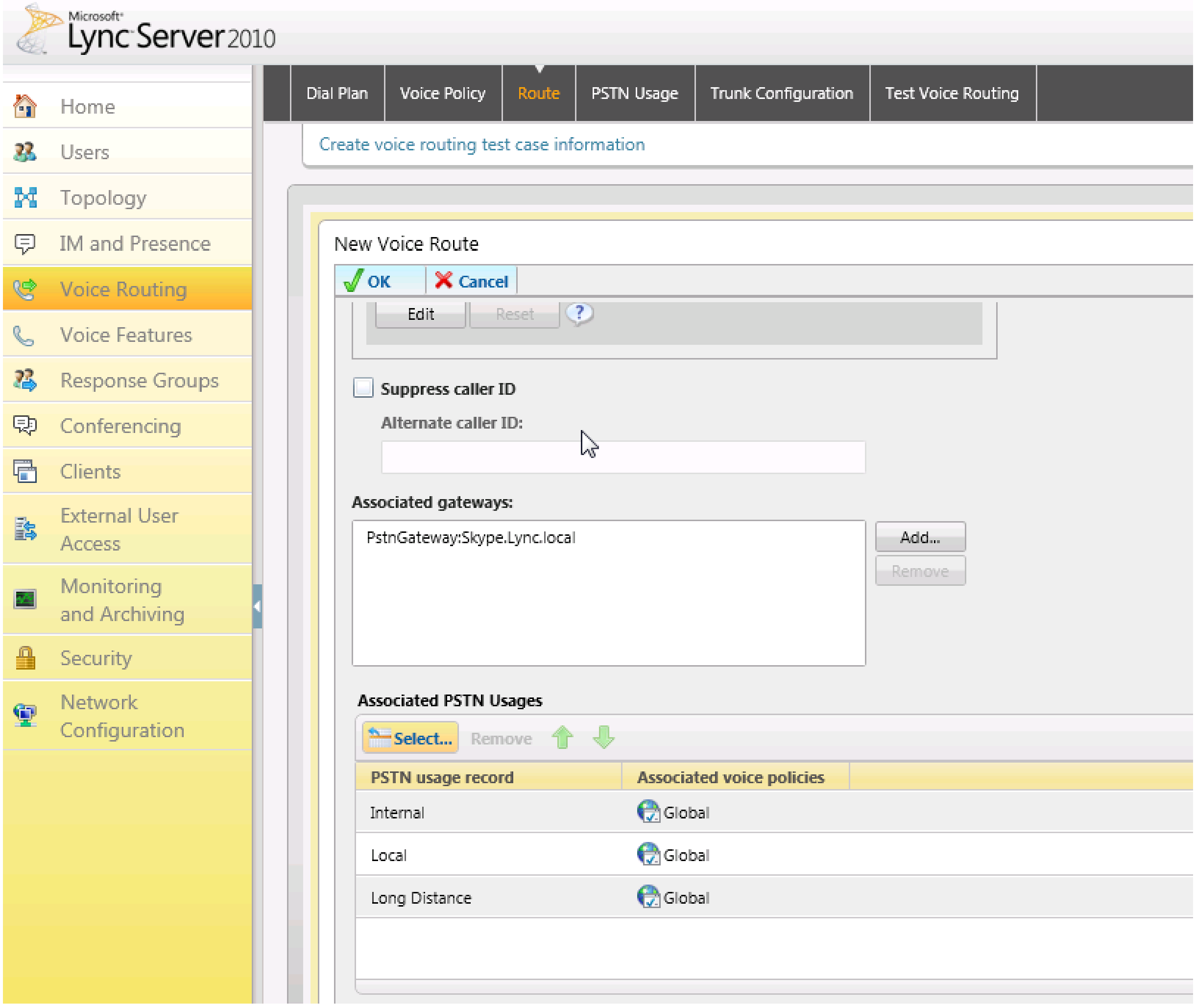
9. Select the Mediant 1000 MSBG Gateway you created above and click **OK**.

Figure 3-23: Selecting the Mediant 1000 MSBG Gateway



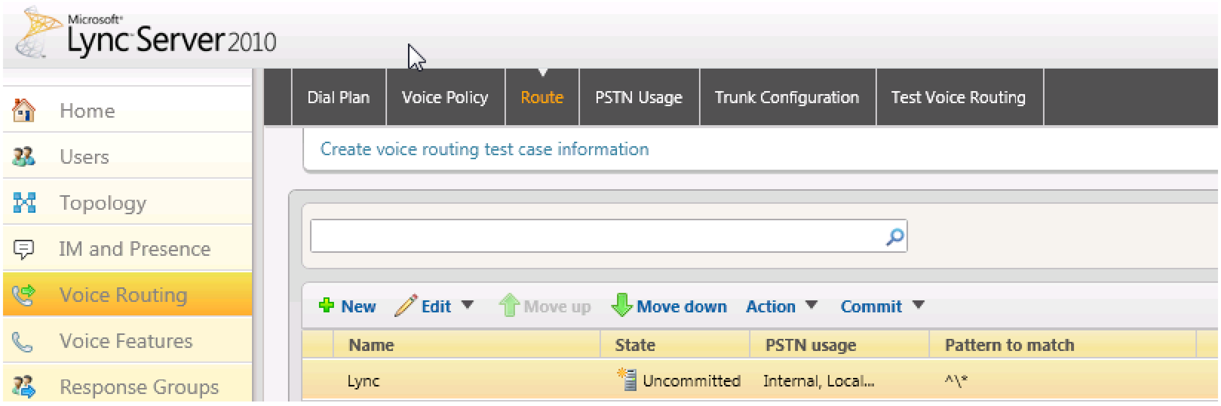
10. Associate a PSTN Usage to this route. In the **Associated PSTN Usages** toolbar, click **Select** and add the associated PSTN Usage.

Figure 3-24: Associating PSTN Usage to Mediant 1000 MSBG Gateway



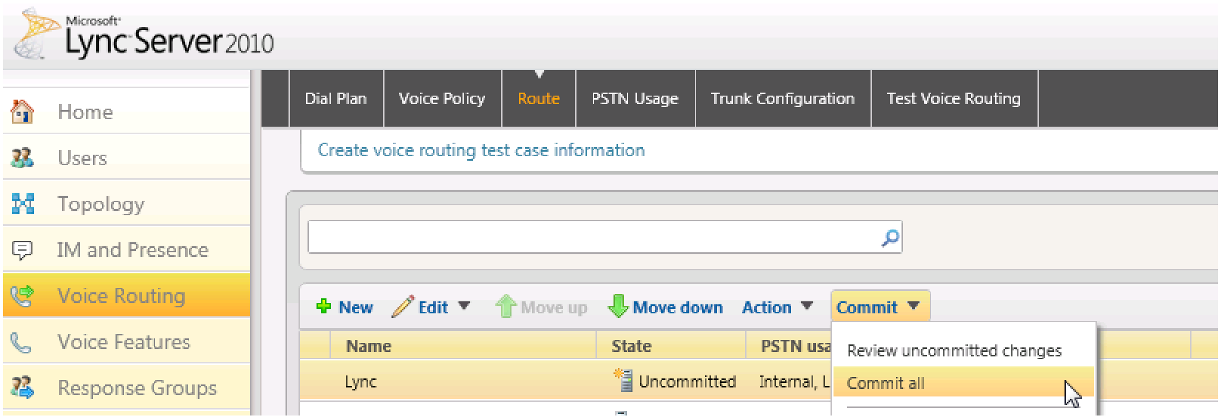
11. Click the **OK** button in the toolbar at the top of the New Voice Route pane.

Figure 3-25: Confirmation of New Voice Route



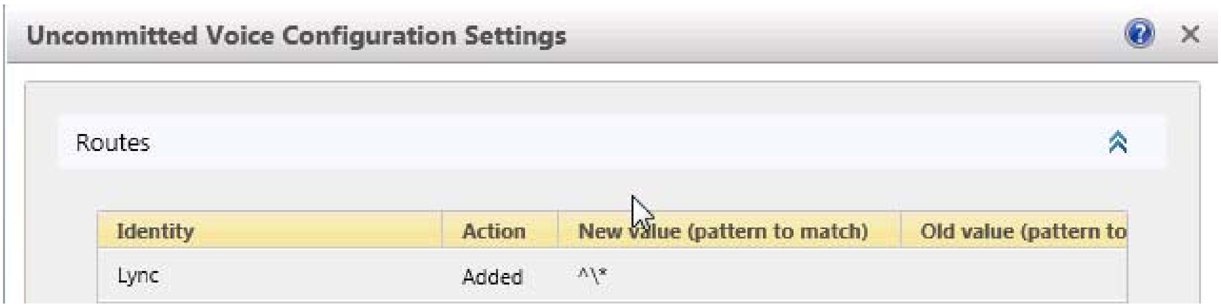
12. In the Content area Toolbar, click on the arrow adjacent to the **Commit** button; a drop-down menu is displayed; select the 'Commit All' option.

Figure 3-26: Committing Voice Routes



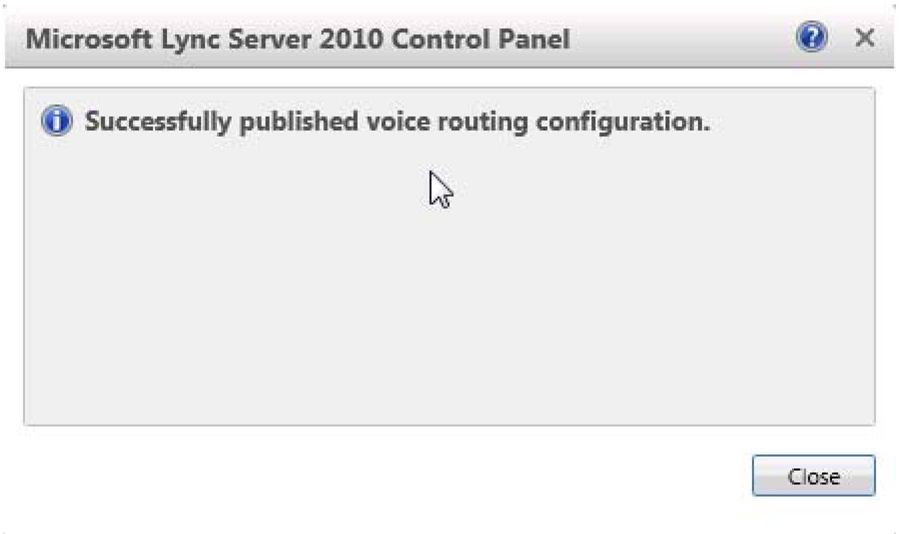
13. In the Uncommitted Voice Configuration Settings window, click **Commit**.

Figure 3-27: Uncommitted Voice Configuration Settings



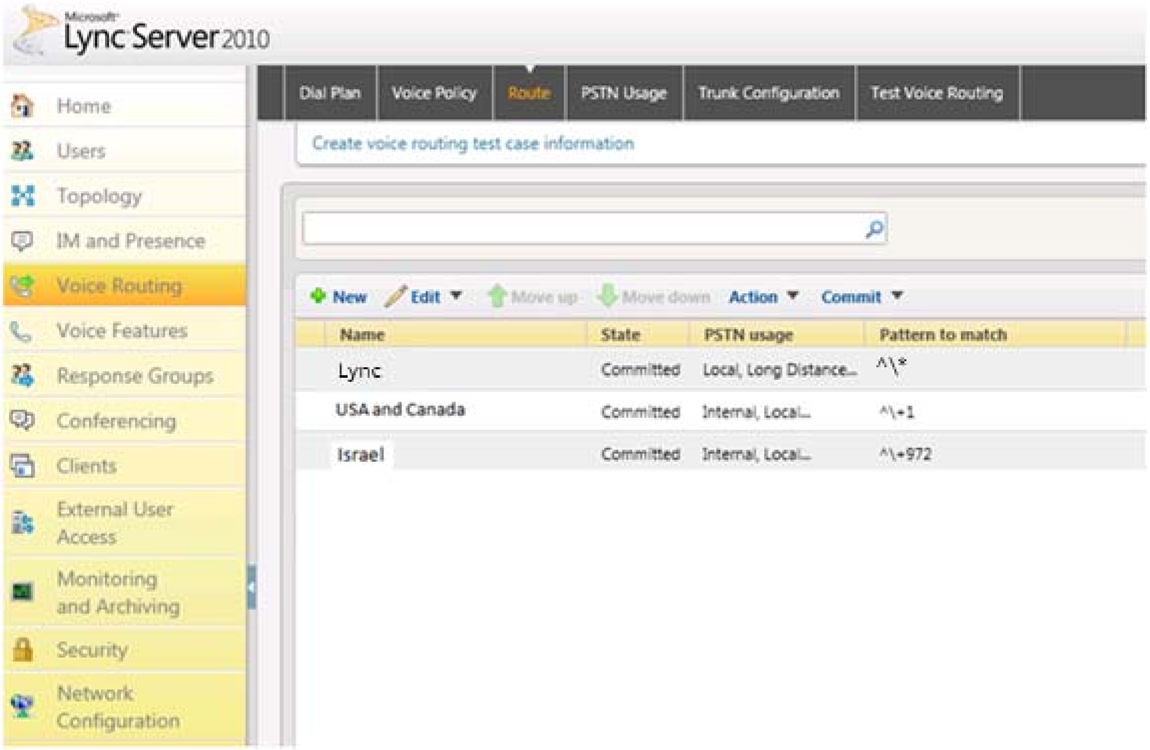
14. A message is displayed, confirming a successful voice routing configuration; in the **Microsoft Lync Server 2010 Control Panel** prompt, click **Close**.

Figure 3-28: Voice Routing Configuration Confirmation



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

Figure 3-29: Voice Routing Screen Displaying Committed Routes



Reader's Notes

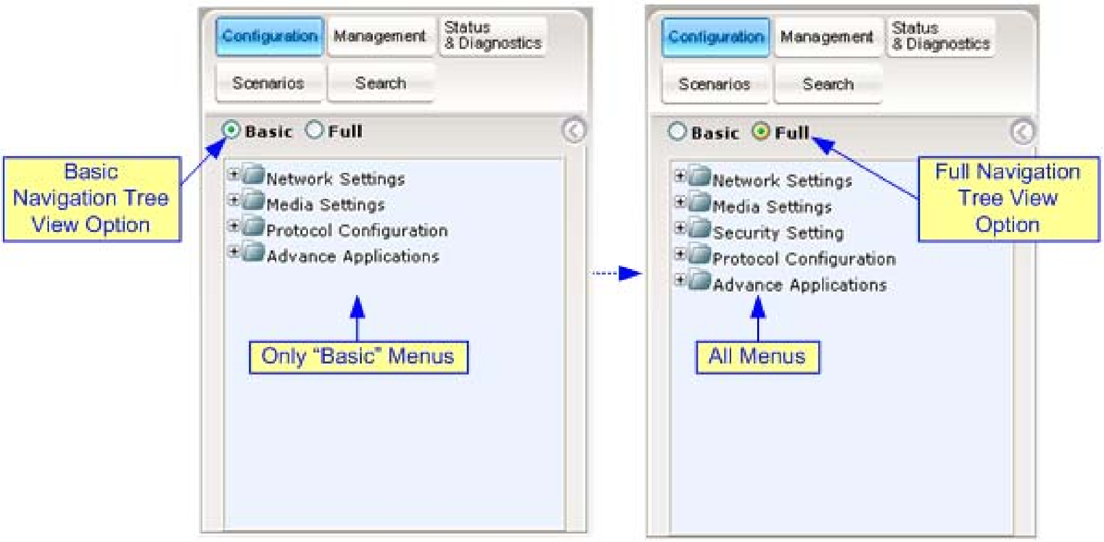
4 Configuring Mediant 1000 MSBG Device

This section describes the following steps for configuring the Mediant 1000 MSBG device in the Skype SIP Trunking environment:

- **Step 1**: Configure IP Addresses. See Section 4.1 on page 39.
- **Step 2**: Configure Data Firewall Settings. See Section 4.2 on page 42.
- **Step 3**: Configure Enable SIP SBC Applications. See Section 4.3 on page 43.
- **Step 4**: Configure Secure Real-Time Transport Protocol (SRTP). See Section 4.4 on page 44.
- **Step 5**: Configure IP Media. See Section 4.5 on page 46.
- **Step 6:** Configure SIP General Parameters. See Section 4.6 on page 47.
- **Step 7**: DTMF and Dialing. See Section 4.7 on page 50.
- **Step 8**: Configure Coders. See Section 4.8 on page 51.
- **Step 9**: Configure Proxy and Registration. See Section 4.9 on page 52.
- **Step 10**: Configure Account table. See Section 4.10 on page 53.
- **Step 11**: Configure Proxy Sets Tables. See Section 4.11 on page 54.
- **Step 12**: Configure Coder Group. See Section 4.12 on page 56.
- **Step 13**: Configure IP Profile. See Section 4.13 on page 58.
- **Step 14**: Configure IP Group Tables. See Section 4.14 on page 60.
- **Step 15**: Configure Routing Rules. See Section 4.15 on page 62.
- **Step 16**: Configure Manipulation Rules. See Section 4.16 on page 64.
- **Step 17:** Configure Secure Calls. See Section 4.17 on page 67.
- **Step 18**: Configure Alternative Routing Reasons. See Section 4.18 on page 69.
- **Step 19:** Define SIP TLS Connection. See Section 4.19 on page 70.
- **Step 19-1**: Configure VoIP DNS Settings. See Section 4.19.1 on page 70.
- **Step 19-2**: Configure NTP Server. See Section 4.19.2 on page 70.
- **Step 19-3**: Configure Certificates. See Section 4.19.3 on page 71.
- **Step 20**: Reset the Gateway. See Section 4.20 on page 77.

The procedures described in this section are performed using the Mediant 1000 MSBG devices' Web-based management tool (i.e., embedded Web server). Before you begin configuring the Mediant 1000 MSBG 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: Configure IP Addresses

This step describes how to configure LAN IP addresses when the internal data-routing capabilities of the Mediant 1000 MSBG device are used in order to connect to the Skype SIP Trunk. In this case, you must configure a separate WAN interface as described in this step.

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.

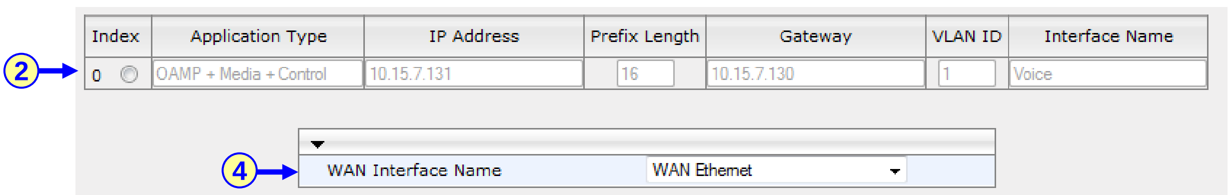
4.1.1 Configuring LAN IP Addresses

This step describes how to configure the LAN addresses.

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

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

Figure 4-2: IP Settings



2. Select the 'Index' radio button corresponding to the Application Type "**OAMP + Media + Control** (i.e., VoIP and management interface), 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).
4. Set the **WAN Interface Name: "**WAN Ethernet". This is the WAN interface (configured in Section 0 on page 41) on which your VoIP traffic interfaces with the public network.

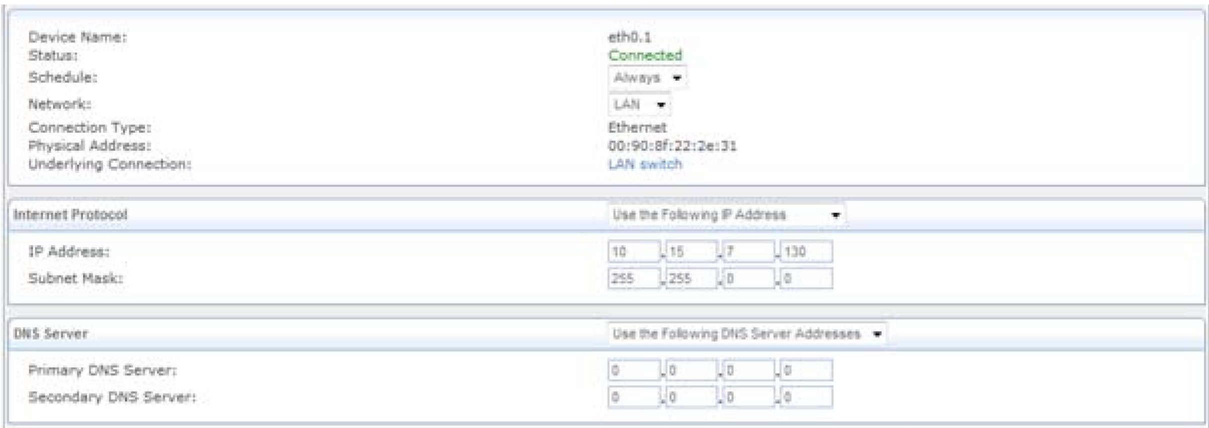
➢ To define the Mediant 1000 MSBG device's LAN data-routing IP address:

1. Access the Mediant 1000 MSBG device's Web interface with the IP address that you assigned to the VoIP and Management interface.
2. Access the 'Connections' page (**Configuration** tab > **Data** menu > **Data System** > **Connections**).

Figure 4-3: Connections Page

3. Click the **Edit** icon corresponding to the "LAN Switch VLAN 1" connection, and then click the **Settings** tab.
4. 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



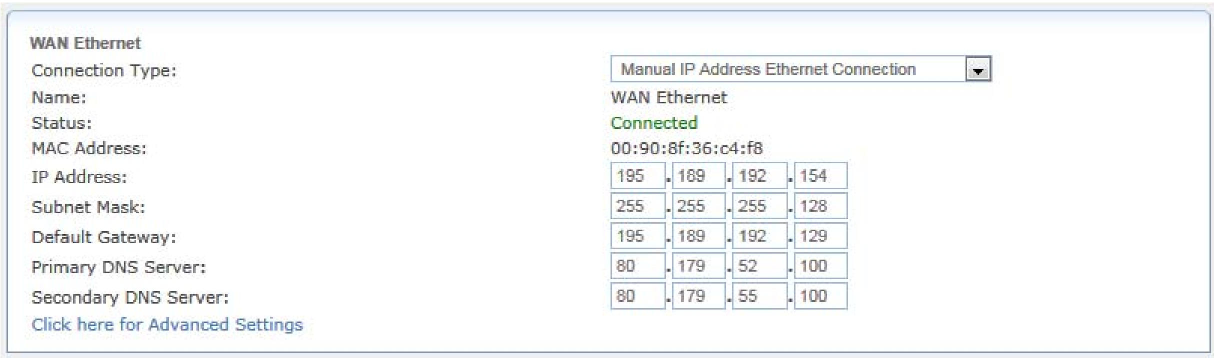
4.1.2 Configure WAN IP Addresses

This step describes how to configure the Mediant 1000 MSBG device firewall IP address used to connect to the WAN.

➢ To configure the WAN IP address:

1. Cable the Mediant 1000 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



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).

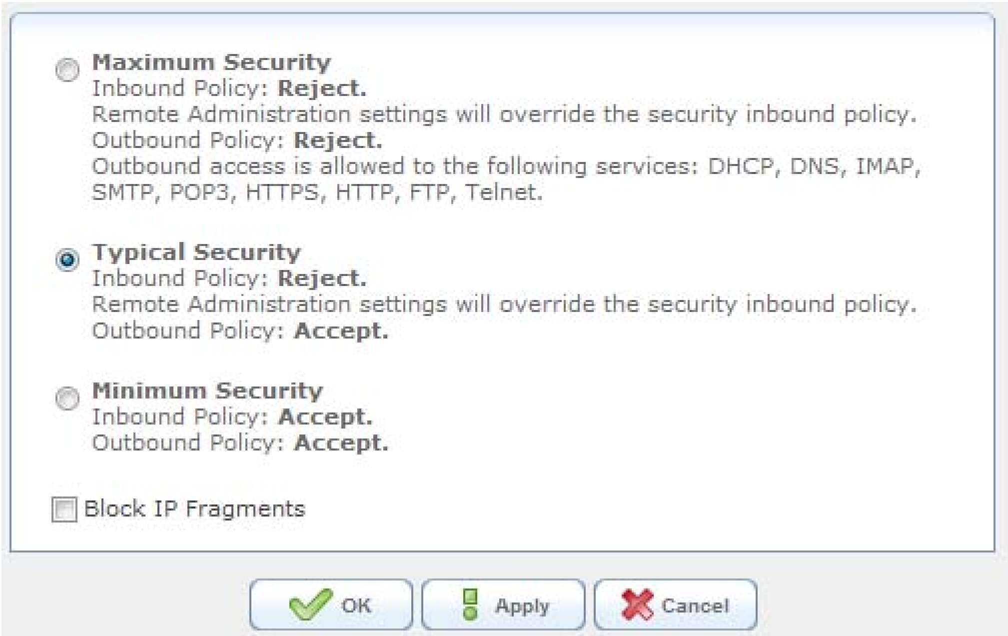
4.2 Step 2: Configure Data Firewall

This step describes how to configure the data firewall settings for the Mediant 1000 MSBG device's WAN interface. You must define firewall rules for the WAN interface to prevent unwanted access from the public network. The configuration shown below represents a typical WAN firewall implementation.

➢ **To configure data firewall settings:**

1. Open the 'General Security' page (**Configuration** tab > **Data** menu > **Firewall and ACL** > **General Security**).

Figure 4-6: General Security



2. Select 'Typical Security'.

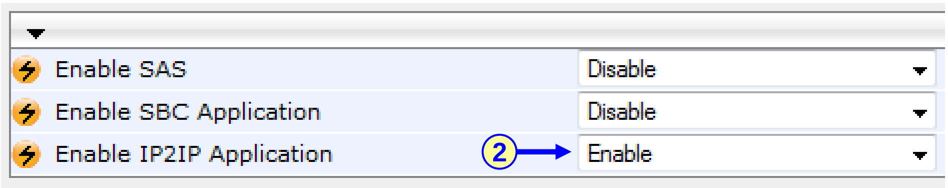
4.3 Step 3: Enable SIP SBC Application Mode

This step describes how to enable the SIP SBC application mode.

➢ **To enable the IP2IP application mode:**

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

Figure 4-7: Applications Enabling



2. Enable **IP2IP Application**.

Note:

1. To enable the SBC and IP2IP capabilities on the AudioCodes gateway, your gateway must be loaded with the feature key that includes the **IP2IP** feature.
2. The Mediant 1000 MSBG device must be running SIP version 6.2 or later.
3. Reset with BURN to FLASH is required.

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

If you configure TLS for the SIP transport link between the Mediant 1000 MSBG and the Mediation Server, you must specify Secure RTP (SRTP) encryption with one of the following options:

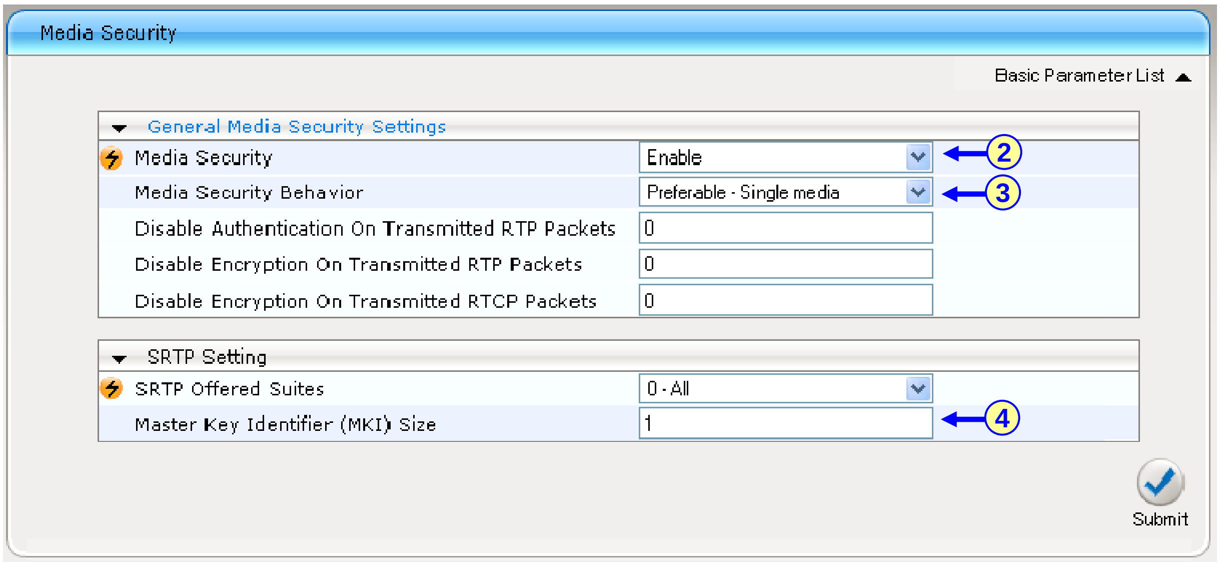
- **Required:** SRTP should be attempted, but do not use encryption if negotiation for SRTP is unsuccessful.
- **Optional:** Attempt to negotiate the use of SRTP to secure media packets. Use RTP if SRTP cannot be negotiated.
- **Not used:** Send media packets using RTP.

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 4-8: Media Security Page



2. Set the **Media Security** to ‘Enable’.
3. Set the **Media Security Behavior**:
   - “Mandatory” if Mediation Server is configured to SRTP Required
   - ”Preferable-Single media” if Mediation Server is configured to SRTP Optional.
4. Set the **Master Key Identifier (MKI) Size** to ‘1’.
5. Click **Submit**.
6. Save (burn) the Mediant 1000 MSBG configuration and reset the Gateway.

Note: 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 52).

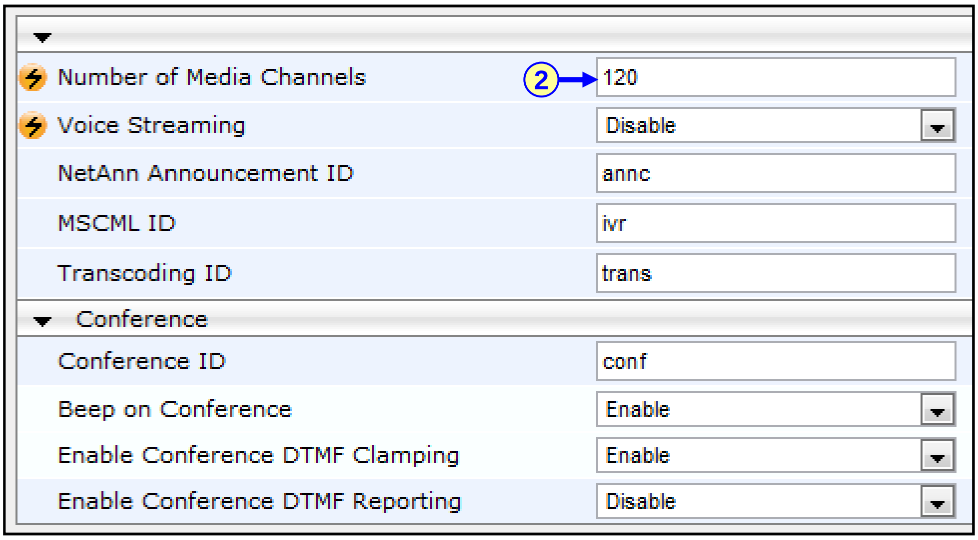
4.5 Step 5: Configure IP Media

This step describes how to configure the number of media channels for the IP media. 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 4-9: IP Media Settings



2. Set **Number of Media Channels** to ‘120’.

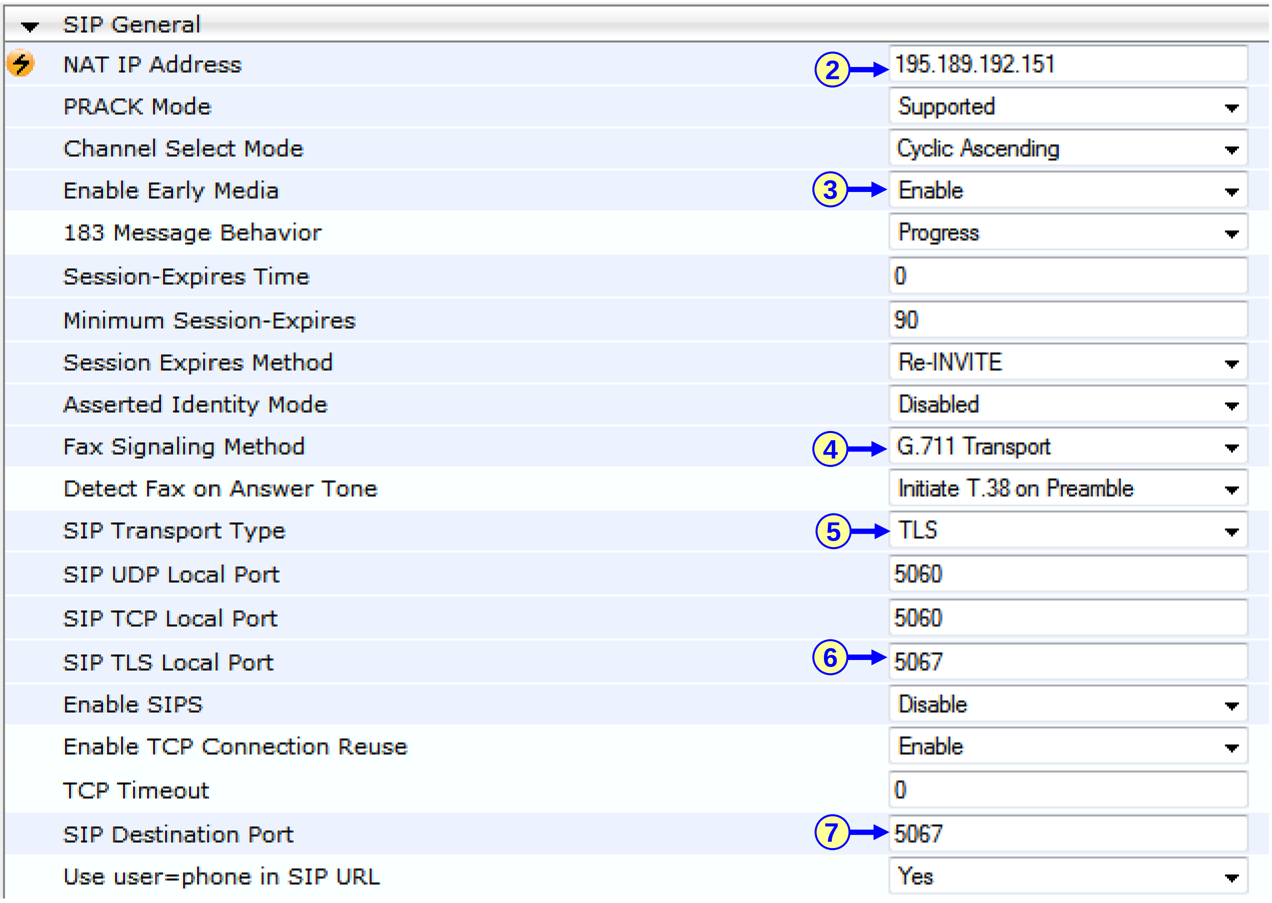
4.6 Step 6: Configure SIP General Parameters

This step describes how to enable SIP General parameters.

➢ To configure SIP General Parameters:

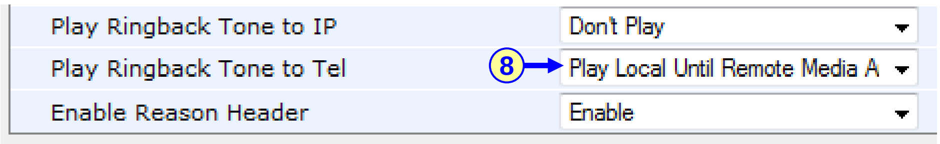
1. Open the 'Applications Enabling' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

Figure 4-10: General Parameters



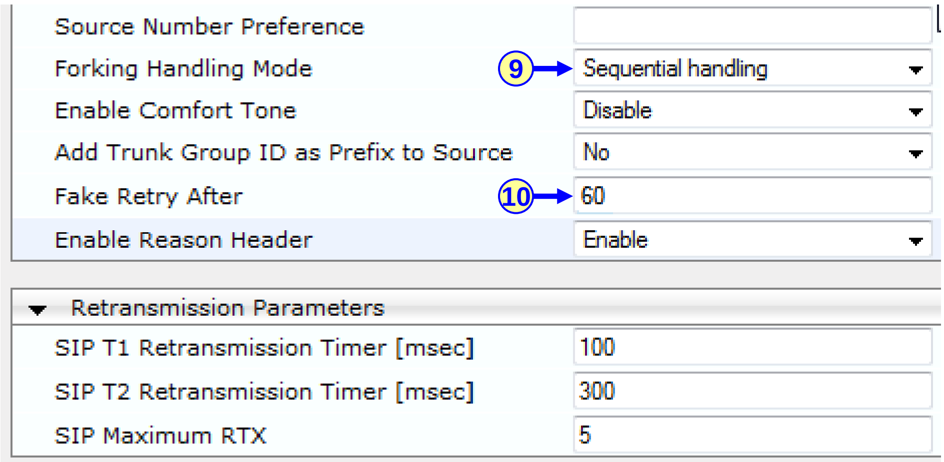
2. Set '**NAT IP Address'**,with the Global (public) IP address of the Mediant 1000 MSBG device.
3. Set **Enable Early Media** to 'Enable'.
4. Set **Fax Signaling Method** to 'G.711 Transport'.
5. Set **SIP Transport Type** to 'TLS'.
6. Set **SIP TLS Local Port** to '5067' (Lync server port)
7. Set **SIP Destination Port** to '5067' (Lync Server port)

Figure 4-11: General Parameters (Cont.)



8. Set **Play Ringback Tone to Tel** to 'Play Local Until Remote Media Arriving'.

Figure 4-10: General Parameters (Cont.)

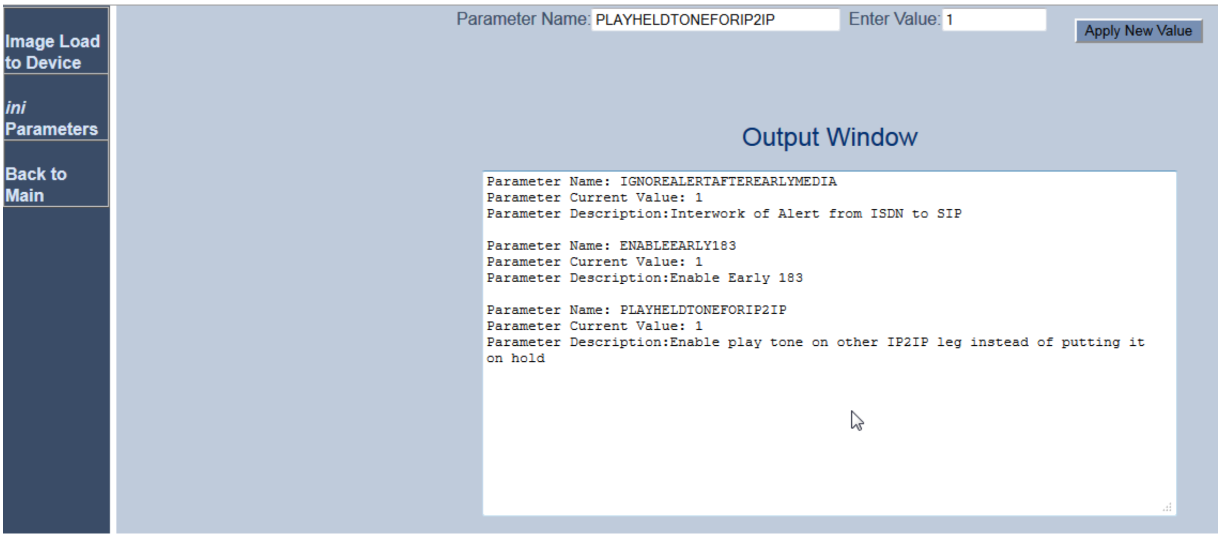


9. Set **Forking Handling Mode** to 'Sequential handling'.
10. Set **Fake Retry After'** to '60'.
11. Open the 'Admin" page, by appending the case-sensitive suffix 'AdminPage' to the Media Gateway's IP address in your Web browser's URL field (e.g., http://10.15.7.131/AdminPage).
12. On the left pane, click ***ini*** Parameters.

    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'
    - **PLAYHELDTONEFORIP2IP**; In the Enter Value field, enter '1'
13. Click **Apply New Value**.

Figure 4-12: INI file Output Window



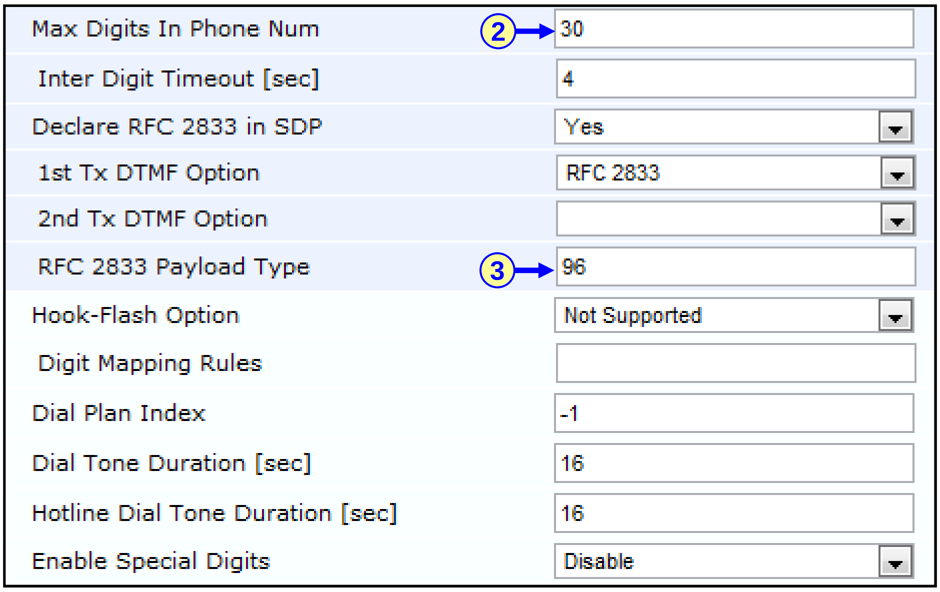
4.7 Step 7: Configure DTMF and Dialing

This step describes how to configure the DTMF and Dialing settings.

➢ **To configure DTMF and Dialing:**

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

Figure 4-13: DTMF and Dialing



2. Set **Max Digits In Phone Num** to ‘30’.
3. Set **RFC 2833 Payload Type** to ‘96’.

4.8 Step 8: Configure Coders

This step describes how to configure the SIP coders. Since the Mediation Server support only G.711A-law and G.711U-law voice coders, while the ITSP SIP trunk additionally supports the G.729 coder, you need to configure for the entries shown in the screen below.

➢ **To configure Coders:**

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

Figure 4-14: 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. Set the coders G.711A-law and G.711U-law.

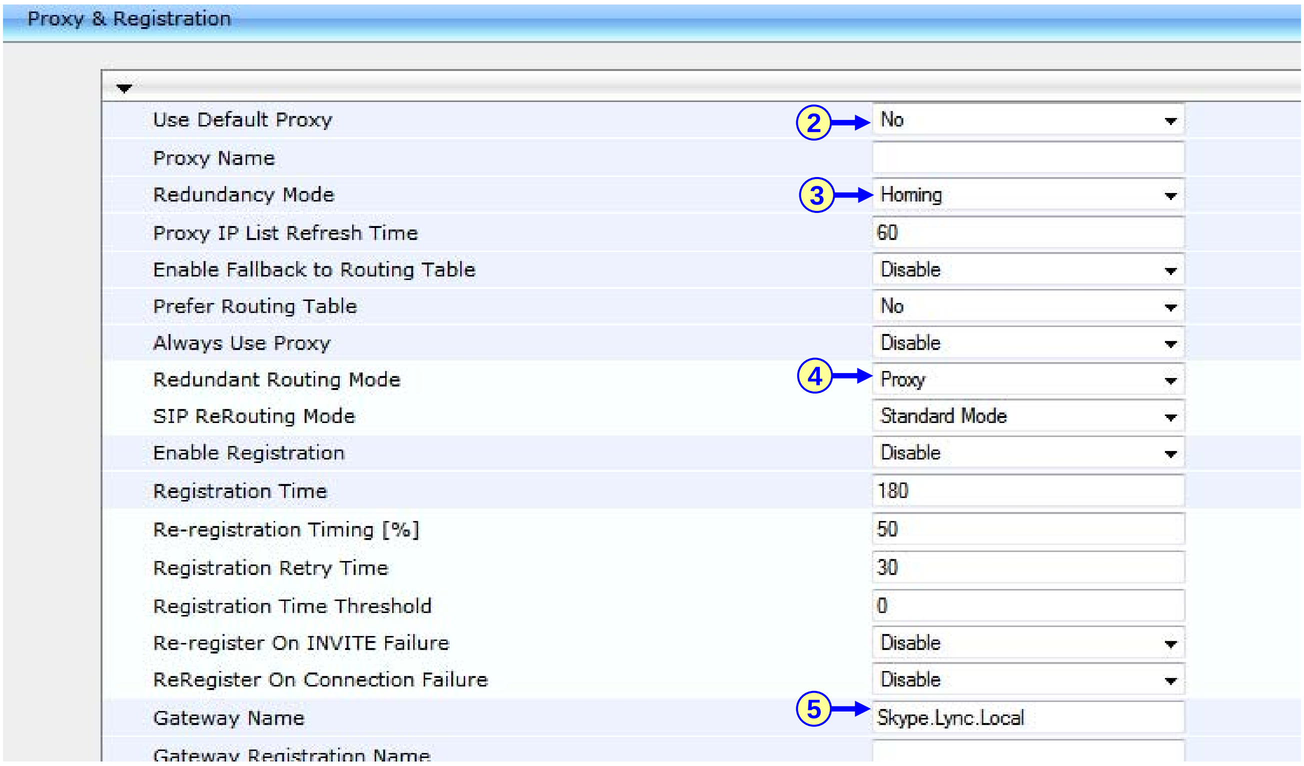
4.9 Step 9: Configure Proxy and Registration

This step 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 and Registration' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy and Registration**).

Figure 4-15: Proxy and Registration



2. Set **Use Default Proxy** to 'No'.
3. Set **Redundancy Mode** to 'Homing'.
4. Set **Redundant Routing Mode** to 'Proxy'.

   This will allow entry back into the Proxy Set table for the next available route.
5. Set **Gateway Name** to Gateway FQDN Name (e.g., 'Skype.Lync.local') (note that you configured this name in Section 4.19.3 on page 71).

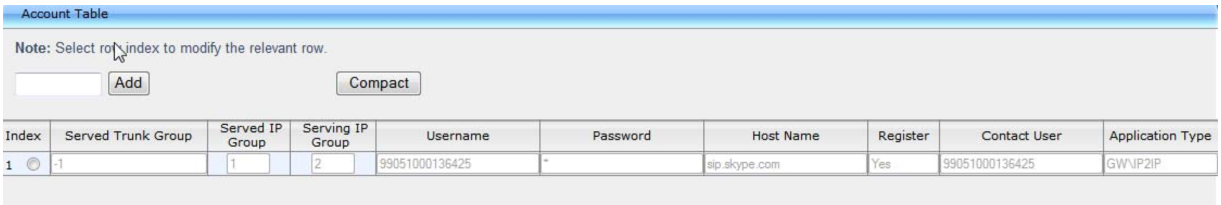
4.10 Step 10: Configure Accounts

This step describes how to configure and register Skype client extensions on the SIP Trunk. The Skype SIP trunk can register 10 Skype user client extensions for each account table entry. In this configuration, a single user client extension is registered. Note that in Section 4.14 on page 60, an IP Group is configured for the user entry in the table below.

➢ To configure Accounts:

1. Open the 'Account Table' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).

Figure 4-16: Account Table



2. Enter an index table entry number, and then click **Add**.
3. Configure the account user entry according to the example table above.

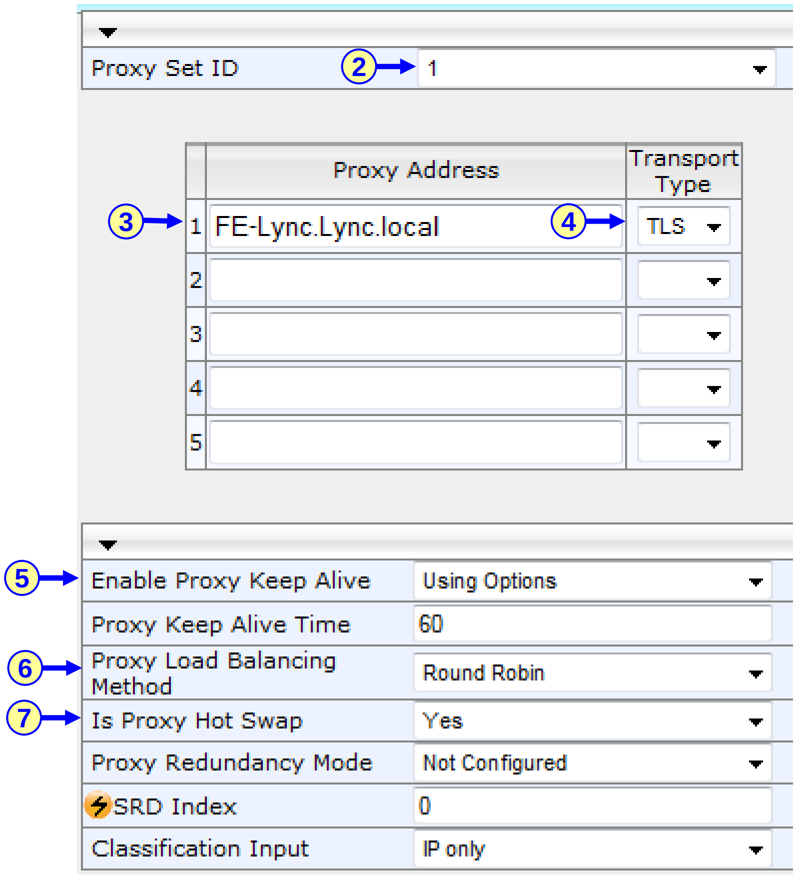
4.11 Step 11: Configure Proxy Sets

This step describes how to configure the proxy set tables. You need to configure two proxy sets, one for the Microsoft Lync server and the other for the Skype SIP trunk.

➢ To configure Proxy Set 1 for Microsoft Lync:

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

Figure 4-17: Proxy Sets Table 1

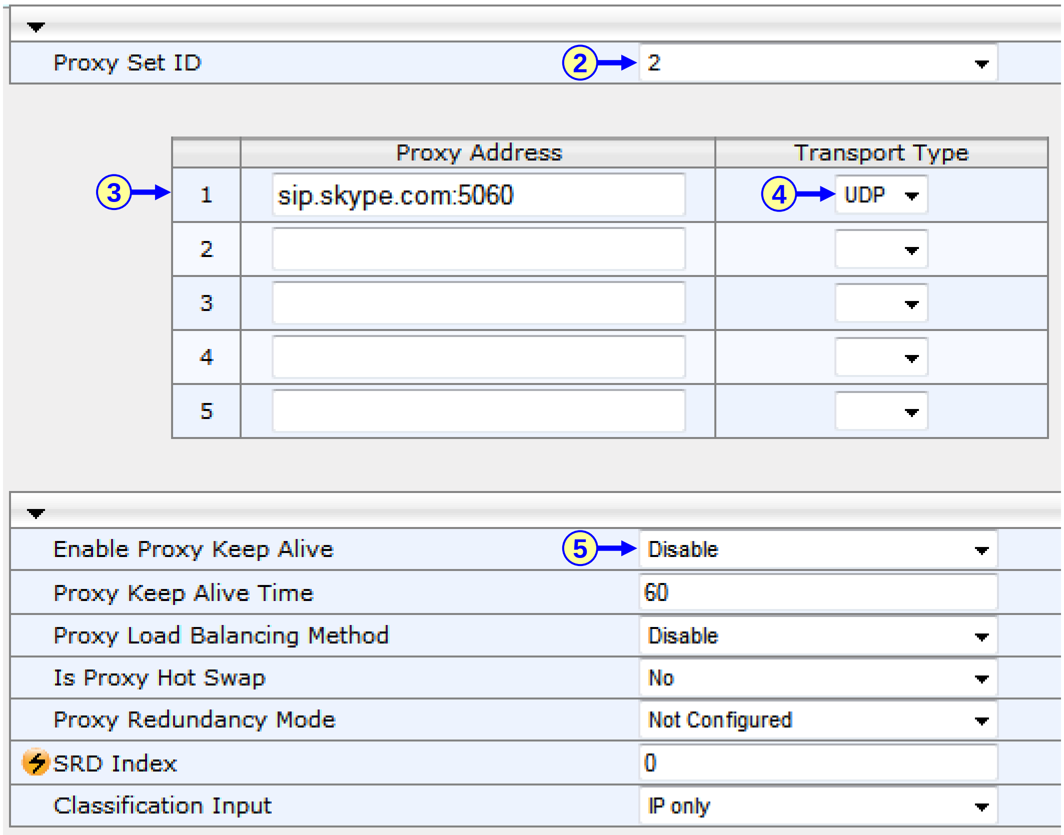


2. Set **Proxy Set ID** to '1'.
3. Configure Microsoft Lync Server SIP Trunking IP-Address or FQDN and Destination Port (e.g., FE-Lync.Lync.local).
4. Set **Transport Type** to 'TLS'.
5. Set **Enable Proxy Keep Alive** to 'Using Options'.
6. Set **Proxy Load Balancing Method** to 'Round Robin'.
7. Set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

➢ To configure Proxy Set 2 for Skype SIP Trunk:

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

Figure 4-18: Proxy Sets Table 2



2. Set **Proxy Set ID** to ‘2’.
3. Configure Skype IP-Address or FQDN and Destination Port (e.g., ’sip.skype.com:5060’).
4. Set **Transport Type** to ‘UDP’.
5. Set **Enable Proxy Keep Alive** to ‘Disable’.

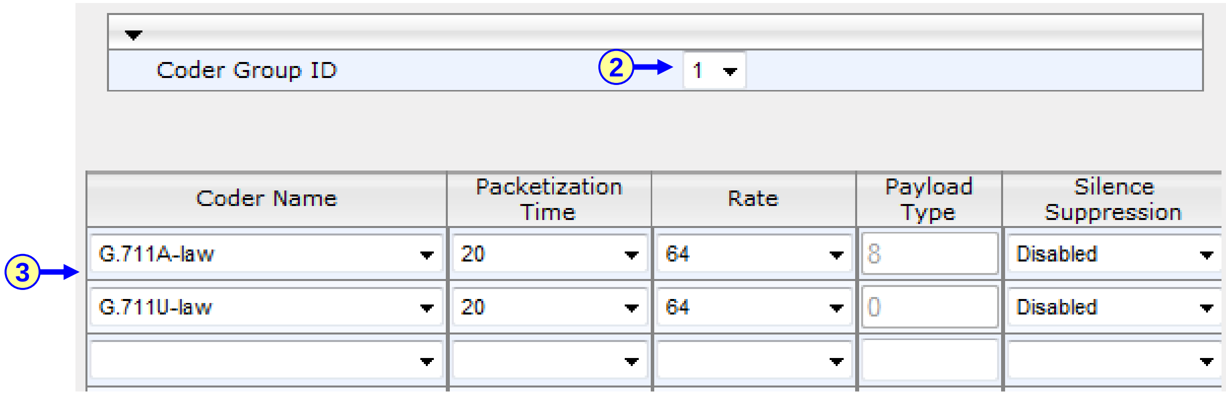
4.12 Step 12: Configure Coder Group

This step describes how to configure the Coder Groups. Microsoft Lync supports only the G.711 coder, while the network connection to Skype may restrict you to work with lower bandwidth coders, such as G.729. The 'Coder Group Settings' allow you to define up to four different Coder Groups. These Coder Groups are then assigned to IP Profiles, where each IP profile is based on the respective supported coder (see Section 4.13 on page 58).

➢ **To configure Coders Group for Microsoft Lync connection:**

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

Figure 4-19: Coders Group Settings

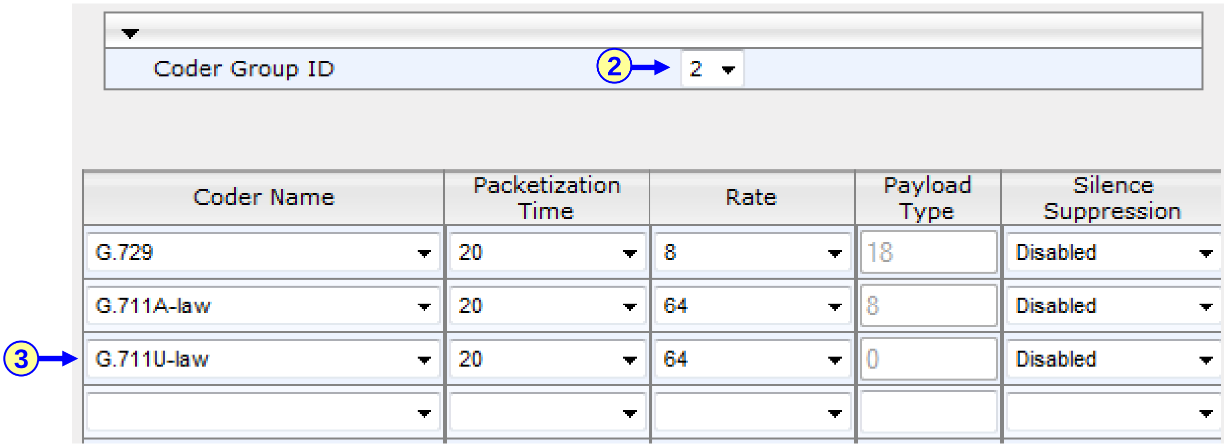


2. Select **Coder Group ID 1**.
3. Set **Coder Name** G.711A-law and G.711U-law.
4. Click **Submit**.

➢ To configure Coders Group for Skype SIP Trunk connection:

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

Figure 4-20: Coders Group Settings



2. Select **Coder Group ID 2**.
3. Set **Coder Name** G.729, G.711A-law and G.711U-law.
4. Click **Submit**.

4.13 Step 13: Configure IP Profile

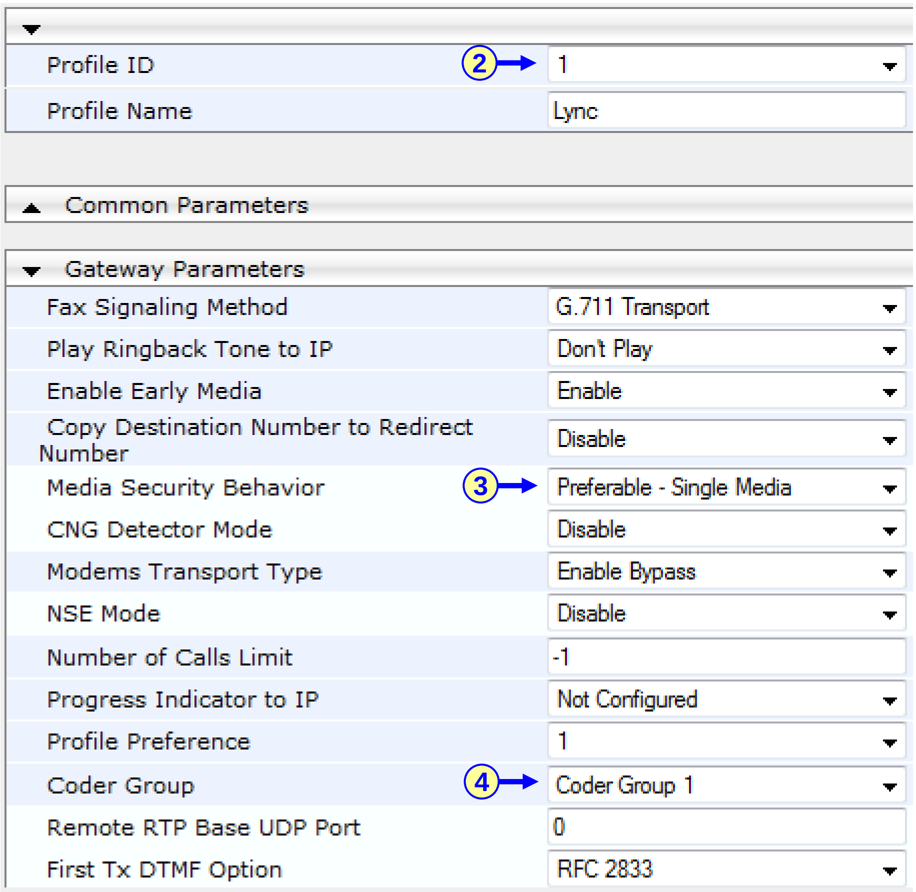
This step describes how to configure the IP Profile. In this configuration, the IP Profile is used to configure the SRTP/TLS mode and the Coder Group (see Section 4.12 on page 56).

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

➢ 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 4-21: IP Profile Settings

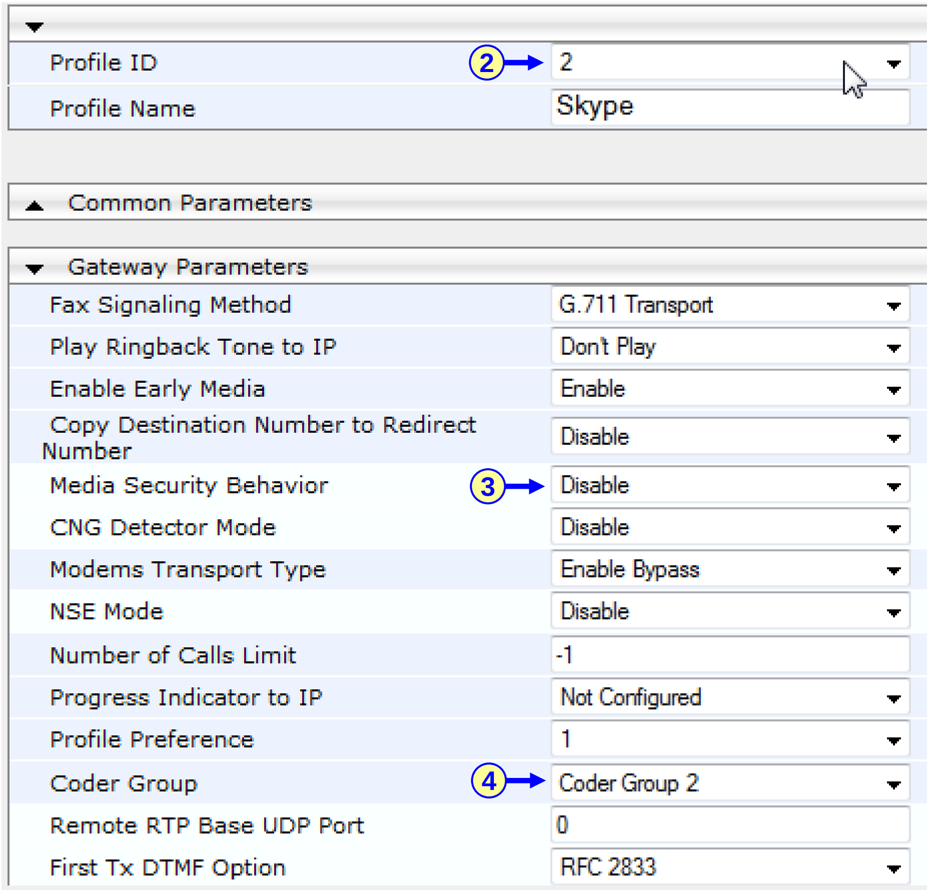


2. Select **Profile ID 1**.
3. Set **Media Security Behavior** to ‘Preferable – Single Media’.
4. Set **Coder Group** to ‘Coder Group 1’.
5. Click **Submit**.

➢ To configure IP Profile for Skype SIP Trunk:

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

Figure 4-22: IP Profile Settings



2. Select **Profile ID 2**.
3. Set **Media Security Behavior** to ‘Disable’.
4. Set **Coder Group** to ‘Coder Group 2’.
5. Click **Submit**

4.14 Step 14: Configure IP Group Tables

This step 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:

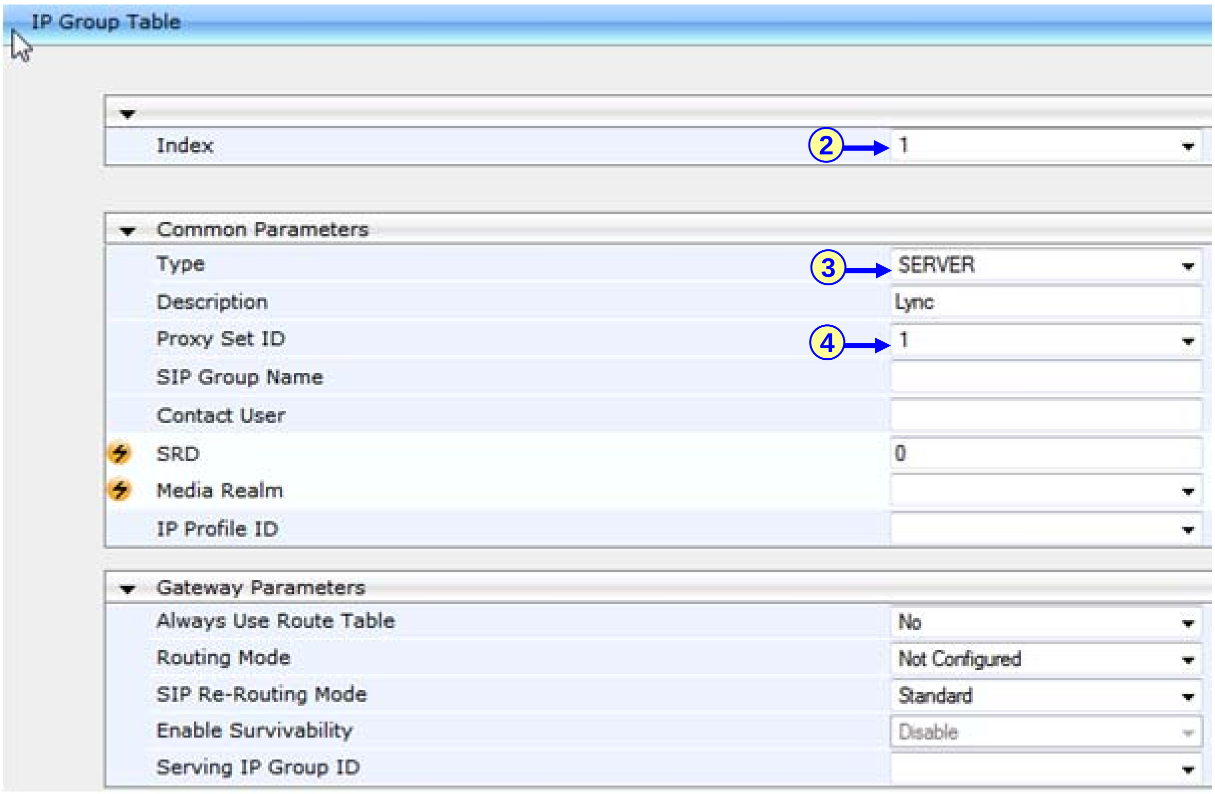
1. Lync Server 2010 – Mediation Server
2. Skype SIP SIP Trunk

These IP groups are later used by the IP2IP application for routing calls.

➢ To configure IP Group 1:

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

Figure 4-23: IP Group Table 1

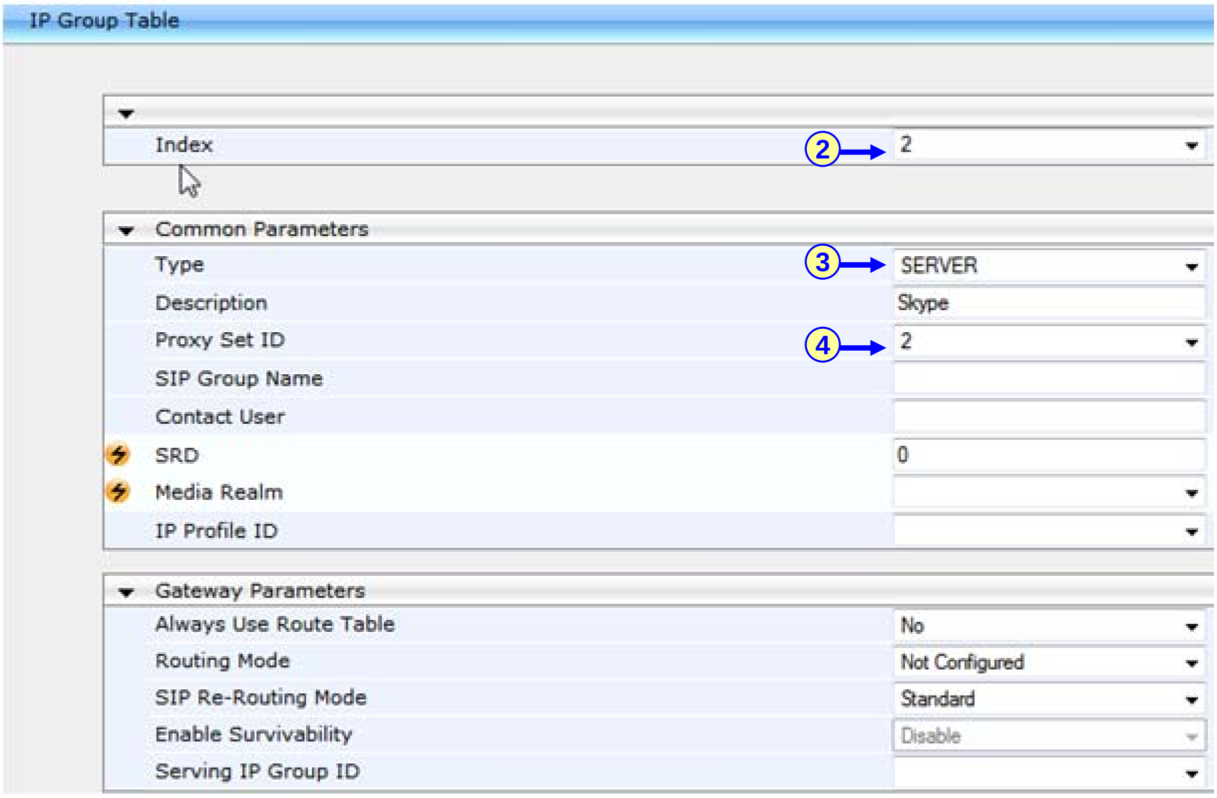


2. Set **Index** to ‘1’.
3. Set **Type** to ‘SERVER’.
4. Set **Proxy Set ID** to‘1’.

➢ **To configure IP Group 2:**

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

Figure 4-24: IP Group Table 2



2. Set **Index** to ‘2’.
3. Set **Type** to ‘Server’.
4. Set **Proxy Set ID** to‘2’.

4.15 Step 15: Configure Routing Rules

This step 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. Those tables provides 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.

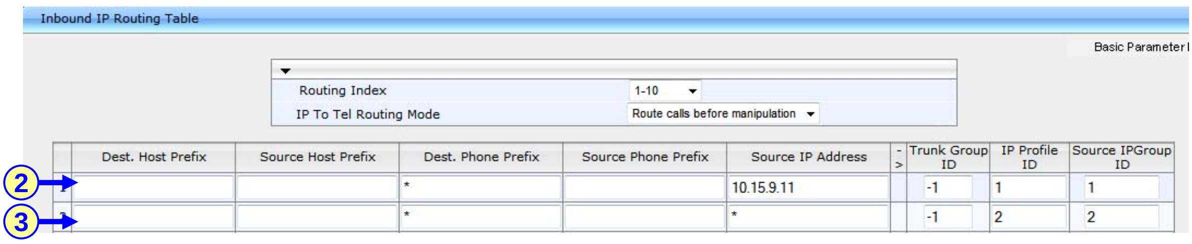
It is crucial that you adhere to the following guidelines when configuring your IP-to-IP routing rules:

- 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 inbound IP routing rules:

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 4-25: Inbound IP Routing Table

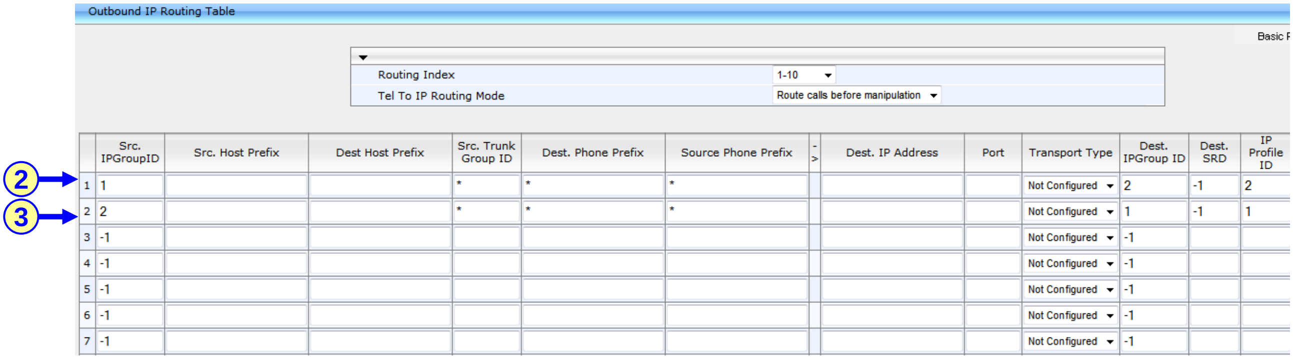


2. Calls that arriving from the Microsoft Lync server will be send to the 'Tel to IP Routing Table' (-1) with 'IP Profile ID' = 1 and marks as 'Source IPGroup ID' = 1.
3. Calls the arriving from Skype will be send to the 'Tel to IP Routing Table' (-1) with 'IP Profile ID' = 2 and marks as 'Source IPGroup ID'=2.

➢ To configure outbound IP routing rules:

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 4-26: Outbound IP Routing Table



	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
2	2			*	*	*				Not Configured	1	-1	1
3	-1									Not Configured	-1		
4	-1									Not Configured	-1		
5	-1									Not Configured	-1		
6	-1									Not Configured	-1		
7	-1									Not Configured	-1		

2. Calls from Source IPGroup ID ‘1’ (e.g., from Microsoft Lync) will be send to ‘Dest. IPGroup ID’ 2 (e.g., To Skype).
3. Calls from Source IPGroup ID ‘2’ (e.g., from Skype) will be send to ‘Dest. IPGroup ID’ 1 (e.g., To Lync).

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

4.16 Step 16 Configure Manipulation Rules

This step describes how to configure the manipulation tables.

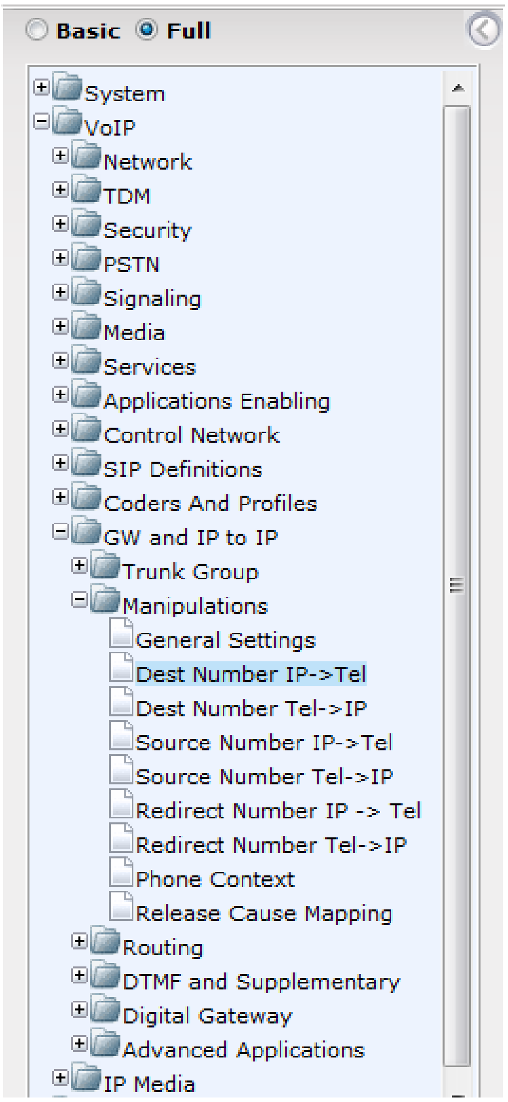
The Manipulation Tables submenu allows you to configure number manipulation and mapping of NPI/TON to SIP messages.

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

➢ To configure Manipulation Tables:

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

Figure 4-27: Manipulation Tables

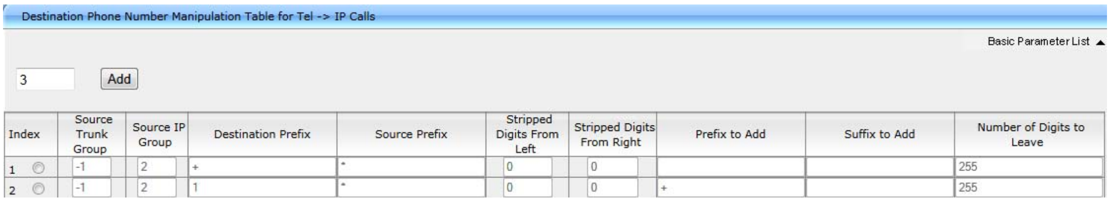


The following includes examples for number manipulation on destination and source numbers in the Tel-to-IP tables:

➢ To configure destination phone number manipulation rules for Tel-to-IP calls :

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

Figure 4-38: Destination Phone Number Manipulation Table for Tel-to-IP Calls Page



Destination Phone Number Manipulation Table for Tel -> IP Calls

Basic Parameter List

3 Add

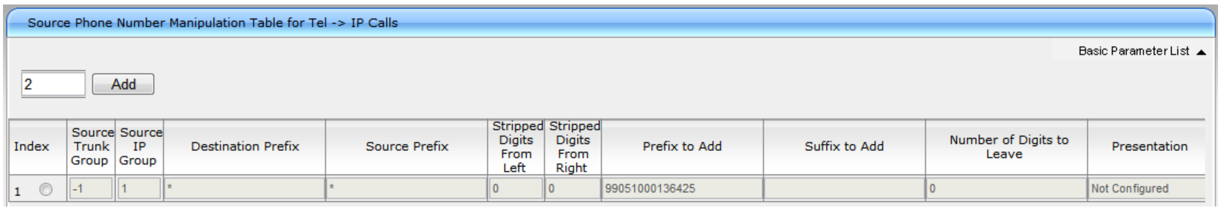
Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave
1	-1	2	+	*	0	0			255
2	-1	2	1	*	0	0	+		255

- **Index #1** defines the destination number manipulation of IP calls from the Skype SIP Trunk**.** All calls received from Source IP Group 2 (i.e., from the Skype SIP Trunk) and the destination number prefix begins with '+', do not perform any changes to the number.
- **Index #2** defines the destination number manipulation of IP calls from the Skype SIP Trunk. All calls received from Source IP Group 2 (i.e., from Skype SIP Trunk) and the destination number prefix begins with '1', add the '+' prefix to the number.

➢ To configure source phone number manipulation rules for Tel-to-IP calls:

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

Figure 4-40: Source Phone Number Manipulation Table for Tel -> IP Calls Page



Source Phone Number Manipulation Table for Tel -> IP Calls

Basic Parameter List

2 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	*	*	0	0	99051000136425		0	Not Configured

- **Index #1** defines source number manipulation of IP calls from the MS Lync Server. All calls received from Source IP Group 1 (i.e., from the MS Lync Server) for any source number, replace the number with the Account Number (i.e., with 99051000136425 in the above example).

4.17 Step 17: Secure Calls

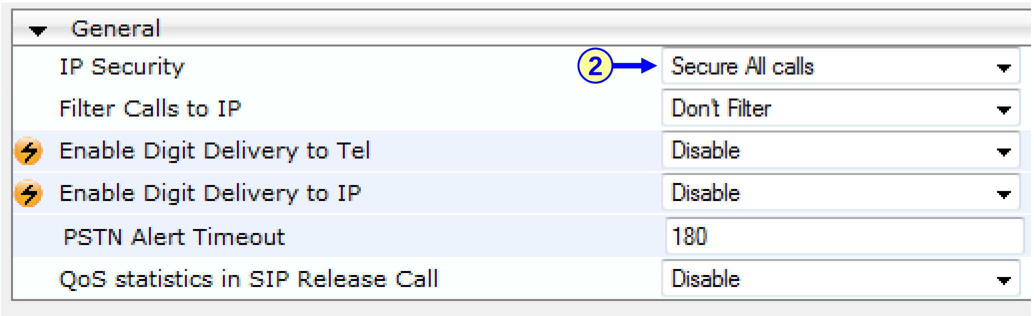
This step describes how to ensure that incoming calls to the LAN are sourced from valid IP addresses. This action prevents unwanted SIP calls, SIP messages, and/or VoIP spam. This feature is configured according to the device's policy on accepting or blocking SIP calls. You can configure the valid IP addresses by using one of the following methods:

- Using Proxies or Proxy Sets (see Section 4.11 on page 54).
- Using the Tel to IP routing table (see example below).

➢ **To configure Secure Calls:**

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

Figure 4-28: Advanced Parameters



2. Set **IP Security** to 'Secure All calls'.

➢ **To configure allowed IP in 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 4-29: Tel to IP Routing Table

Outbound IP Routing Table

Basic P

Routing Index	1-10
Tel To IP Routing Mode	Route calls before manipulation

	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
2	2			*	*	*				Not Configured	1	-1	1
3	-1									Not Configured	-1		
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			*	*	* 2		78.141.179.70		Not Configured	-1	-1	0
10	-1			*	*	*		10.15.9.11		Not Configured	-1	-1	0

2. Configure the allowed IP-Addresses (see example topology above).

4.18 Step 18: Alternative Routing Reasons

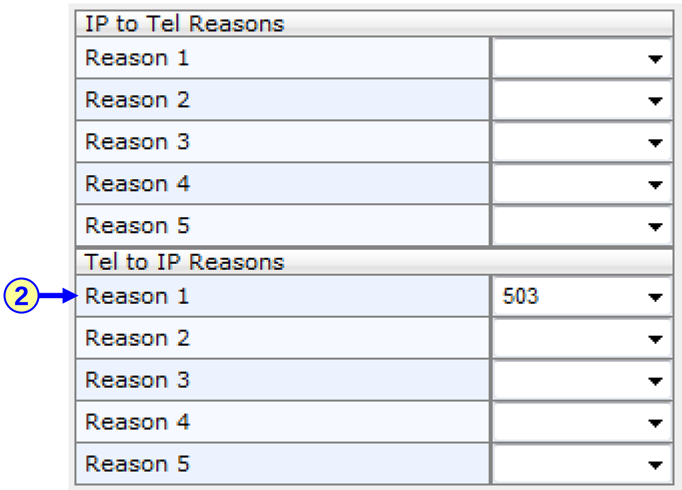
This step describes how to format the Alternative Routing Reasons. A 503 SIP response from the Mediation Server to an INVITE must cause the Mediant 1000 MSBG device to perform a failover. In other words, if the Lync Mediation Server primary proxy server is not responding, an attempt is made to establish communication with the secondary proxy server. For this event to occur, you need to perform the following actions:

- Configure the Reasons for Alternative Routing for Tel-to-IP calls to '503 SIP response' (see below).
- Configure the Lync Mediation Proxy Set for redundancy purposes. See Section 4.11 on page 54.

➢ To configure Alternative Routing Reasons:

1. Open the 'Alternative Routing Reasons' page (**Configuration** tab > **VoIP** menu > **Routing** > **Alternative Routing Reasons**).

Figure 4-30: Alternative Routing Reasons Table



2. Set **Tel to IP Reason 1** to '503'.
3. Click **Submit**.

4.19 Step 19: Define SIP TLS Connection

This step describes how to configure 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.

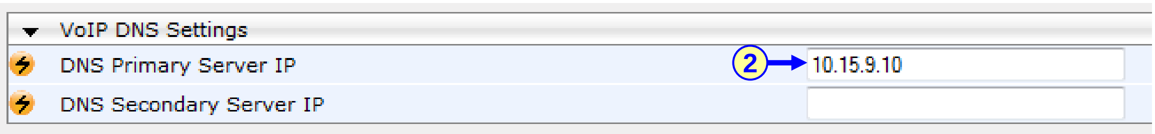
4.19.1 Step 19-1: Configure VoIP DNS Settings

This step 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 4-31: VoIP DNS Settings



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>.

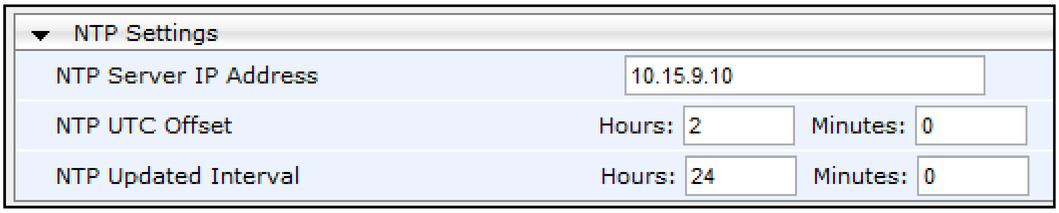
4.19.2 Step 19-2: Configure NTP Server

This step describes how to configure the NTP Server IP address. It is recommended to implement an NTP server (third-party) so that the Mediant 1000 MSBG 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 4-32: NTP Settings



2. Set the **NTP Server IP Address** to <NTP Server IP-Address> (e.g., 10.15.9.10).

4.19.3 Step 19-3: Configure a Certificate

This step describes how to exchange a certificate with the Microsoft Certificate Authority. The certificate is used by the Mediant 1000 MSBG device to authenticate the connection with the management PC (the PC used to manage the Mediant 1000 MSBG using the embedded Web server).

➢ **To configure a certificate:**

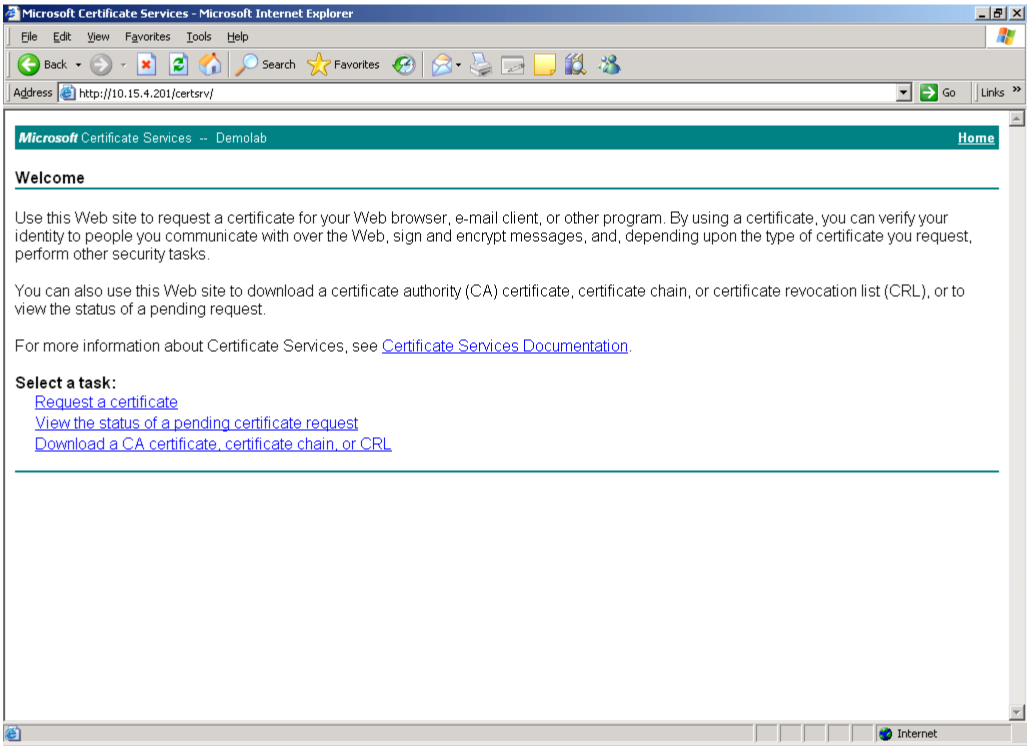
1. Open the ‘Certificates’ page (**Configuration** tab > **System** menu > **Certificates**).

Figure 4-33: Certificates Page

2. In the ‘Subject Name’ field, enter the Media Gateway name i.e **Skype.Lync.local** and then click **Generate CSR**; a Certificate request is generated.
3. Copy the CSR (from the line “----BEGIN CERTIFICATE” to “END CERTIFICATE REQUEST----”) to a text file (such as Notepad), and then save it to a folder on your PC as *certreq.txt*.

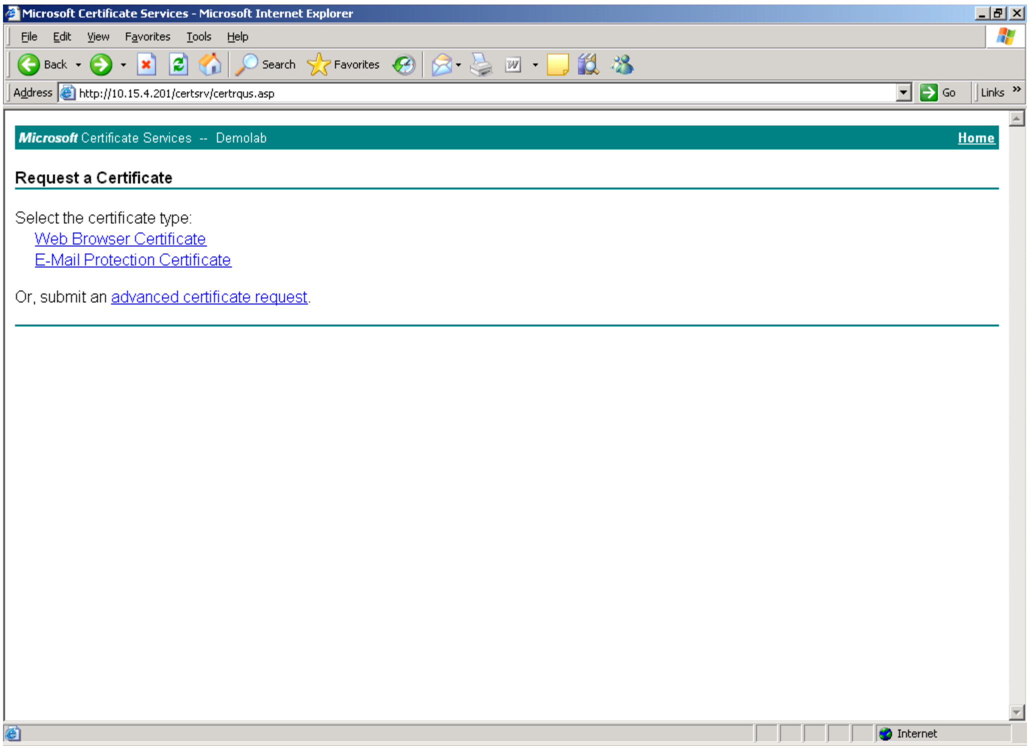
4. Navigate to the certificate 'Server http://<Certificate Server>/CertSrv'.

Figure 4-34: Microsoft Certificate Services Web Page



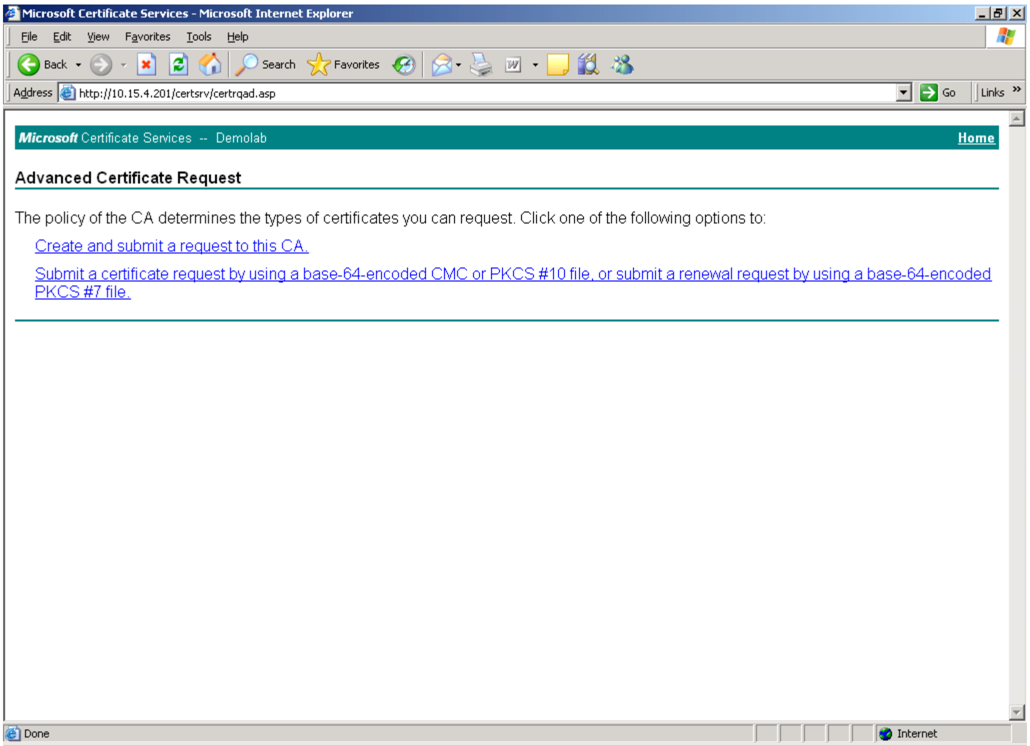
5. Click the link **Request a Certificate**.

Figure 4-35: Request a Certificate Page



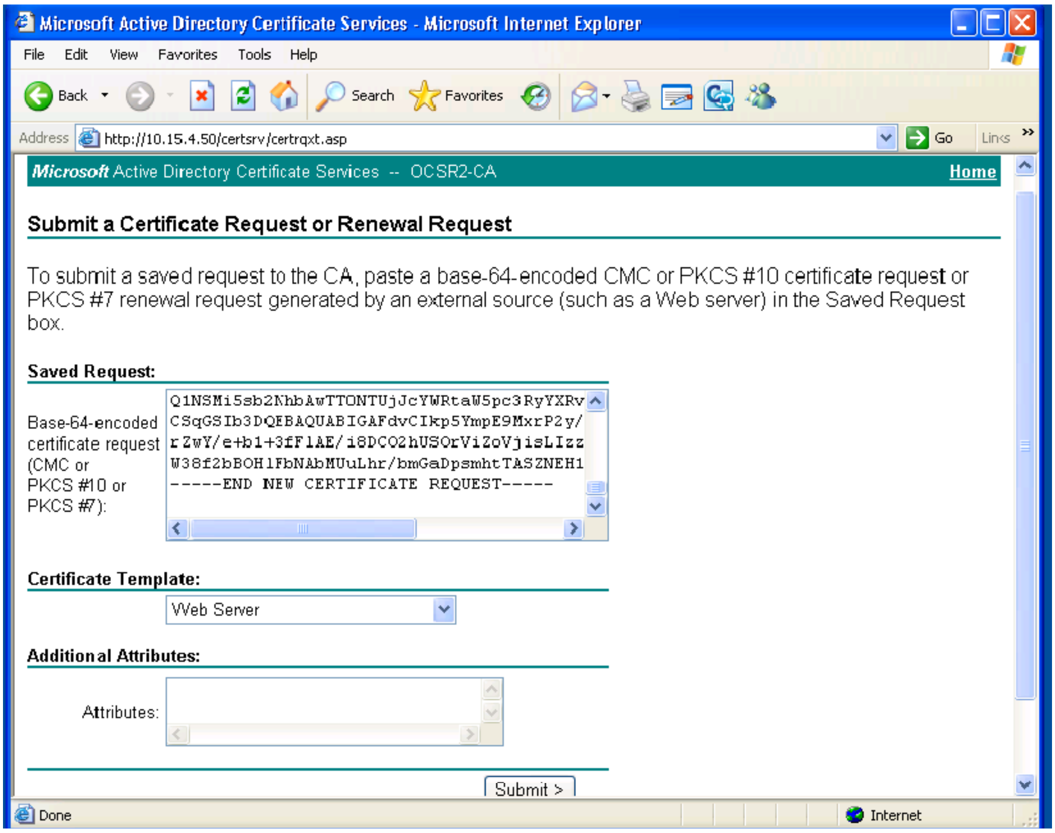
6. Click the link **Advanced Certificate Request**, and then click **Next**.

Figure 4-36: Advanced Certificate Request Page



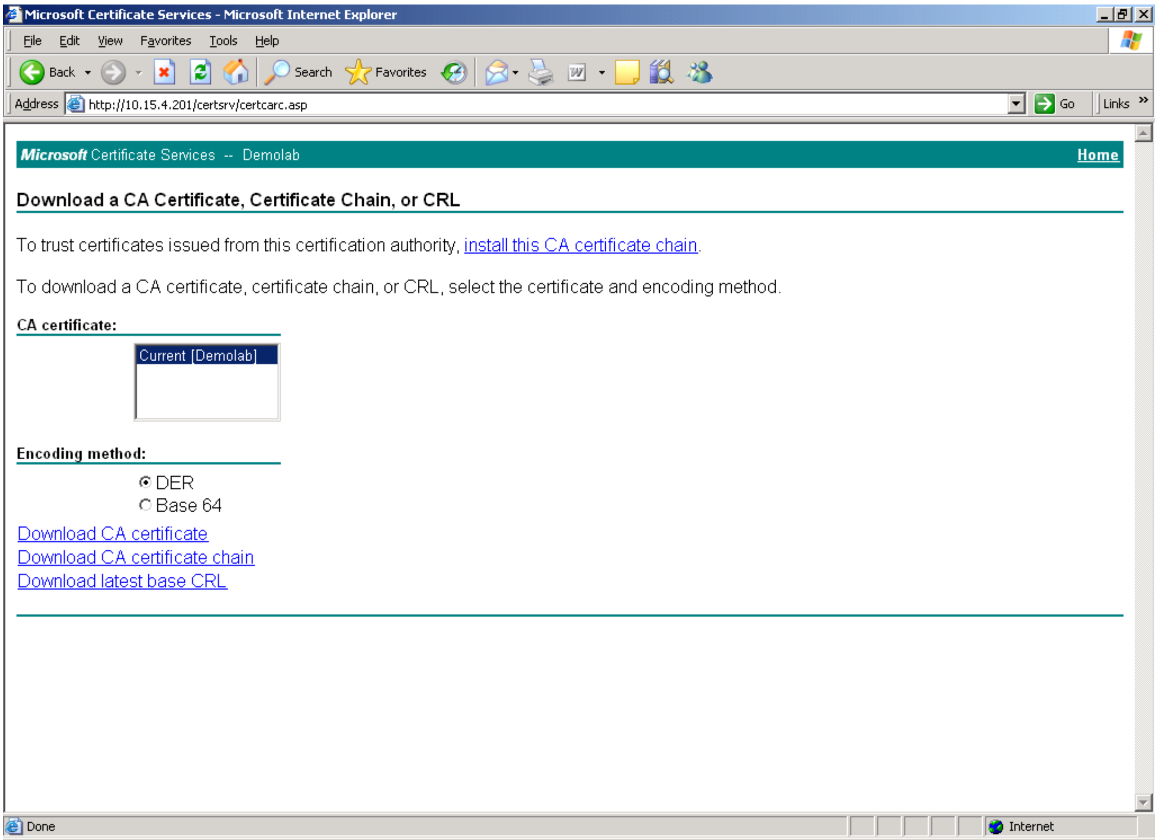
7. Click the link **Submit a Certificate request by using base64 encoded...**, and then click **Next**.

Figure 4-37: Submit a Certificate Request or Renewal Request Page



8. Open the *certreq.txt* file that you created and saved (see Step 3), and then copy its contents to the 'Base64 Encoded Certificate Request' text box.
9. Select "Web Server" from the **Certificate Template** drop-down box.
10. Click **Submit**.
11. Choose the 'Base 64' encoding option, and then click the link **Download CA certificate**.
12. Save the file as '*gateway.cer'* in a folder on your PC.
13. Navigate to the certificate Server http://<Certificate Server>/CertSrv.
14. Click the link **Download a CA Certificate**, **Certificate Chain or CRL**.

Figure 4-38: Download a CA Certificate, Certificate Chain, or CRL Page



15. Under the Encoding method group, perform the following:
    a. Select the ‘Base 64’ encoding method option.
    b. Click the link Download CA certificate.
16. Save the file as ‘*certroot.cer’* in a folder on your PC.
17. Navigate back (in the Mediant 1000 MSBG device) to the ‘Certificates’ page.
18. In the ‘Certificates’ page, in the ‘Server Certificate’ field, click **Browse** and select the ‘*Gateway.cer’* certificate file that you saved on your local disk (see Step 12), and then click **Send File** to upload the certificate.

19. In 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 16), and then click **Send File** to upload the certificate.

Figure 4-39: Certificates Page

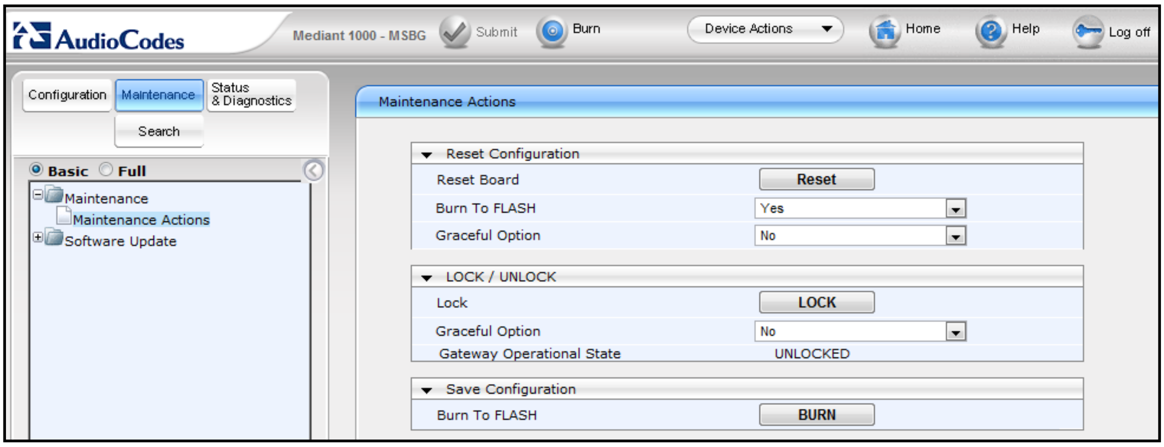
20. Save (burn) the Media Gateway configuration and reset the Media Gateway, using the Web interface's 'Maintenance Actions' page (On the Navigation bar, click the **Management** tab, and then in the Navigation tree, select the **Management Configuration** menu, and then choose the **Maintenance Actions**).

4.20 Step 20: Reset 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 4-40: Reset the GW



Note: Reset with BURN to FLASH is required.

Reader's Notes

5 Appendix A: AudioCodes INI file

This step shows the Mediant 1000 MSBG device INI file. This file reflects the configuration described in Section 4 on page 37.

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

;Board: Mediant 1000 - MSBG
;Serial Number: 3589366
;Slot Number: 1
;Software Version: 6.20A.022.003
;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: 12  Num DSP Channels: 48
;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
FireWallandVPN 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 : Empty
;      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 = '1,43,48,15'
```

```
[BSP Params]

PCMLawSelect = 3
EnableLANWatchdog = 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]

BrokenConnectionEventTimeout = 100
EnableAGC = 1
EnableDSPIPMDetectors = 1
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
FarEndDisconnectSilenceMethod = 2
FarEndDisconnectSilencePeriod = 120
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
WanMgmtHttpPort = 80
WanMgmtHttpsPort = 443

[SIP Params]
```

```
MEDIACHANNELS = 120
ISPROXYUSED = 0
ISREGISTERNEEDED = 0
AUTHENTICATIONMODE = 1
SIPDESTINATIONPORT = 5067
PLAYRBTONE2TEL = 3
SECURECALLSFROMIP = 2
GWDEBUGLEVEL = 5
ENABLEEARLYMEDIA = 1
SIPGATEWAYNAME = 'GW-131.Lync.Local'
STATICNATIP = 195.189.192.151
PROGRESSINDICATOR2IP = -1
PROXYREDUNDANCYMODE = 1
CDRSYSLOGSERVERIP = 0.0.0.0
PSTNALERTTIMEOUT = 180
ISFAXUSED = 2
SIPTRANSPORTTYPE = 2
TLSLOCALSIPPORT = 5067
MEDIASECURITYBEHAVIOUR = 3
REDUNDANTROUTINGMODE = 2
ENABLECONTACTRESTRICTION = 1
FORKINGHANDLINGMODE = 1
ENABLEIP2IPAPPLICATION = 1
ENABLEEARLY183 = 1
FAKERETRYAFTER = 60

[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 ]
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 8 = *, 78.141.179.70, *, 0, 255, 0, -1, , -1, , -1, -1, -1;
PREFIX 9 = *, 10.15.9.11, *, 0, 255, 0, -1, , -1, , -1, -1, -1;

[ \PREFIX ]

;
;  *** TABLE NumberMapIp2Tel ***
;
;

[ NumberMapIp2Tel ]
FORMAT NumberMapIp2Tel_Index = NumberMapIp2Tel_DestinationPrefix,
NumberMapIp2Tel_SourcePrefix, NumberMapIp2Tel_SourceAddress,
NumberMapIp2Tel_NumberType, NumberMapIp2Tel_NumberPlan,
NumberMapIp2Tel_RemoveFromLeft, NumberMapIp2Tel_RemoveFromRight,
NumberMapIp2Tel_LeaveFromRight, NumberMapIp2Tel_Prefix2Add,
NumberMapIp2Tel_Suffix2Add,
NumberMapIp2Tel_IsPresentationRestricted,
NumberMapIp2Tel_SrcTrunkGroupID, NumberMapIp2Tel_SrcIPGroupID;
NumberMapIp2Tel 1 = +999, *, *, 255, 255, 4, 0, 255, +972, , 255, -
1, -1;
NumberMapIp2Tel 2 = +, *, *, 255, 255, 0, 0, 255, , , 255, -1, -1;
NumberMapIp2Tel 3 = *, *, *, 255, 255, 0, 0, 255, +, , 255, -1, -1;

[ \NumberMapIp2Tel ]

;
;  *** 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 = *, , *, 255, 255, 0, 0, 0,
99051000136425, , 0, -1, 1;
SourceNumberMapTel2Ip 2 = *, +, *, 255, 255, 0, 0, 255, , , 255, -
1, -1;
SourceNumberMapTel2Ip 3 = *, *, *, 255, 255, 0, 0, 255, +, , 255, -
1, -1;

[ \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 = *, -1, , *, 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:5067, 2, 1;
ProxyIp 1 = sip.skype.com:5060, 0, 2;

[ \ProxyIp ]

;
;  *** TABLE IpProfile ***
;
;

[ 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_SBCDiversionMode, IpProfile_SBCHistoryInfoMode;
IpProfile 1 = Lync, 1, 0, 2, 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 = Skype, 1, 1, 2, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 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 = 0, 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, 0, -1, -1, -1,
;
IPGroup 2 = 0, Skype, 2, , , 0, -1, 0, 0, -1, 0, , 1, 0, -1, -1, -
1, ;
[ \IPGroup ]

;
;  *** TABLE Account ***
;
;

[ Account ]
FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroup, Account_ServingIPGroup, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 1 = -1, 1, 2, 99051000136425, *, sip.skype.com, 1,
99051000136425, 0;

[ \Account ]

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

```
;

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

[ \CodersGroup0 ]
```

```
;
;  *** TABLE CodersGroup1 ***
;
;

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

[ \CodersGroup1 ]

;
;  *** TABLE CodersGroup2 ***
;
;

[ CodersGroup2 ]
FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = g729, 20, 0, -1, 0;

[ \CodersGroup2 ]
```

Reader's Notes

6 Appendix B: Configuring Skype

This step describes how to access and create a Skype account, in the Skype Manager web site.

6.1 Skype Manager

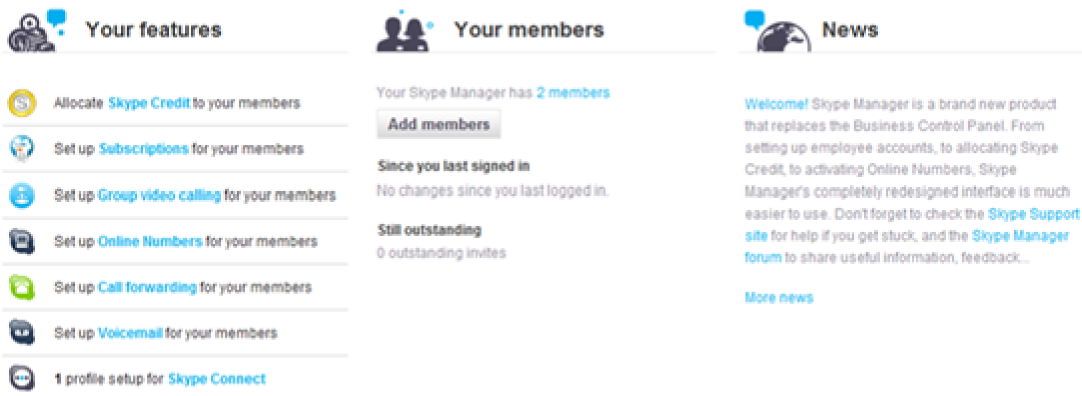
➢ **To access the Skype Manager:**

1. Open the browser and enter the following URL: https://login.skype.com/bcp/login?message=login_required.
2. Enter username and password.
3. Press **Sign me in.**

Figure 6-1: login Page

4. Go to **Skype Connect**:

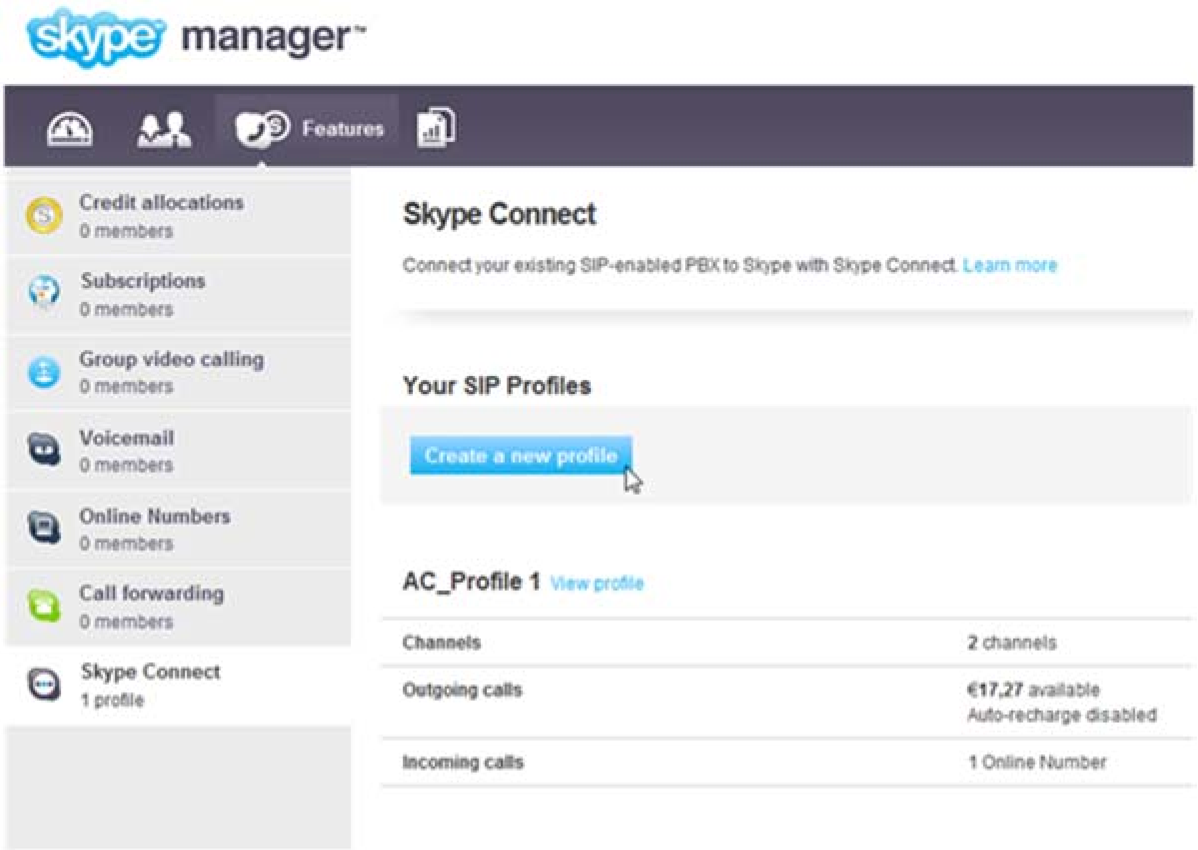
Figure 6-2: Main Page



To create new account:

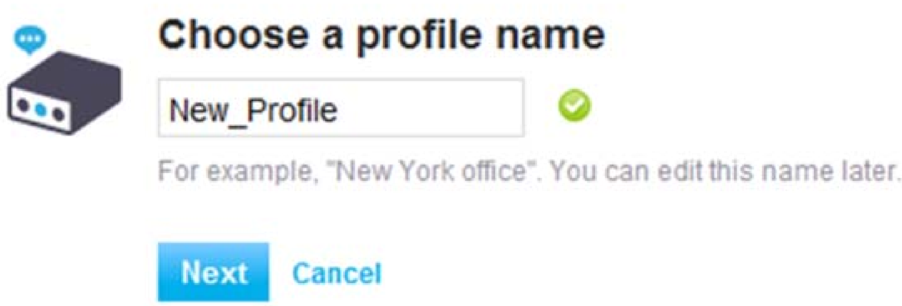
1. Press **Create a new profile.**

Figure 6-3: Skype Connect page



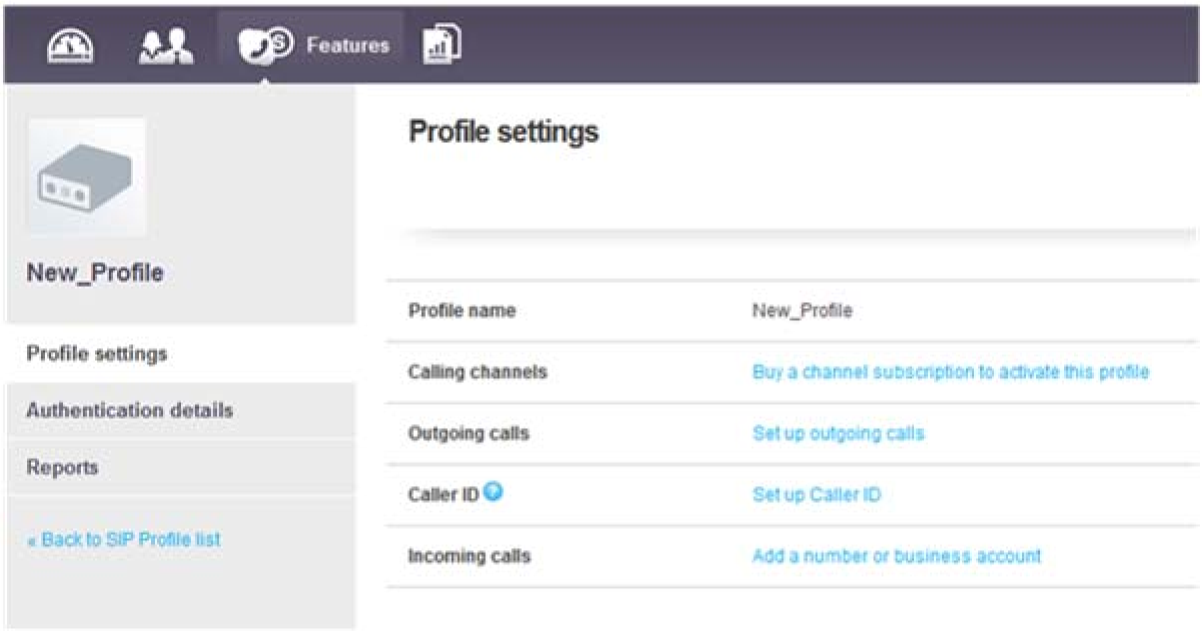
2. Choose profile name and press **Next**.

Figure 6-4: Create Profile Page



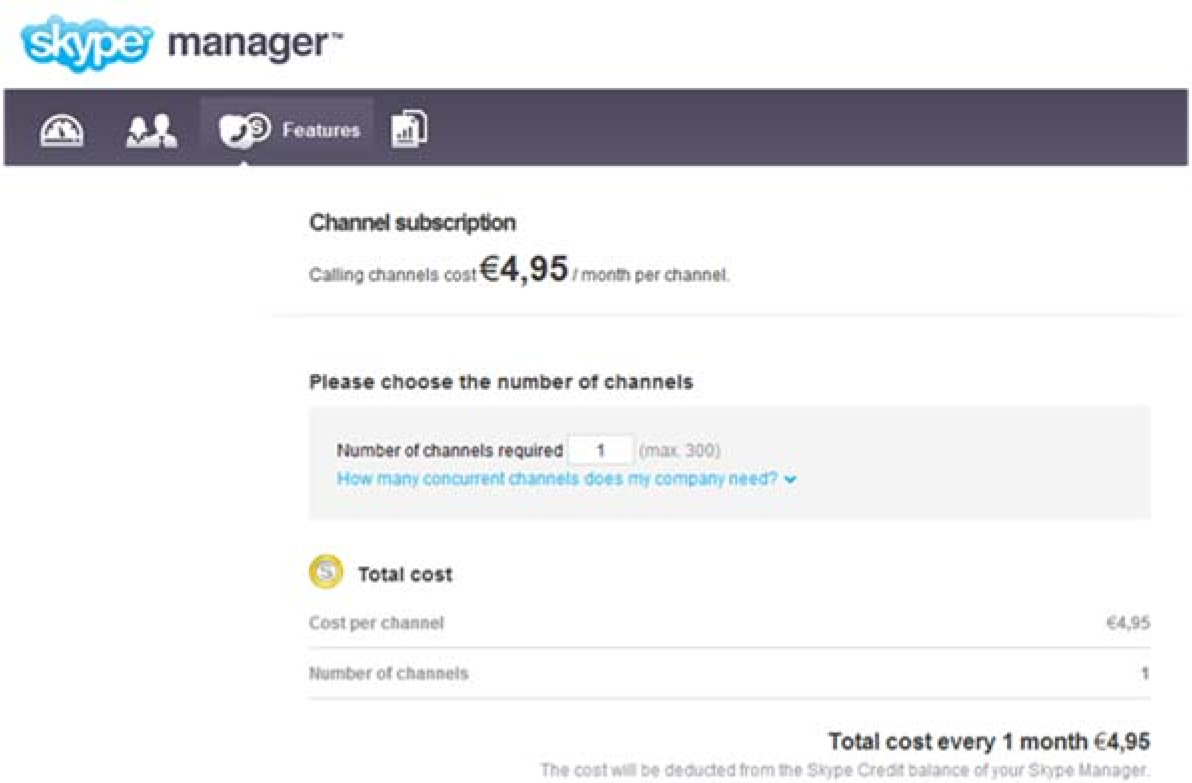
3. Enter **Profile Settings** page to proceed configuration.
4. Press **Buy a channel Subscription to activate this profile**.

Figure 6-5: Profile Settings Page



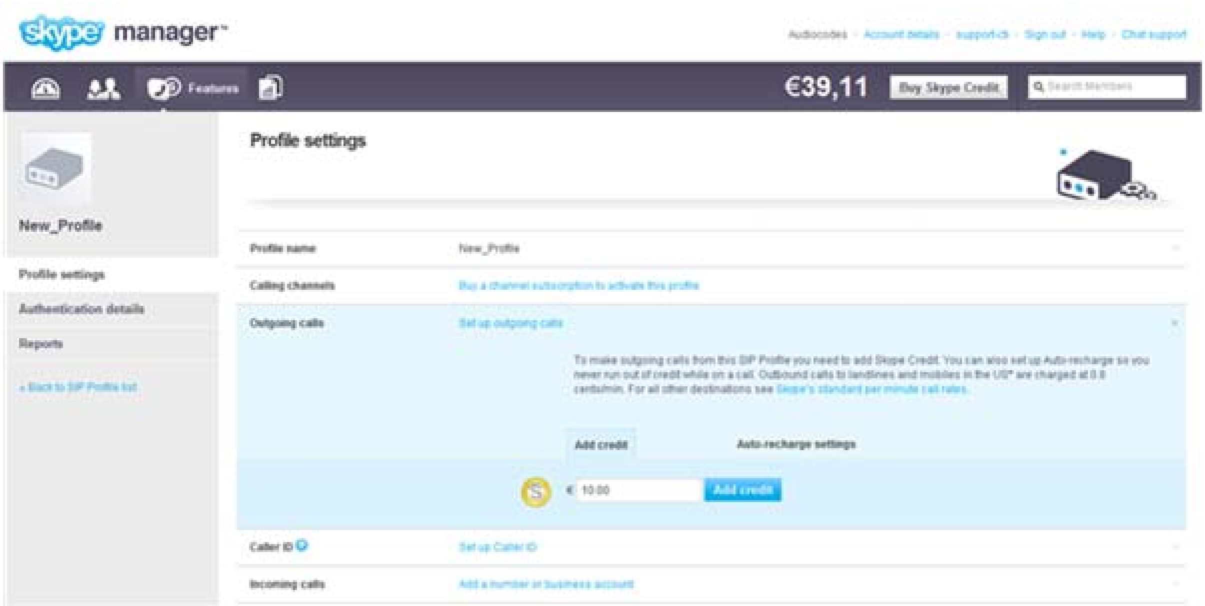
5. Enter the number of channels.

Figure 6-6: Channel Subscription Page



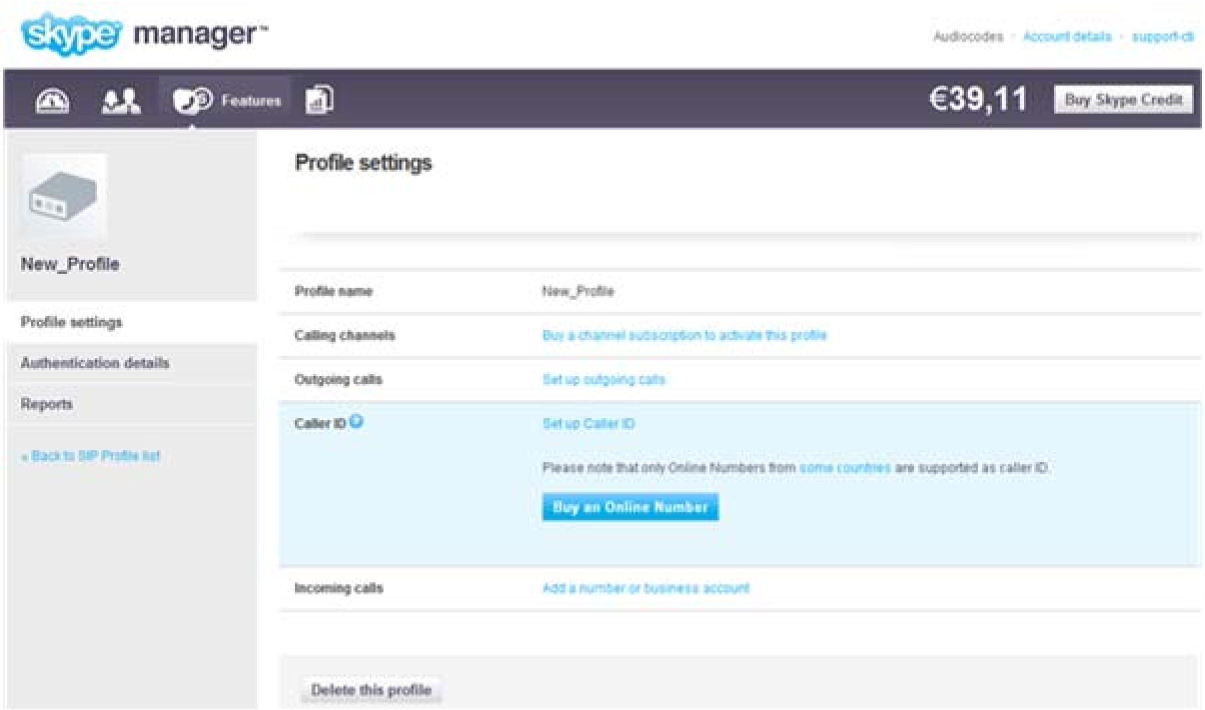
6. Allow outgoing calls (purchase)

Figure 6-7: Outgoing Calls Page



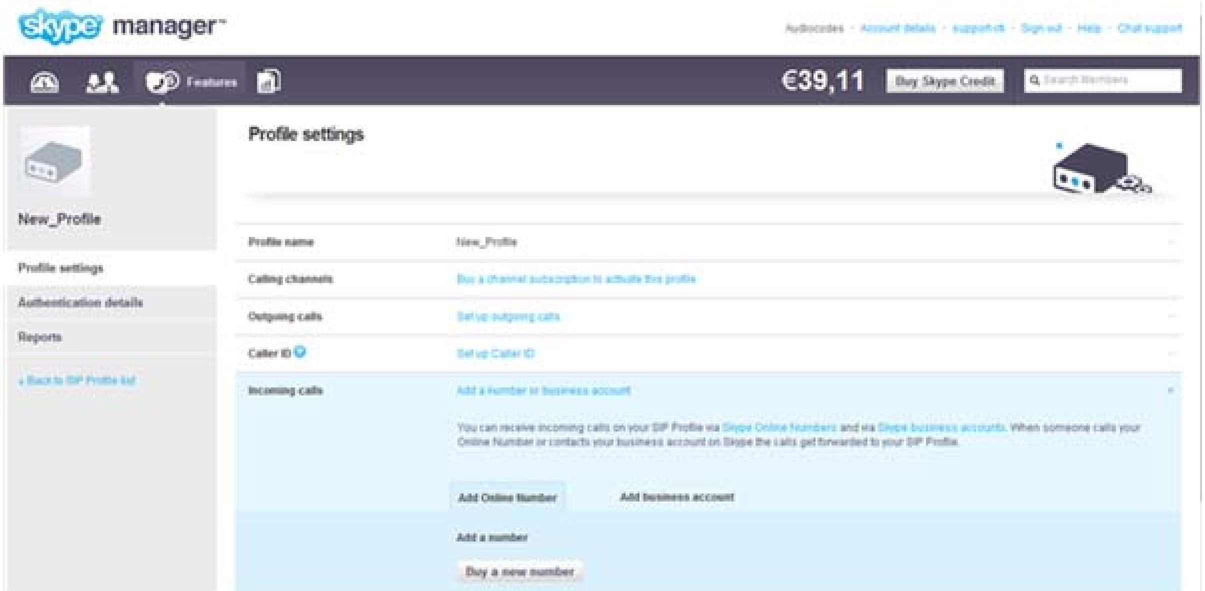
7. Set up Caller ID.

Figure 6-8: Caller ID Page



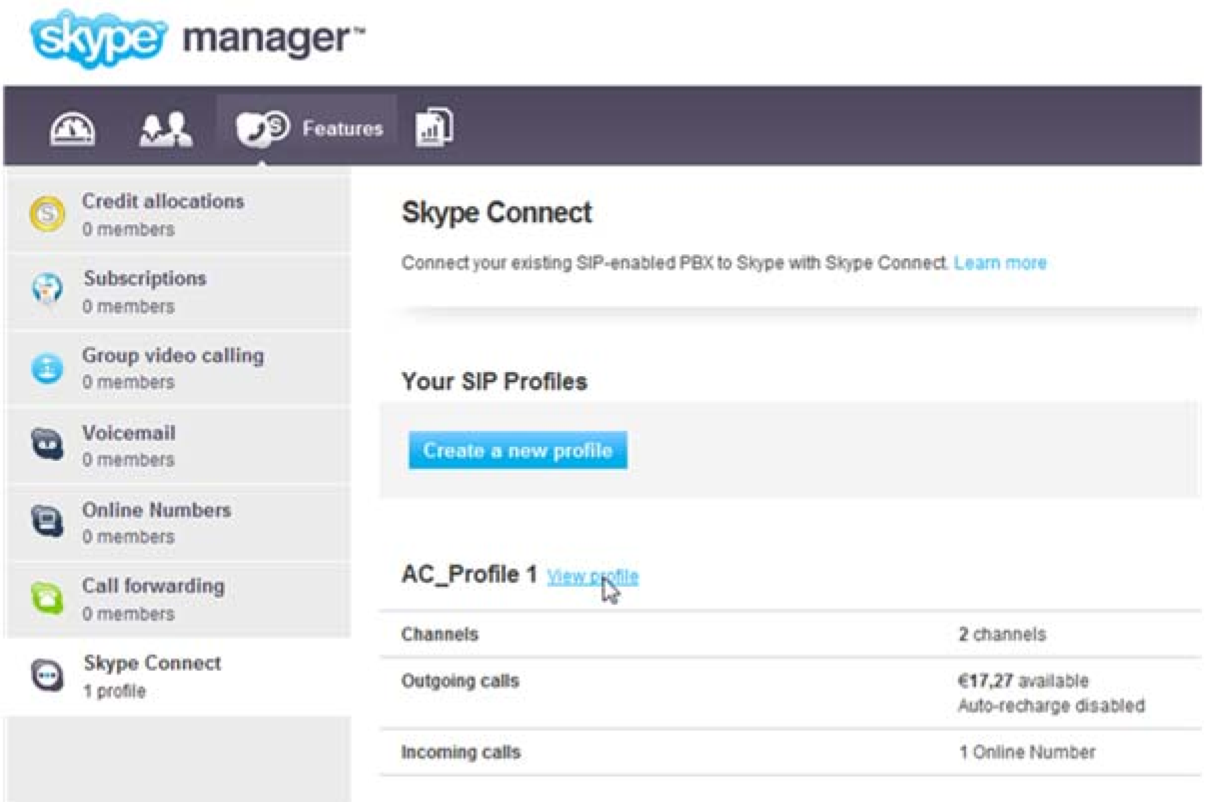
8. Add PSTN number (for incoming calls).

Figure 6-9: Incoming Calls Page



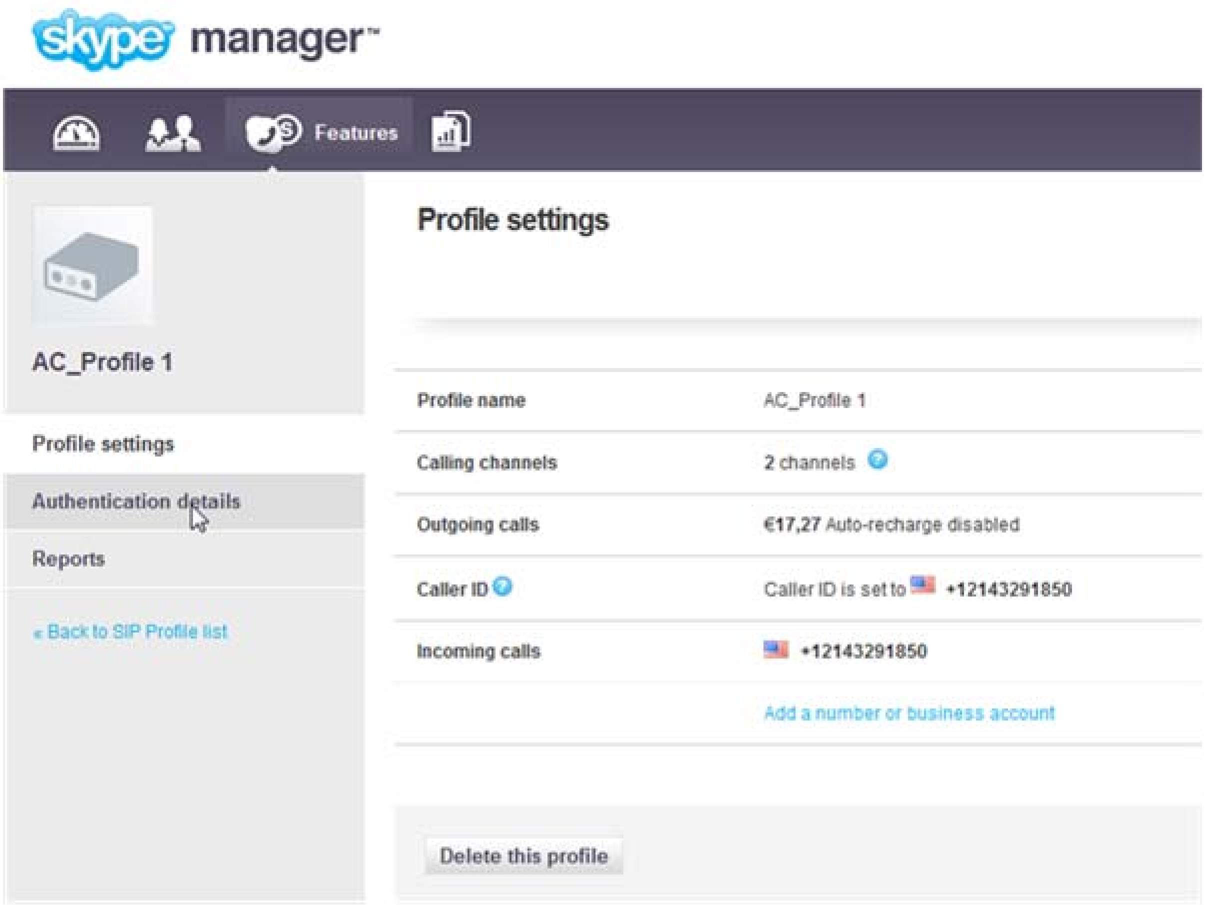
9. View the Skype Account And settings

Figure 6-10: Account page



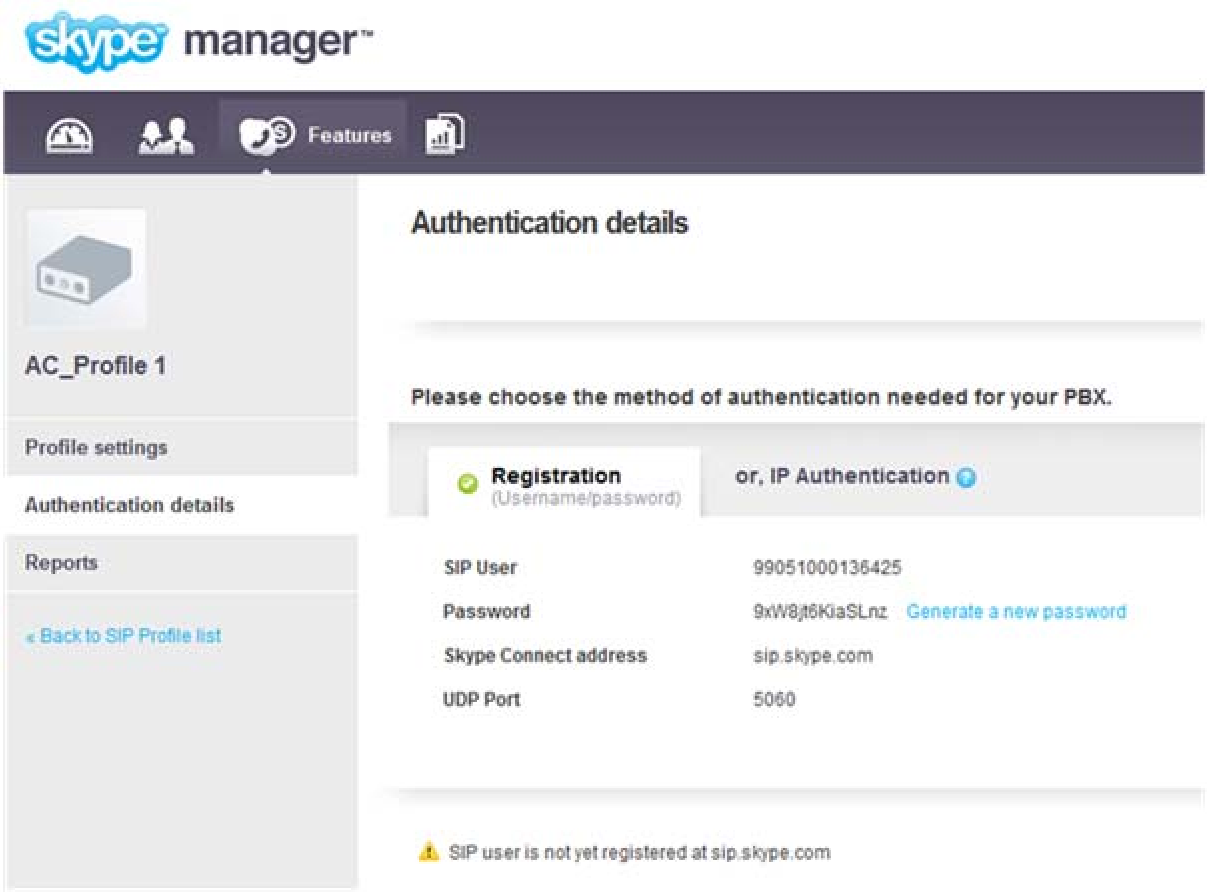
10. Press **view profile.**

Figure 6-11 Profile Page



11. View the Authentication details.
12. Copy the authentication information into the account table on the Mediant 1000 MSBG (see Section 4.10 on page 53).

Figure 6-12 Authentication page



Configuration Note

www.audiocodes.com