Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2010 & Bell Canada SIP Trunk using Mediant E-SBC

Microsoft Partner
Gold Communications

Microsoft® Lync™

Bell

AudioCodes

August 2013

Document # LTRT-39231

Table of Contents

Reader's Notes

Notice

This document describes how to connect the Microsoft Lync Server 2010 and Bell Canada SIP Trunk using AudioCodes Mediant E-SBC product series, which includes the Mediant 800 Gateway & E-SBC, Mediant 1000B Gateway & E-SBC, Mediant 3000 Gateway & E-SBC, Mediant 2600 E-SBC, and Mediant 4000 E-SBC.

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

Date Published: August 22, 2013

Trademarks

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.

Reader's Notes

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between Bell Canada's SIP Trunk and Microsoft's Lync Server 2010 environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Bell Canada Partners who are responsible for installing and configuring Bell Canada's SIP Trunk and Microsoft's Lync Server 2010 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	F6.60A.235.010
Protocol	▪ SIP/UDP (to the Bell Canada SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 Bell Canada SIP Trunking Version

Table 2-2: Bell Canada Version

Vendor/Service Provider	Bell Canada
SSW Model/Service	BroadSoft
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2010 Version

Table 2-3: Microsoft Lync Server 2010 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2010 4.0.7577 CU6
Protocol	SIP
Additional Notes	None

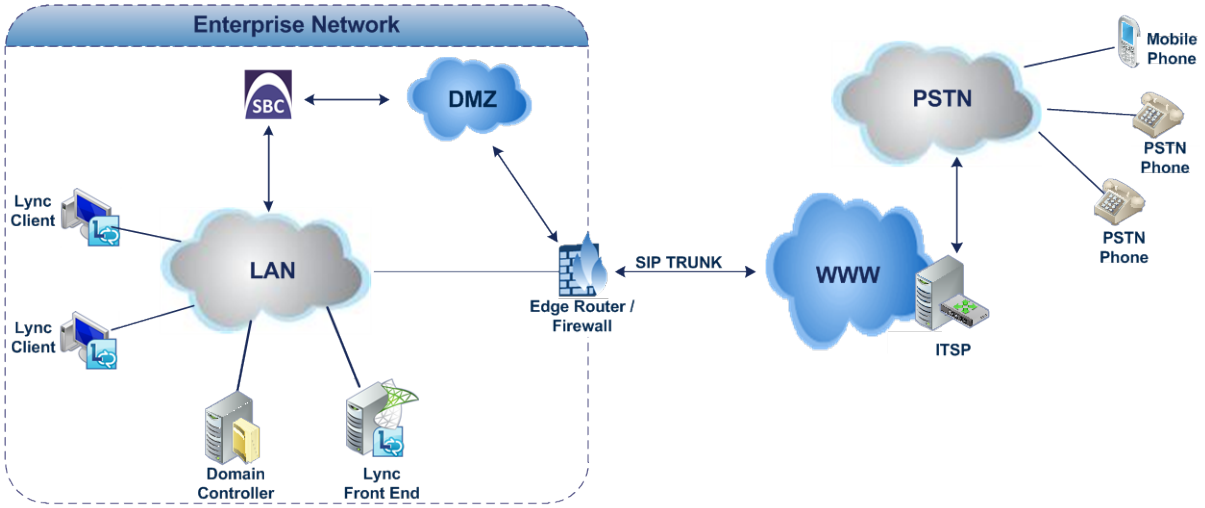
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Bell Canada SIP Trunk with Lync 2010 was done using the following topology setup:

- Enterprise deployed with Microsoft Lync Server 2010 in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Bell Canada's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between Lync Server 2010 network in the Enterprise LAN and Bell Canada's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

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



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Lync Server 2010 environment is located on the Enterprise's LAN ▪ Bell Canada SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2010 operates with SIP-over-TLS transport type ▪ Bell Canada SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2010 supports G.711A-law and G.711U-law coders ▪ Bell Canada SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2010 operates with SRTP media type ▪ Bell Canada SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2010 and Bell Canada's SIP Trunk.

Reader's Notes

3 Configuring Lync Server 2010

This chapter describes how to configure Microsoft Lync Server 2010 to operate with AudioCodes E-SBC.

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

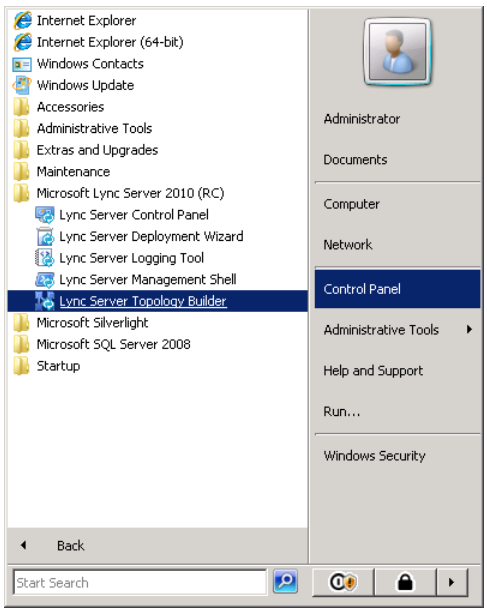
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

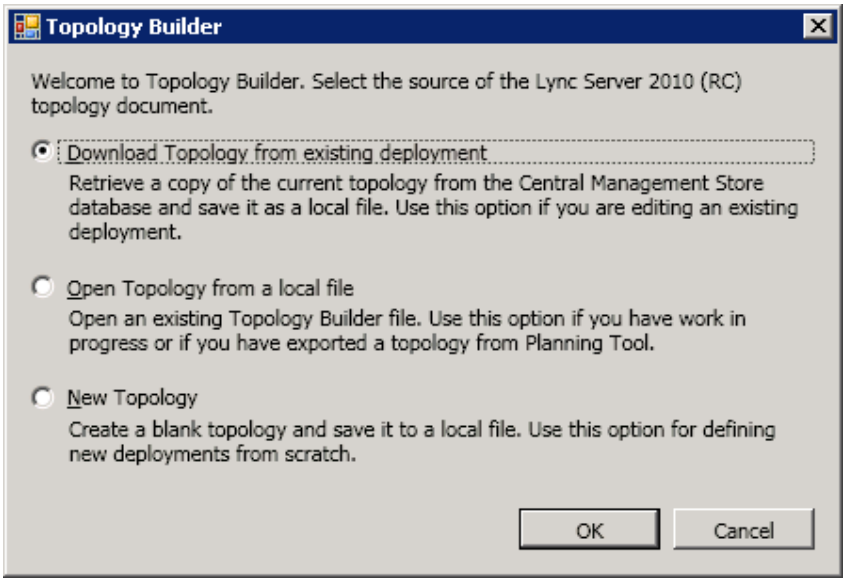
1. On the server where the Topology Builder is installed, start the Lync Server 2010 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder



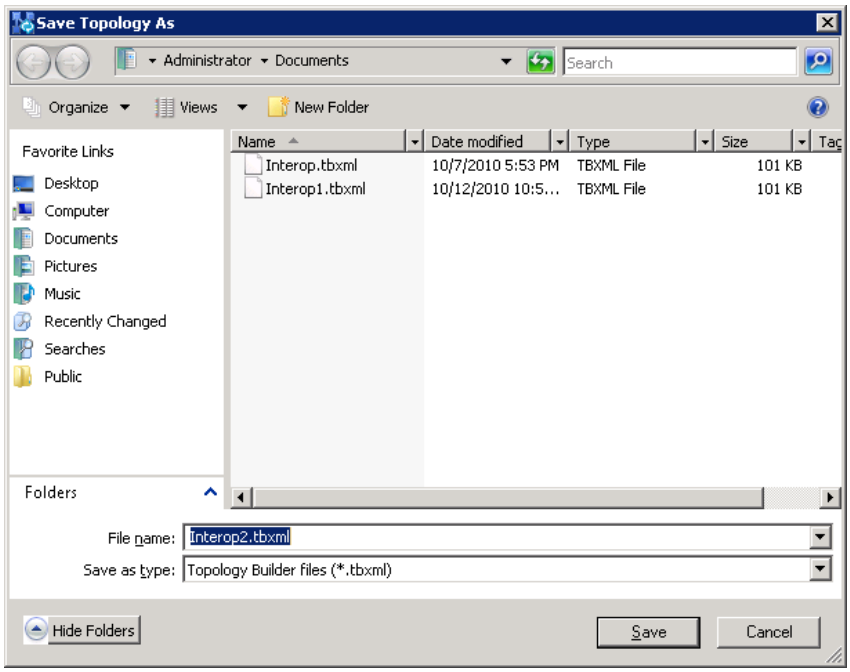
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

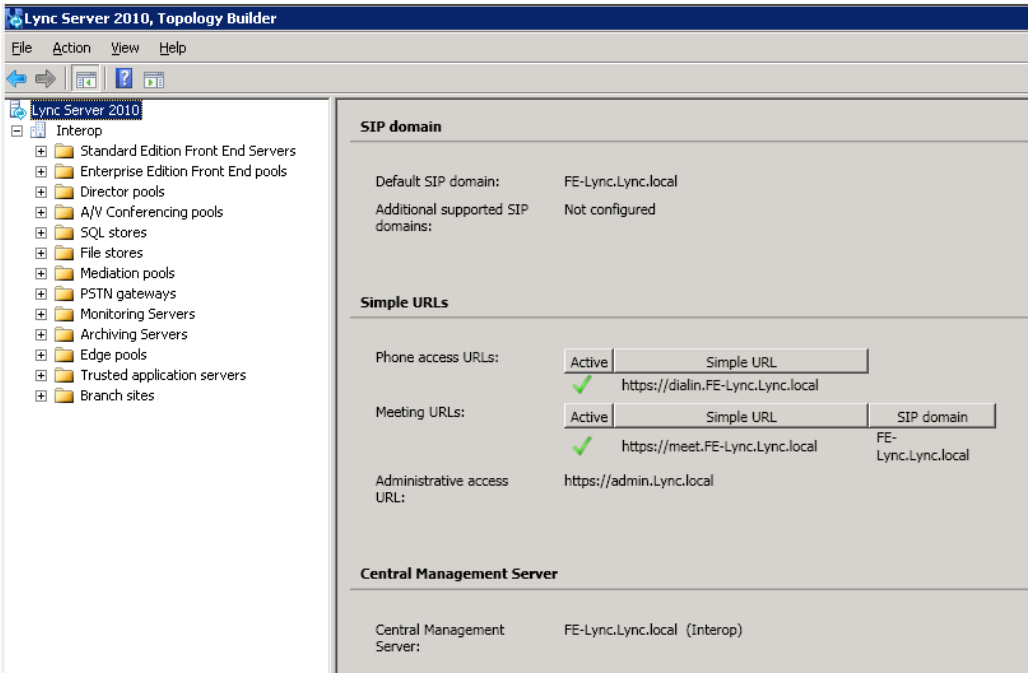
Figure 3-3: Save Topology Dialog Box



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

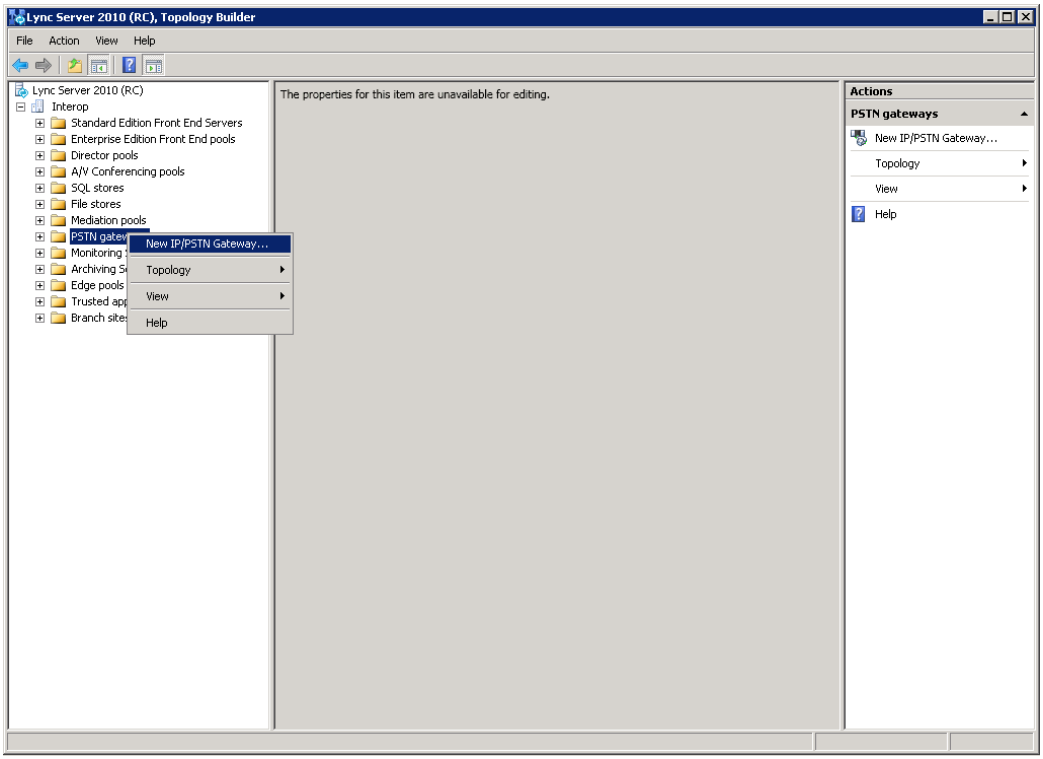
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



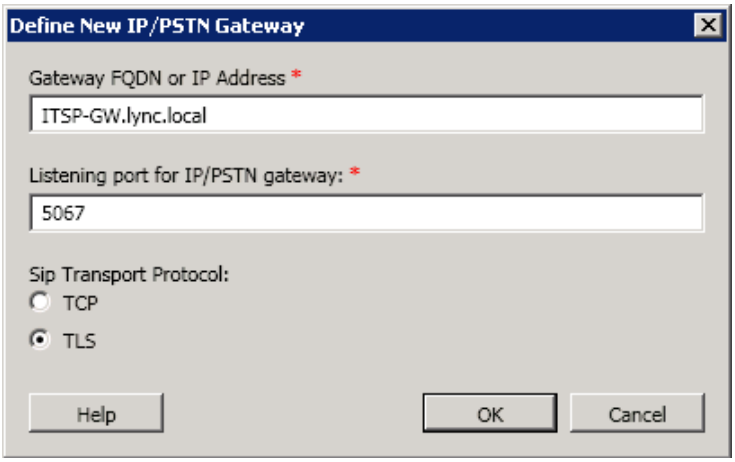
4. Expand the site tree located in the left pane.
5. Right-click the **PSTN gateways** folder, and then choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN

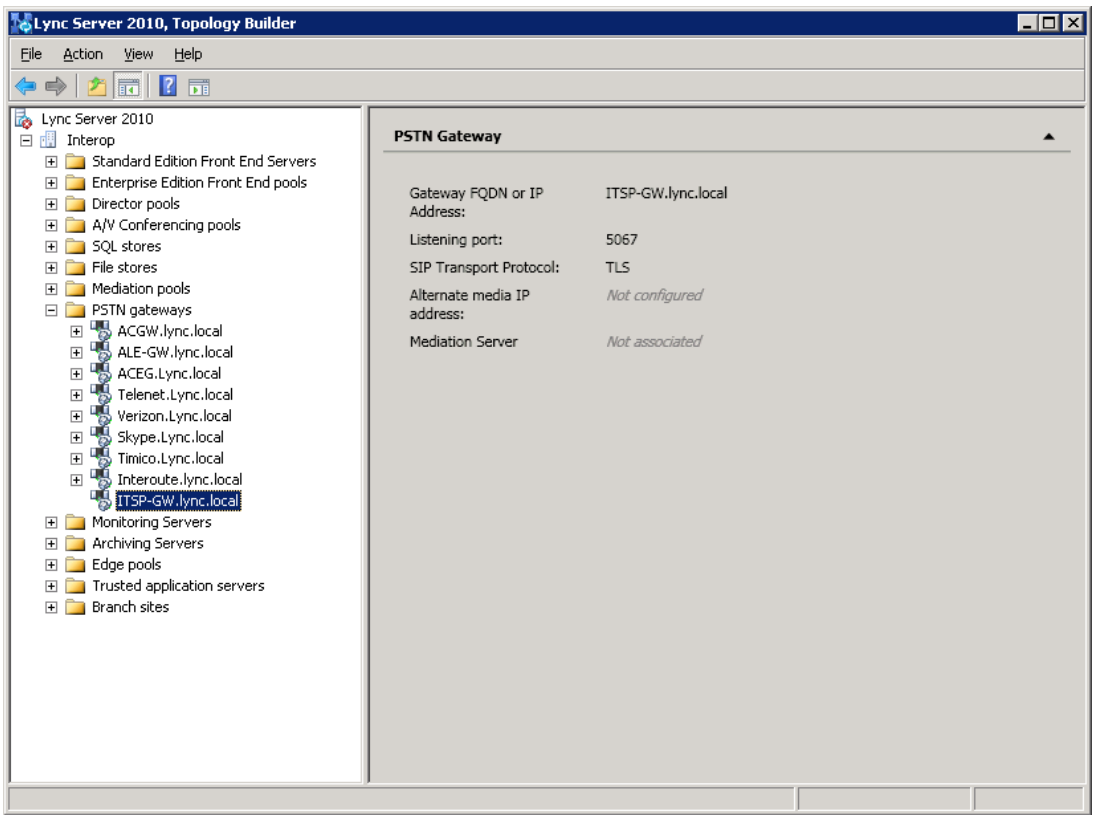


6. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP-GW.lync.local**). Update this FQDN in the relevant DNS record, and then click **OK**.

Note: The listening port for the Gateway is 5067 and the transport type is TLS.

The E-SBC is now added as an "IP/PSTN Gateway", as shown below:

Figure 3-7: E-SBC Added as an IP/PSTN Gateway



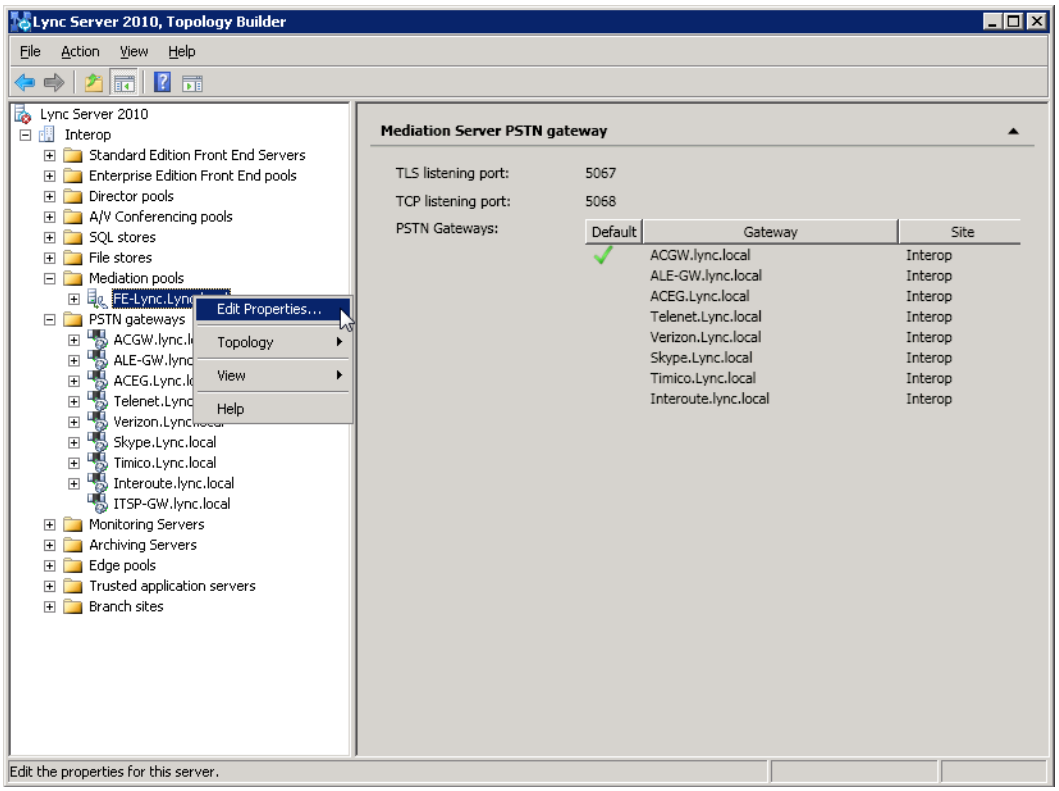
3.2 Associating IP / PSTN Gateway with Mediation Server

The procedure below describes how to associate the IP / PSTN Gateway with the Mediation Server.

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

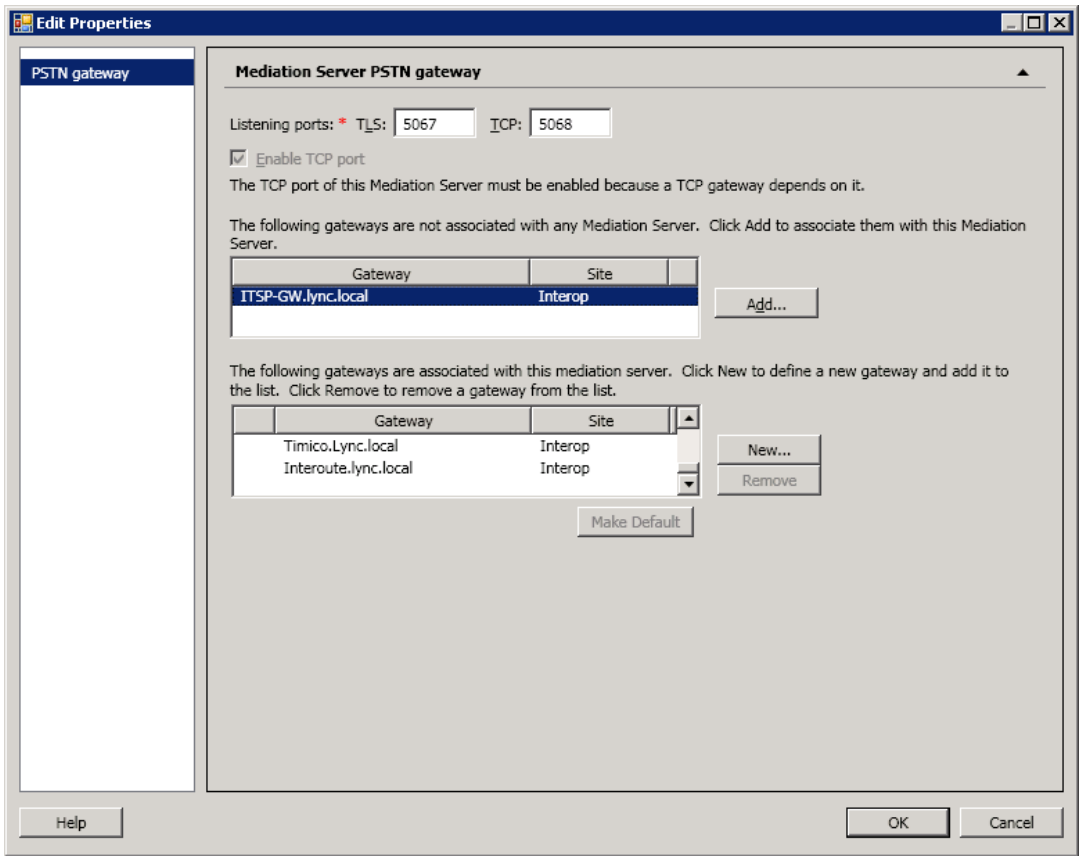
1. In the tree, right-click the Mediation Server that uses the E-SBC (e.g., **FE-Lync.Lync.local**), and then choose **Edit Properties**, as shown below:

Figure 3-8: Choosing Mediation Server



The following screen is displayed:

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

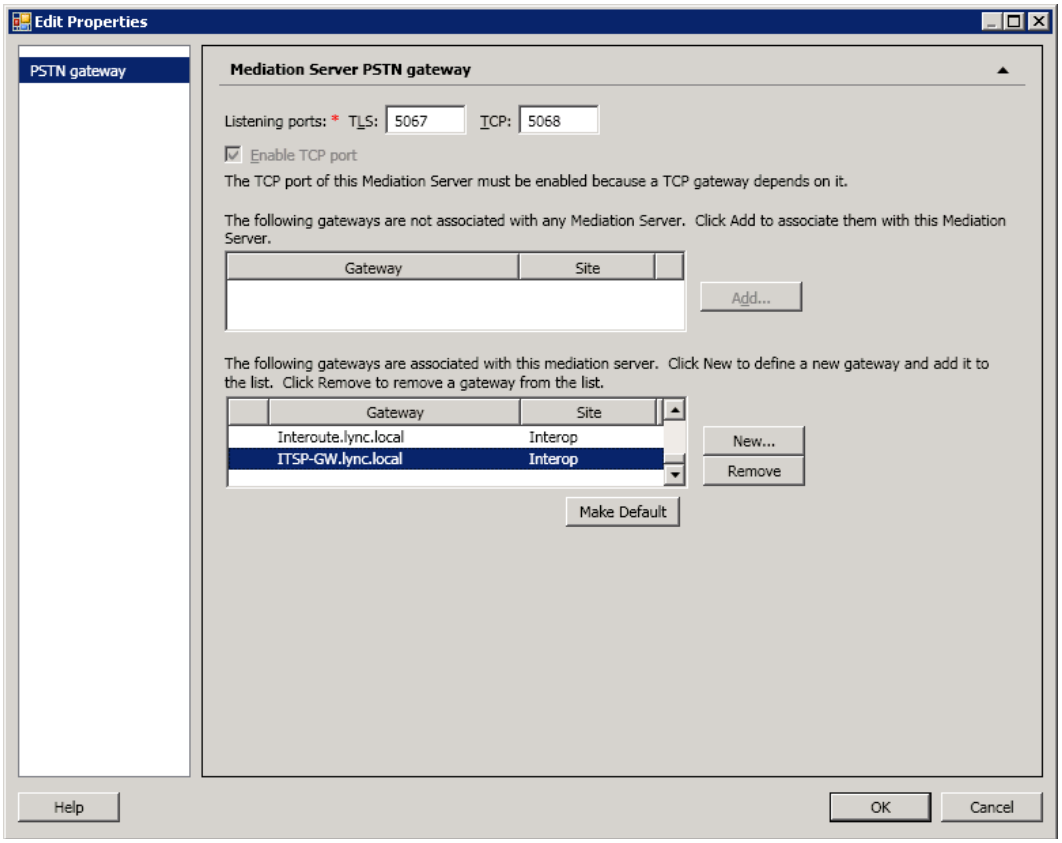


2. In the left pane, choose **PSTN gateway** to open the Mediation Server PSTN gateway pane, and then do the following:
   a. In the list of gateways that are not associated with the Mediation Server, select the E-SBC (e.g., **ITSP-GW.lync.local**).
   b. Click **Add** to associate it with the Mediation Server.

Note: There are two sub-panes; one lists the gateways not associated with the Mediation Server and one lists the gateways associated with the Mediation Server.

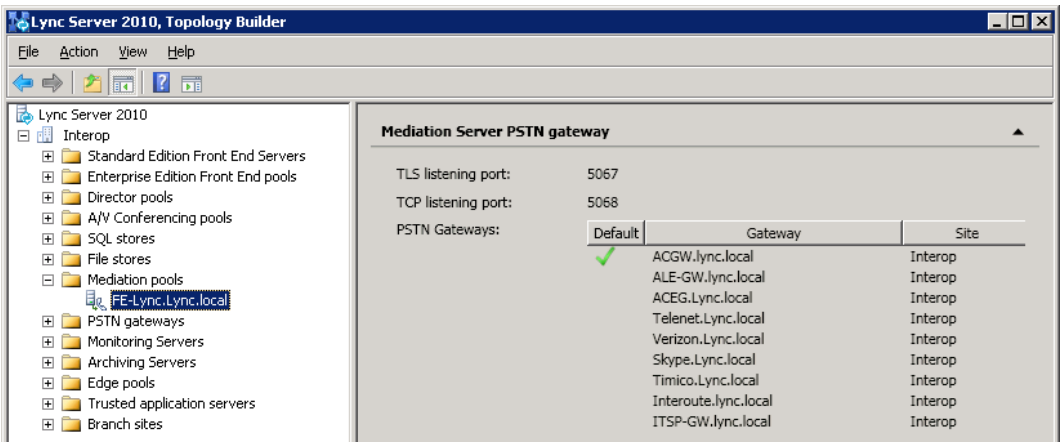
The E-SBC appears in the sub-pane that lists gateways associated with the Mediation Server, as shown below:

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



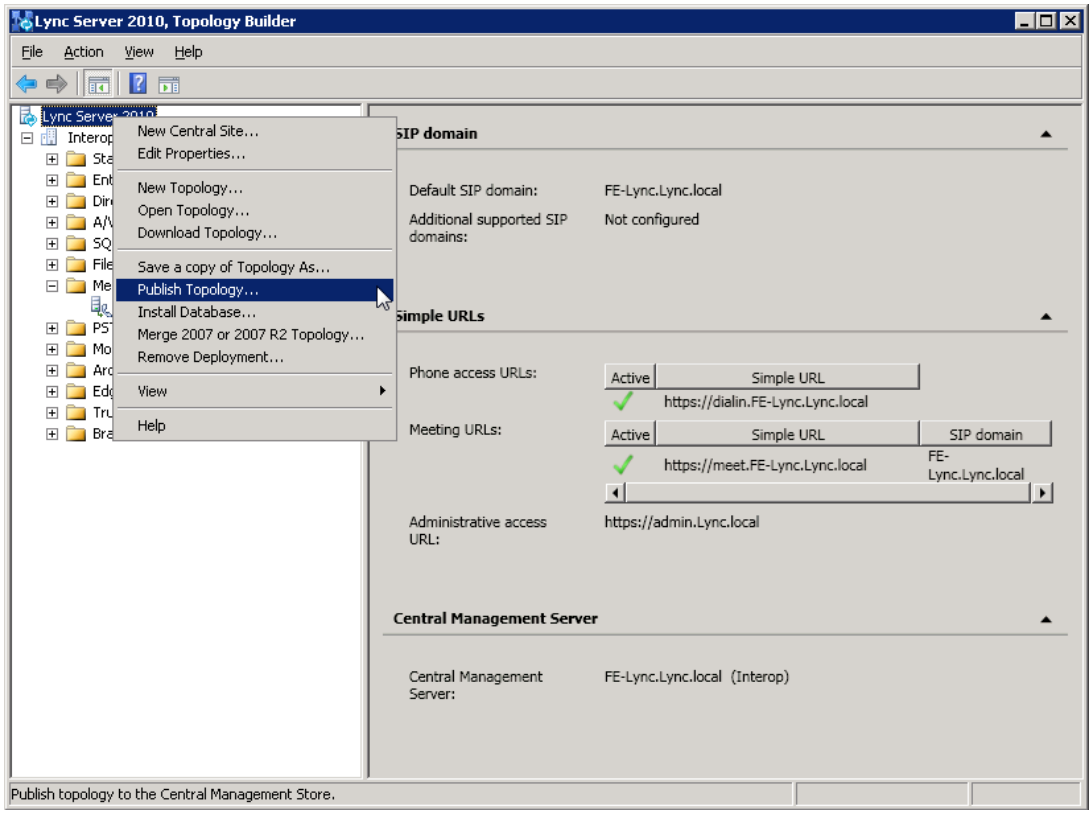
3. Click **OK**.

Figure 3-11: Media Server PSTN Gateway Association Properties



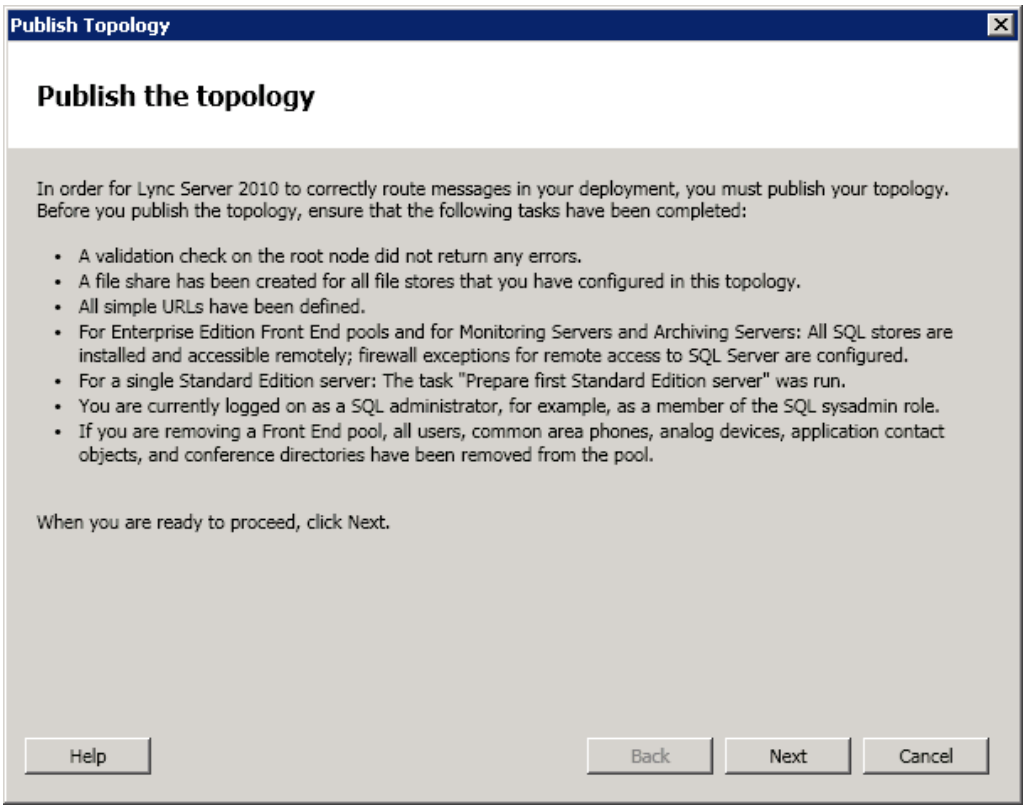
4. In the main tree, select the root item **Lync Server 2010**, and then from the **Action** menu on the menu bar, choose **Publish Topology**, as shown below:

Figure 3-12: Choosing Publish Topology



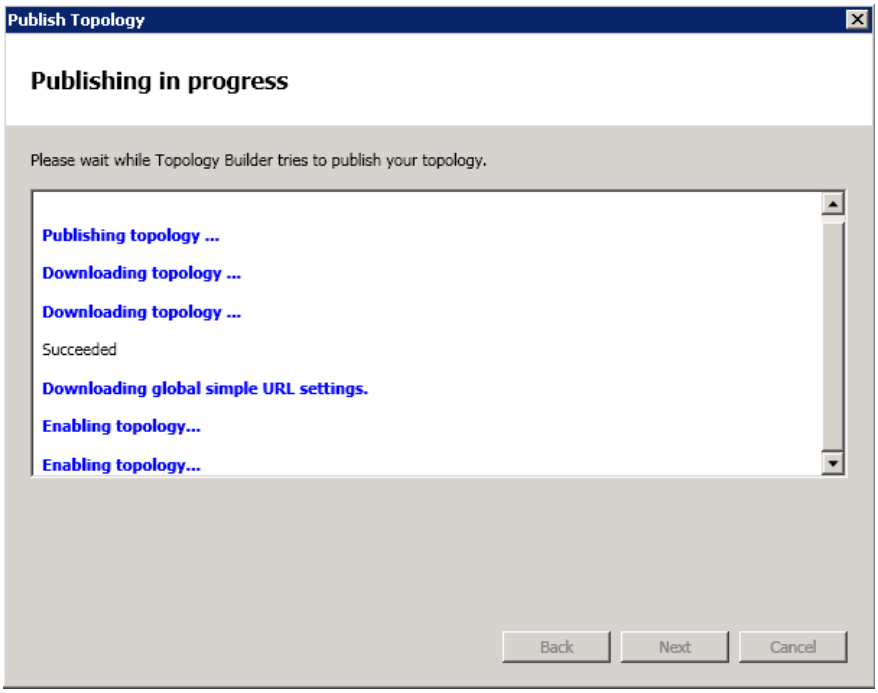
The Publish Topology screen is displayed:

Figure 3-13: Publish Topology Screen



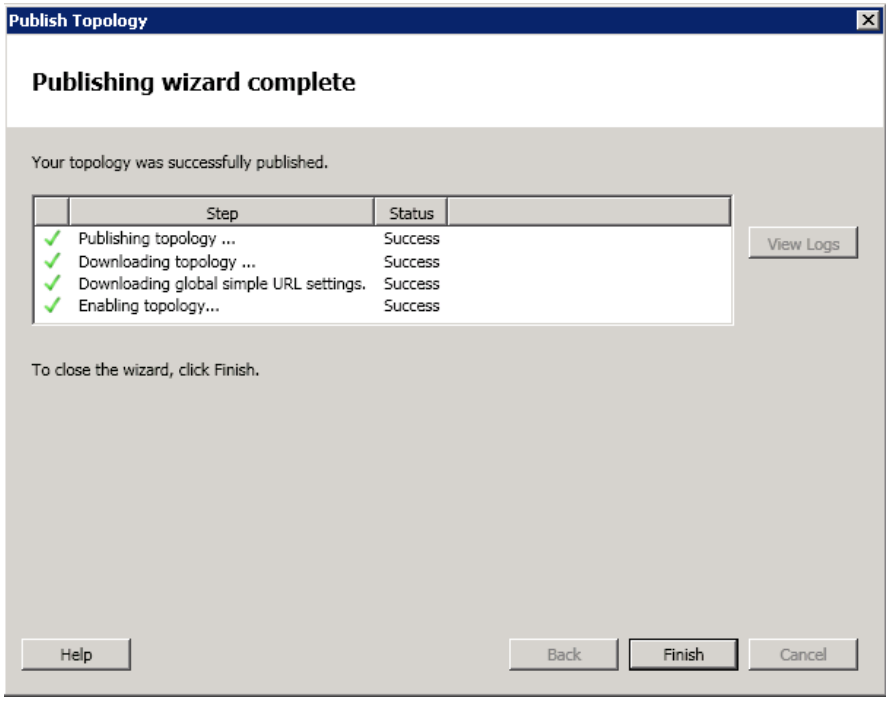
5. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-14: Publish Topology Progress Screen



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

Figure 3-15: Publish Topology Successfully Completed



7. Click **Finish**.

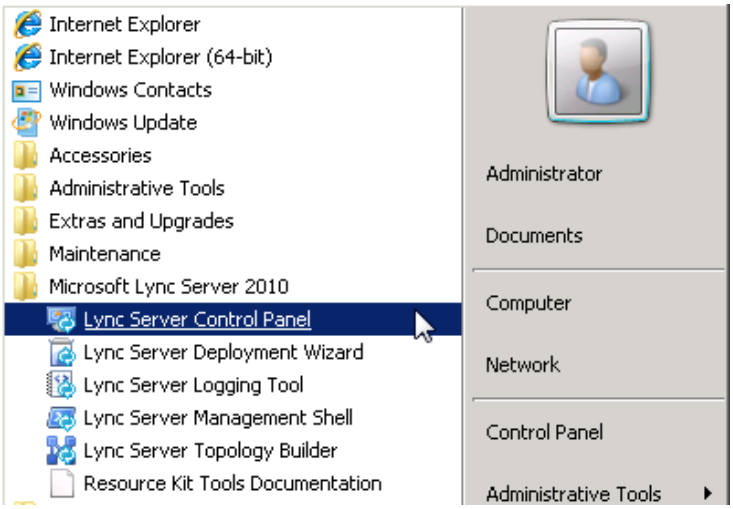
3.3 Configuring the "Route" on Lync Server 2010

The procedure below describes how to configure a "Route" on the Lync Server 2010 and to associate it with the E-SBC PSTN gateway.

➢ **To configure the "route" on Lync Server 2010:**

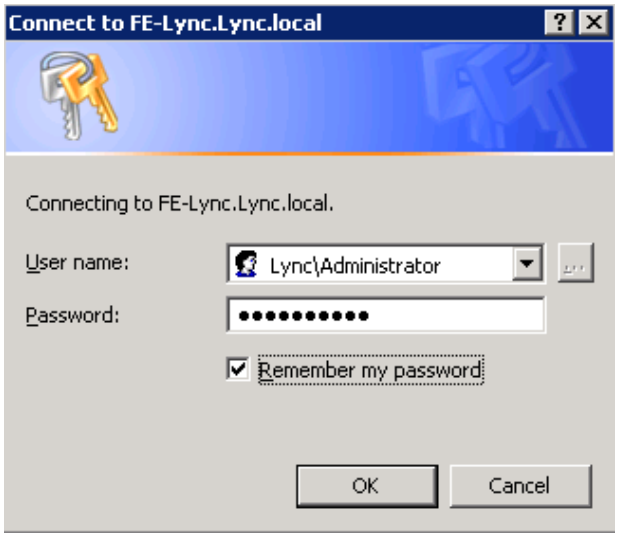
1. Start the Microsoft Lync Server 2010 Control Panel (**Start** > **All Programs** > **Microsoft Lync Server 2010** > **Lync Server Control Panel**), as shown below:

Figure 3-16: Opening the Lync Server Control Panel



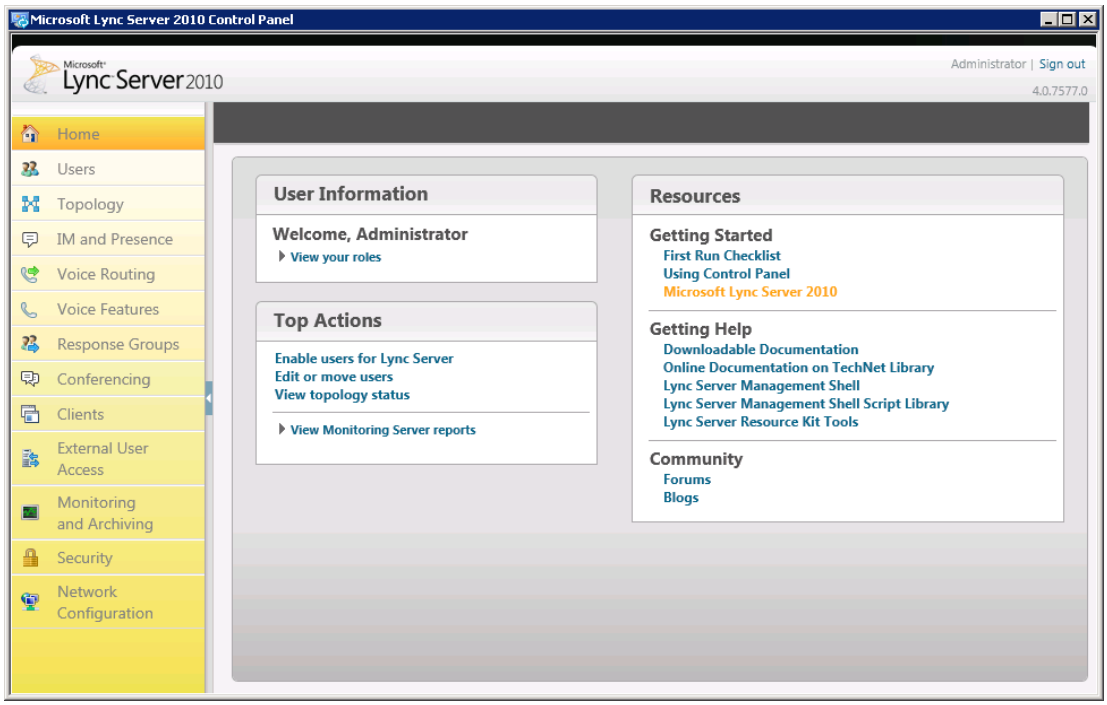
You are prompted to enter your login credentials:

Figure 3-17: Lync Server Credentials



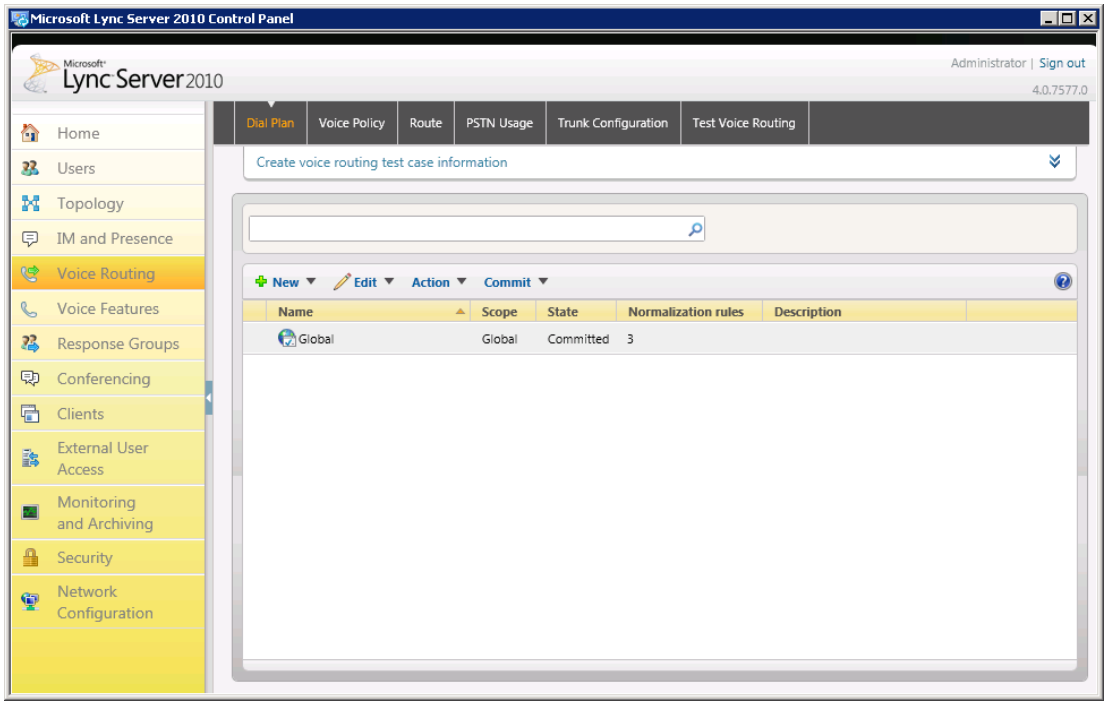
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2010 Control Panel is displayed:

Figure 3-18: Microsoft Lync Server 2010 Control Panel



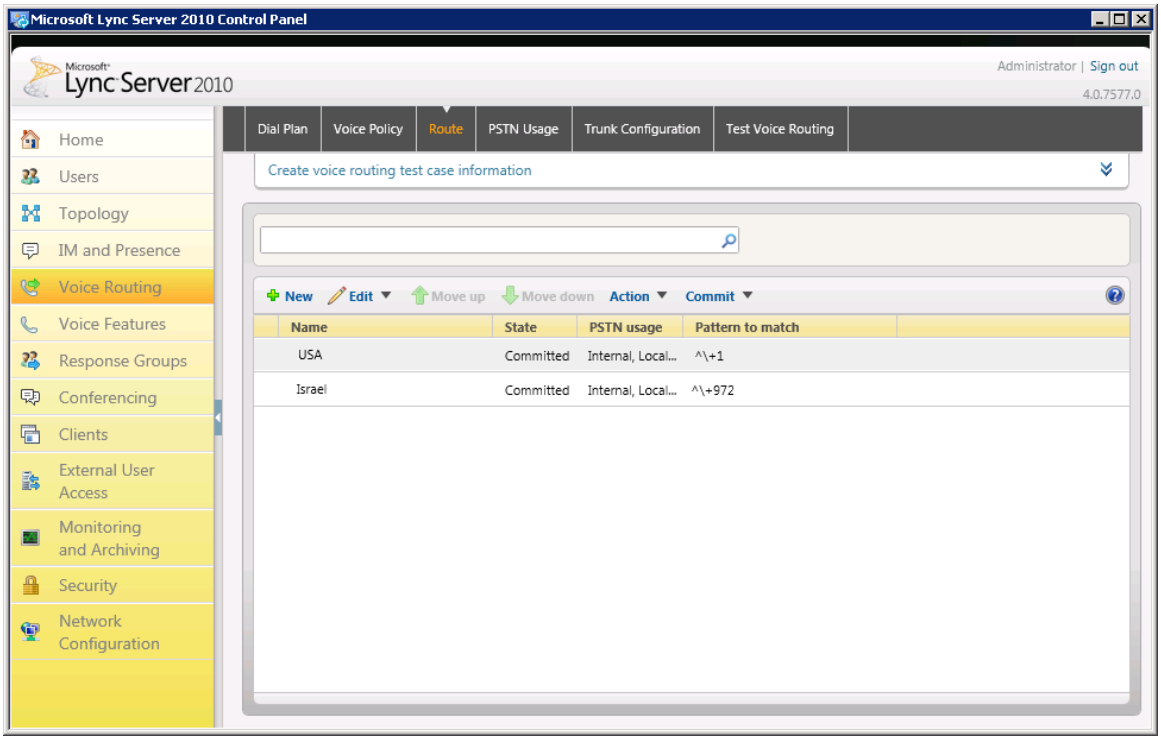
3. In the left navigation pane, select **Voice Routing**.

Figure 3-19: Voice Routing Page



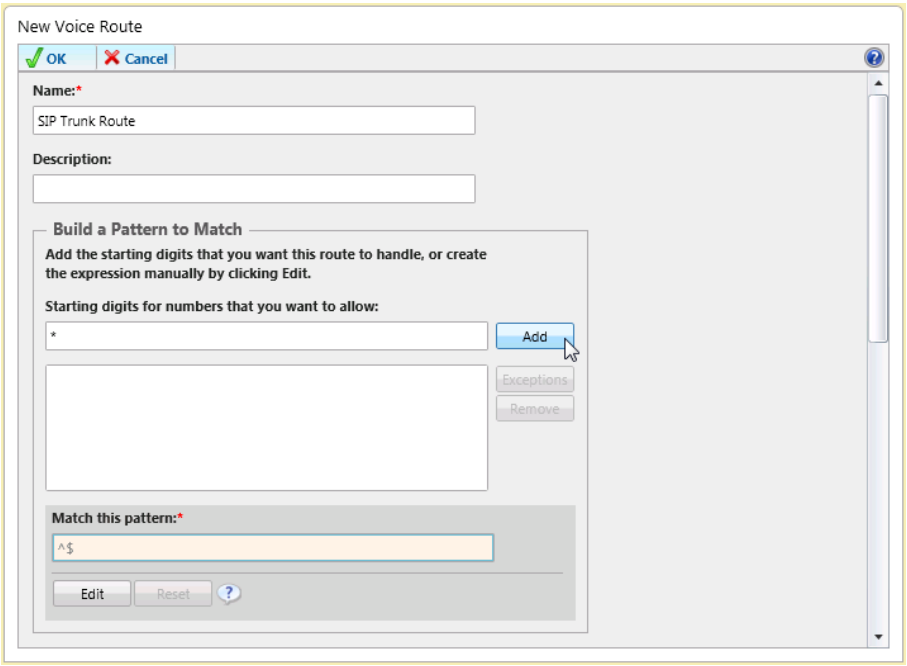
4. In the Voice Routing page, select the **Route** tab.

Figure 3-20: Route Tab



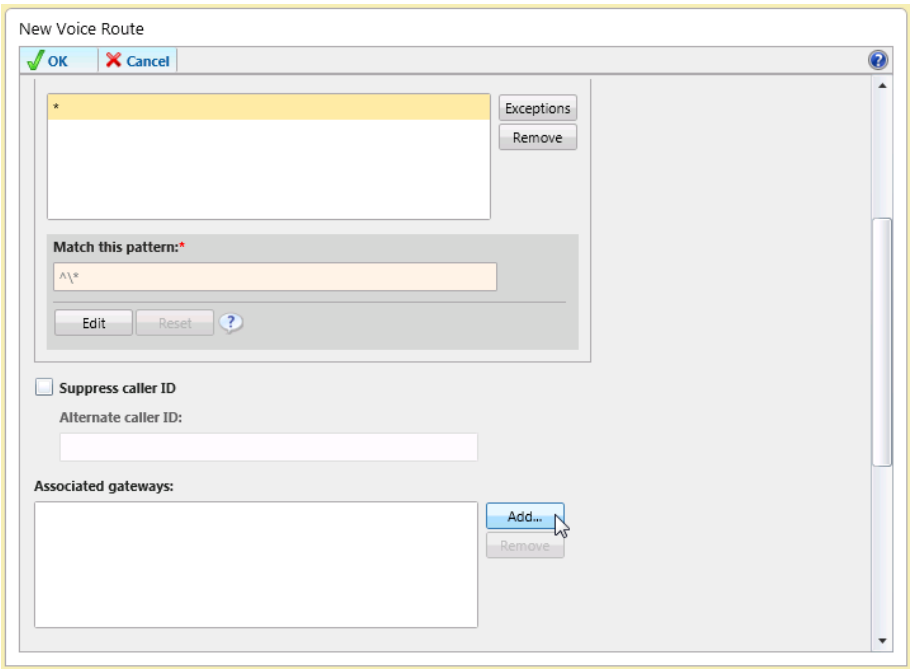
5. Click **New**; the New Voice Route page appears:

Figure 3-21: Adding New Voice Route



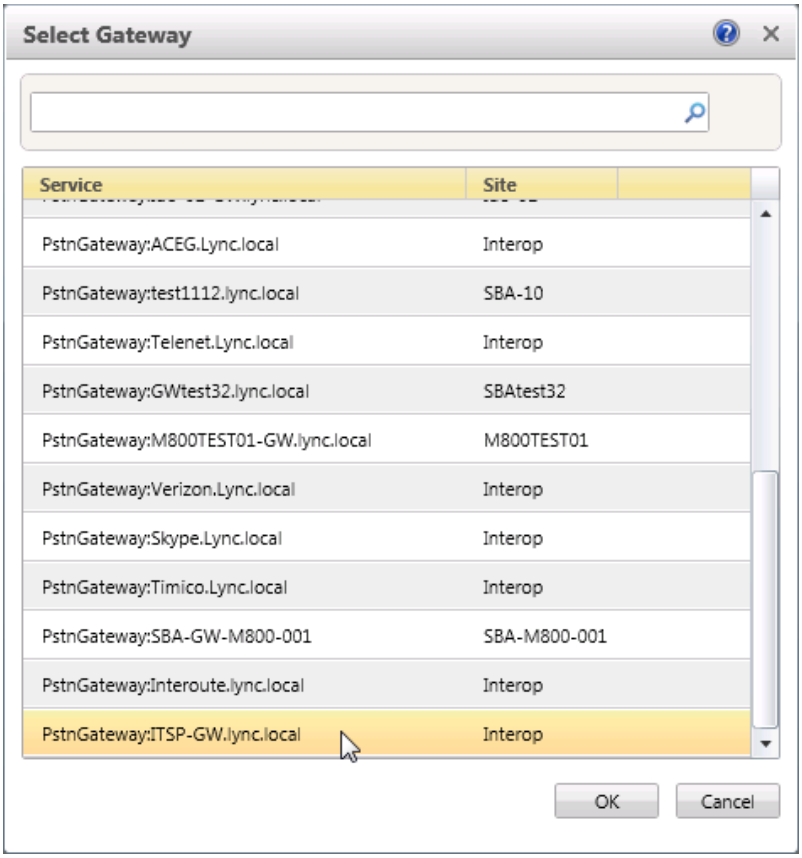
6. In the 'Name' field, enter a name for this route (e.g., **SIP Trunk Route**).
7. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., ***** to match all numbers), and then click **Add**.

Figure 3-22: Adding New E-SBC Gateway



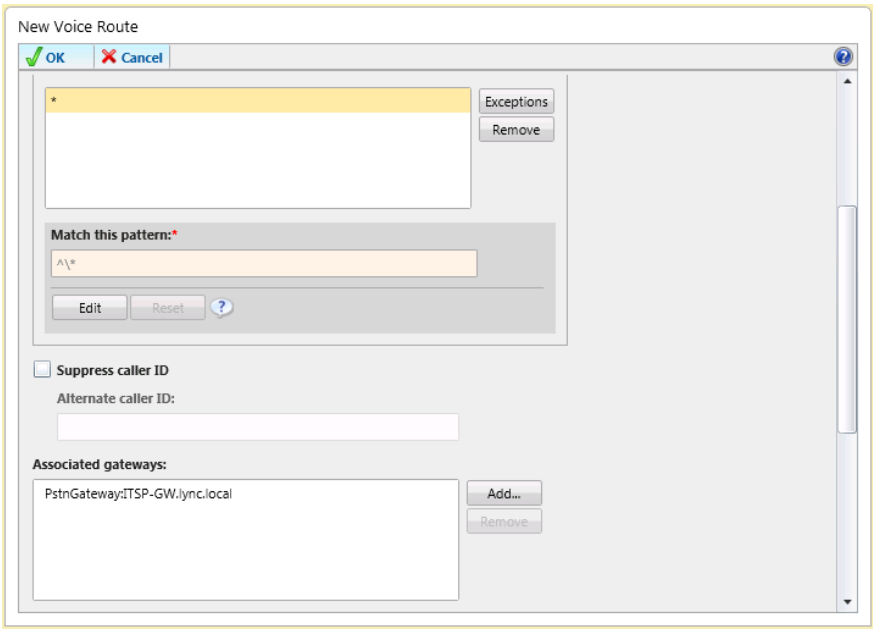
8. Associate the route with the E-SBC IP/PSTN gateway that you created:
   a. Under the 'Associated Gateway' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-23: List of Deployed Trunks



   b. Select the E-SBC Gateway you created, and then click **OK**.

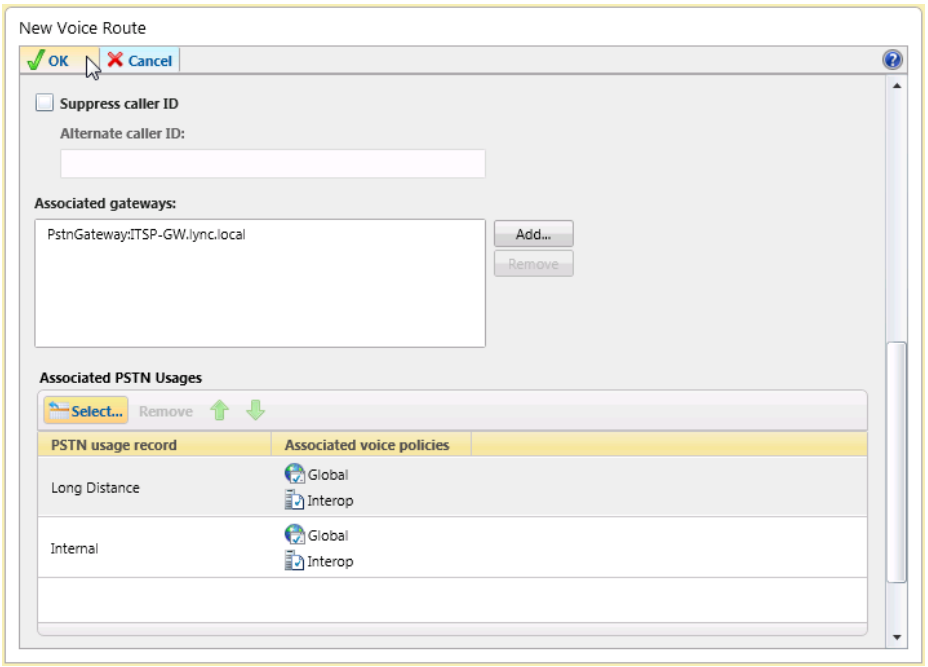
Figure 3-24: Selected E-SBC Trunk



9. Associate a PSTN Usage to this route:

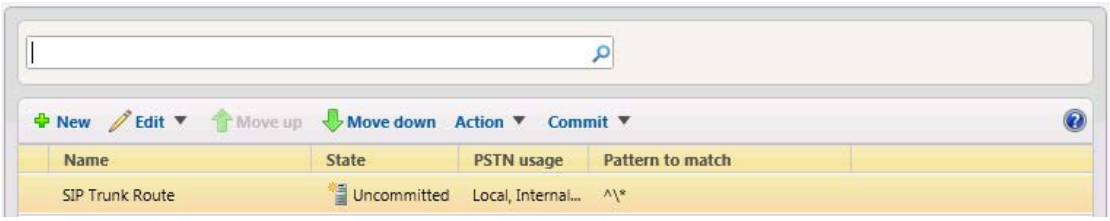
a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

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



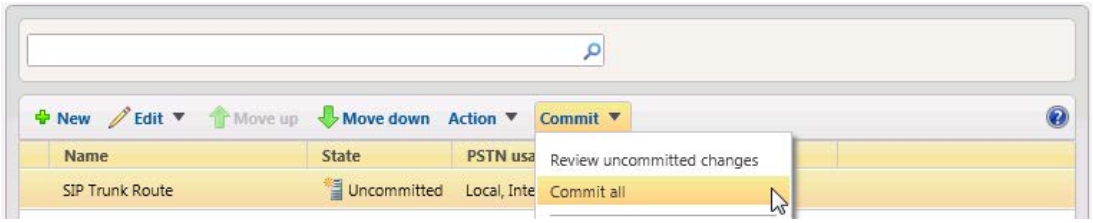
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-26: Confirmation of New Voice Route



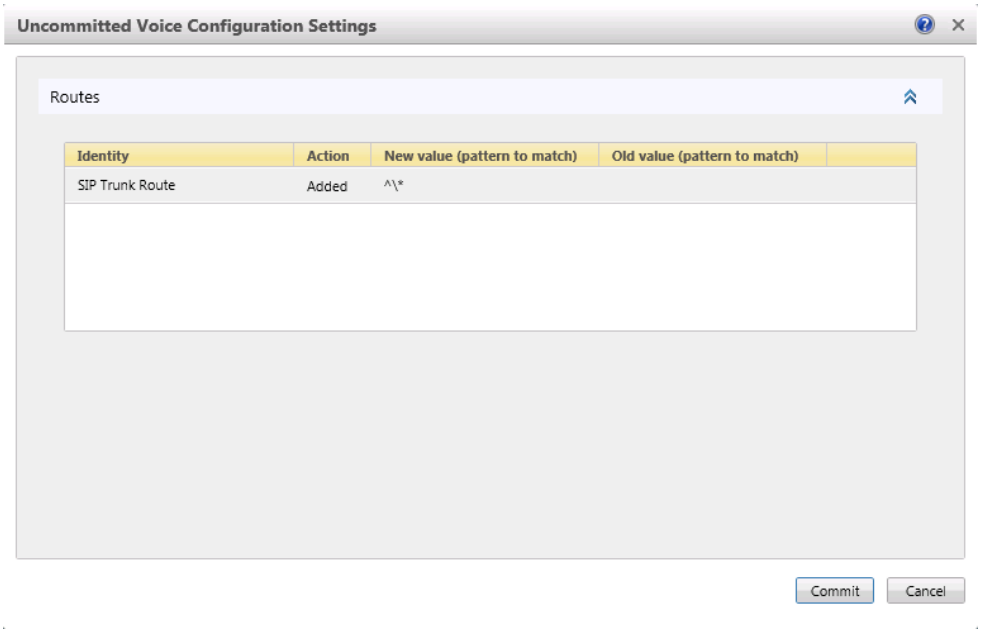
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-27: Committing Voice Routes



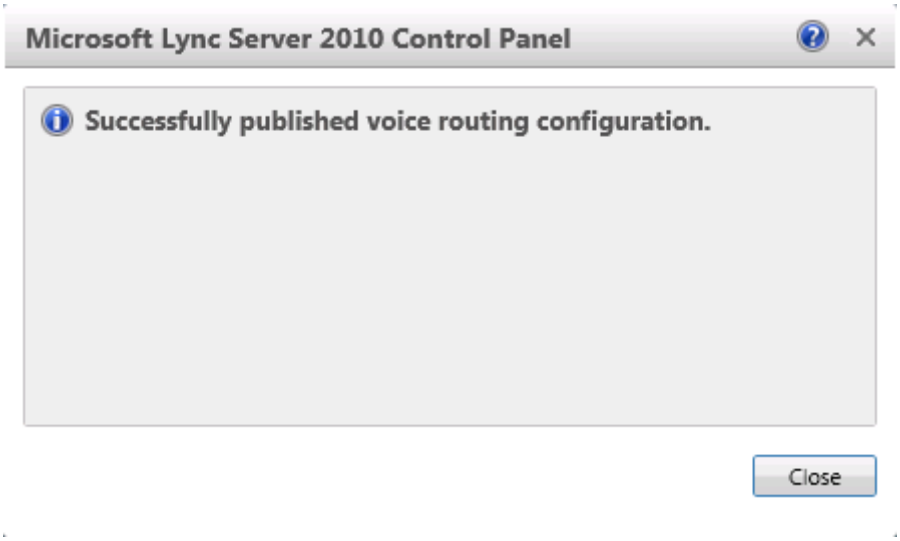
The Uncommitted Voice Configuration Settings page appears:

Figure 3-28: Uncommitted Voice Configuration Settings



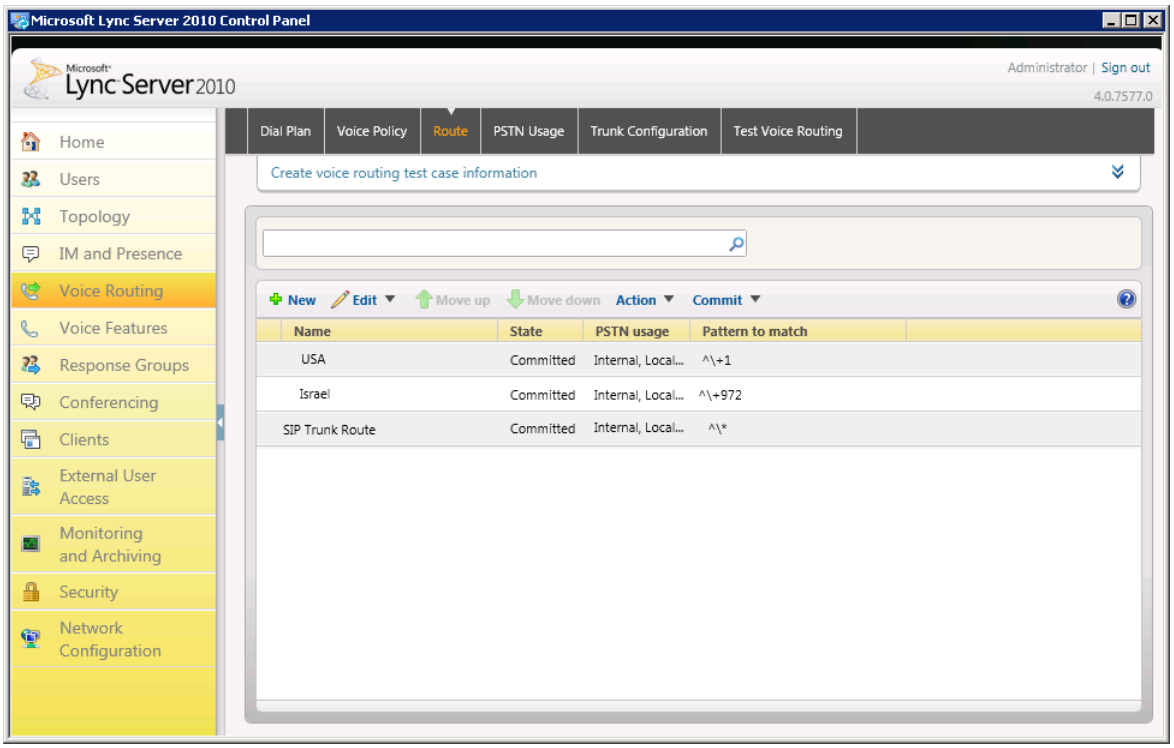
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-29: Confirmation of Successful Voice Routing Configuration



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

Figure 3-30: Voice Routing Screen Displaying Committed Routes



Reader's Notes

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2010 and the Bell Canada SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

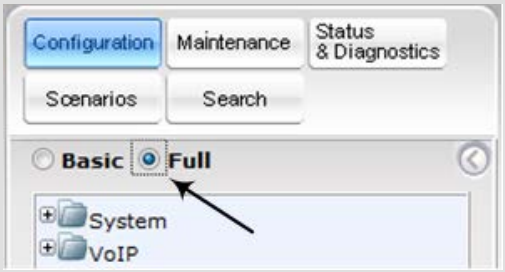
- E-SBC WAN interface - Bell Canada SIP Trunking environment
- E-SBC LAN interface - Lync Server 2010 environment

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

Notes:

- For implementing Microsoft Lync and Bell Canada SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

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



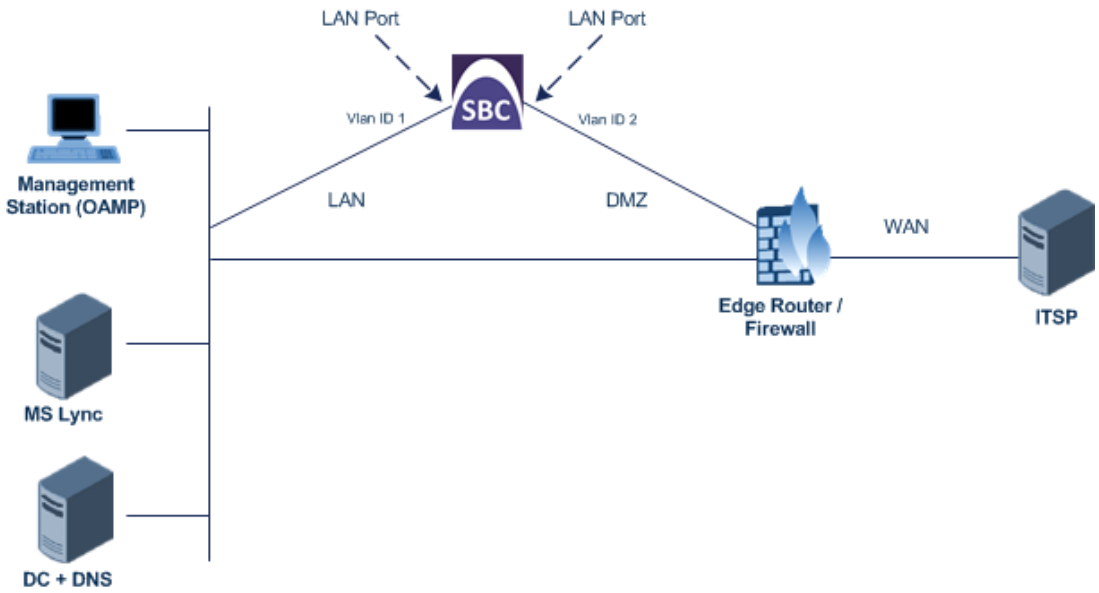
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

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

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

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure Network Interfaces

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

- LAN VoIP (assigned the name "Lync")
- WAN VoIP (assigned the name "BellCanada")

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

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

Parameter	Value
IP Address	**10.15.17.70** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Lync** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.21.10**
Underlying Interface	**GROUP_1** (Ethernet port group)

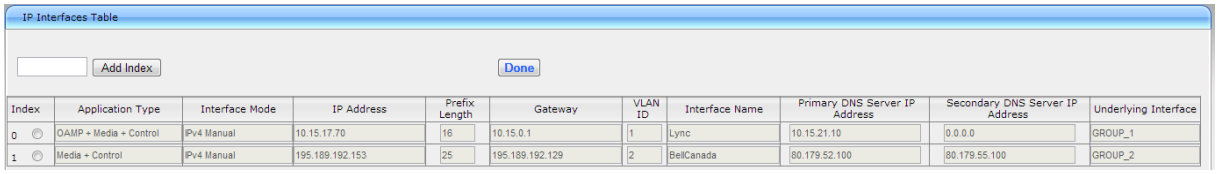
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.189.192.153** (WAN IP address)
Prefix Length	**25** (for 255.255.255.128)
Gateway	**195.189.192.129** (router's IP address)
VLAN ID	**2**
Interface Name	**BellCanada**
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Interface	**GROUP_2**

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

The configured IP network interfaces are shown below:

Figure 4-2: Configured Network Interfaces in IP Interfaces Table



IP Interfaces Table

Add Index | Done

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	IPv4 Manual	10.15.17.70	16	10.15.0.1	1	Lync	10.15.21.10	0.0.0.0	GROUP_1
1	Media + Control	IPv4 Manual	195.189.192.153	25	195.189.192.129	2	BellCanada	80.179.52.100	80.179.55.100	GROUP_2

4.1.2 Step 1b: Configure the Native VLAN ID

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

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

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

Figure 4-3: Configured Port Native VLAN

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
2	GE_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
3	GE_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
4	GE_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

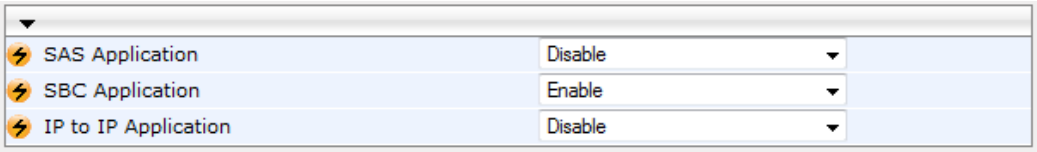
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.16 on page 71).

4.3 Step 3: Signaling Routing Domains Configuration

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

The SRD is composed of the following:

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

4.3.1 Step 3a: Configure Media Realms

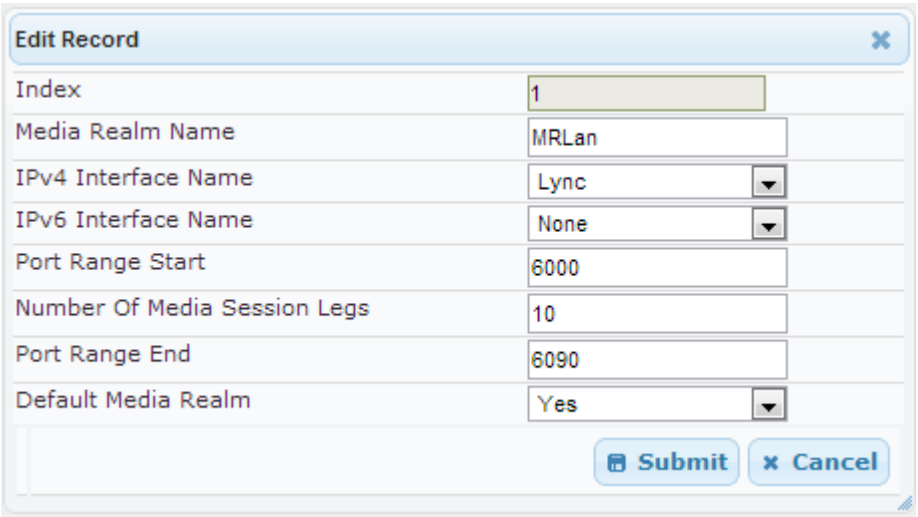
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

Parameter	Value
Index	**1**
Media Realm Name	**MRLan** (descriptive name)
IPv4 Interface Name	**Lync**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

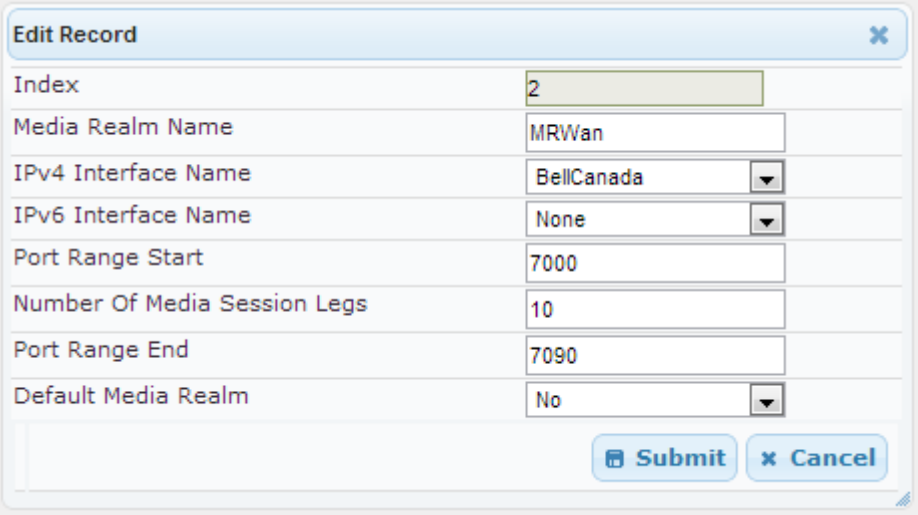
Figure 4-5: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

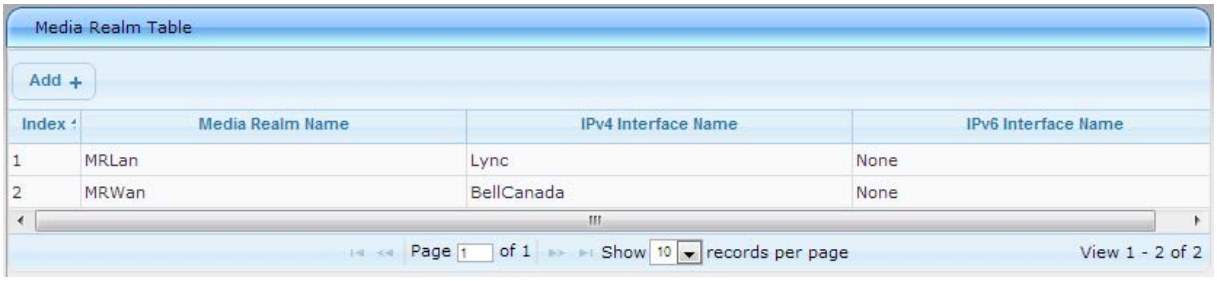
Parameter	Value
Index	**2**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**BellCanada**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-7: Configured Media Realms in Media Realm Table



4.3.2 Step 3b: Configure SRDs

This step describes how to configure the SRDs.

➢ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **Control Network** > **SRD Table**).
2. Configure an SRD for the E-SBC's internal interface (toward Lync Server 2010):

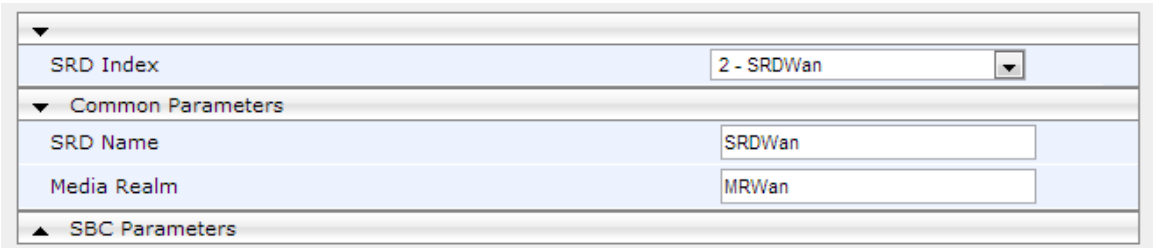
Parameter	Value
SRD Index	**1**
SRD Name	**SRDLan** (descriptive name for SRD)
Media Realm	**MRLan** (associates SRD with Media Realm)

Figure 4-8: Configuring LAN SRD

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

Parameter	Value
SRD Index	**2**
SRD Name	**SRDWan**
Media Realm	**MRWan**

Figure 4-9: Configuring WAN SRD



4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

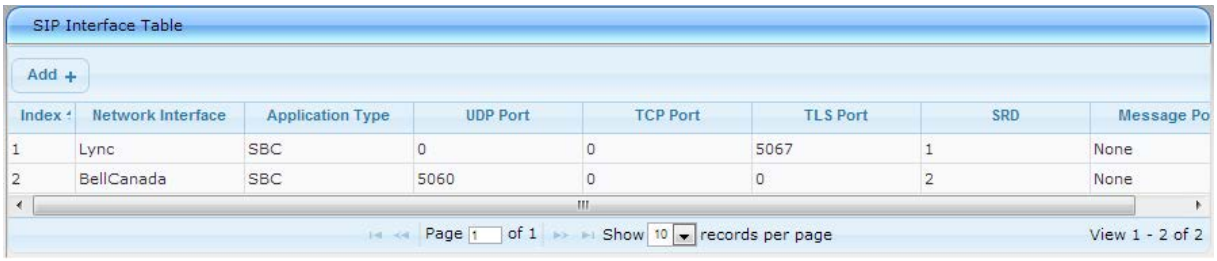
Parameter	Value
Index	**1**
Network Interface	**Lync**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**1**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
Network Interface	**BellCanada**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0**
SRD	**2**

The configured SIP Interfaces are shown in the figure below:

Figure 4-10: Configured SIP Interfaces in SIP Interface Table



4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Lync Server 2010
- Bell Canada SIP Trunk

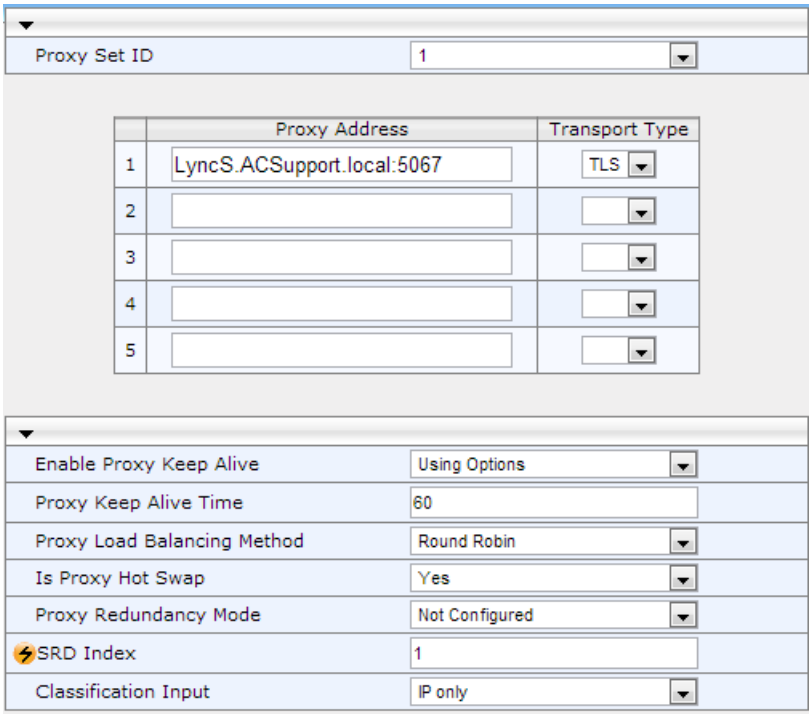
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for Lync Server 2010:

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**LyncS.ACSupport.local:5067** (Lync Server 2010 IP address / FQDN and destination port)
Transport Type	**TLS**
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
SRD Index	**1**

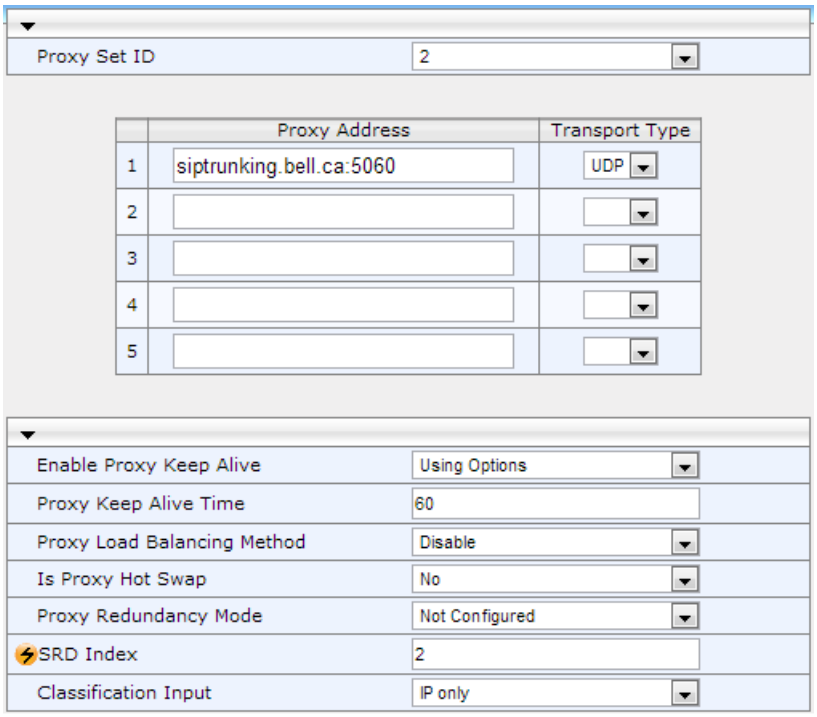
Figure 4-11: Configuring Proxy Set for Microsoft Lync Server 2010



3. Configure a Proxy Set for the Bell Canada SIP Trunk:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**Siptrunking.bell.ca:5060** (Bell Canada IP address / FQDN and destination port)
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**No**
SRD Index	**2** (enables classification by Proxy Set for SRD of IP Group belonging to Bell Canada SIP Trunk)

Figure 4-12: Configuring Proxy Set for Bell Canada SIP Trunk



4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.16 on page 71).

4.5 Step 5: Configure IP Groups

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

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

- Lync Server 2010 (Mediation Server) located on LAN
- Bell Canada SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Configure an IP Group for the Lync Server 2010 Mediation Server:

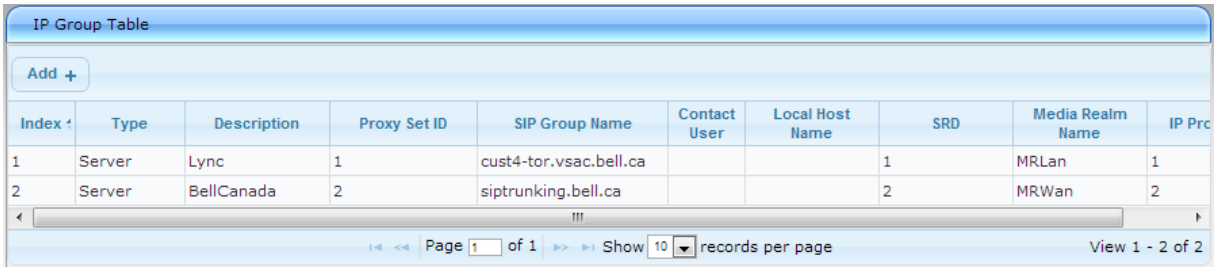
Parameter	Value
Index	**1**
Type	**Server**
Description	**Lync** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**cust4-tor.vsac.bell.ca**
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

3. Configure an IP Group for the Bell Canada SIP Trunk:

Parameter	Value
Index	**2**
Type	**Server**
Description	**BellCanada** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**siptrunking.bell.ca**
SRD	**2**
Media Realm Name	**MRWan**
IP Profile ID	**2**

The configured IP Groups are shown in the figure below:

Figure 4-13: Configured IP Groups in IP Group Table



4.6 Step 6: Configure IP Profiles

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

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

- Microsoft Lync Server 2010 - to operate in secure mode using SRTP and TLS
- Bell Canada SIP trunk - to operate in non-secure mode using RTP and UDP

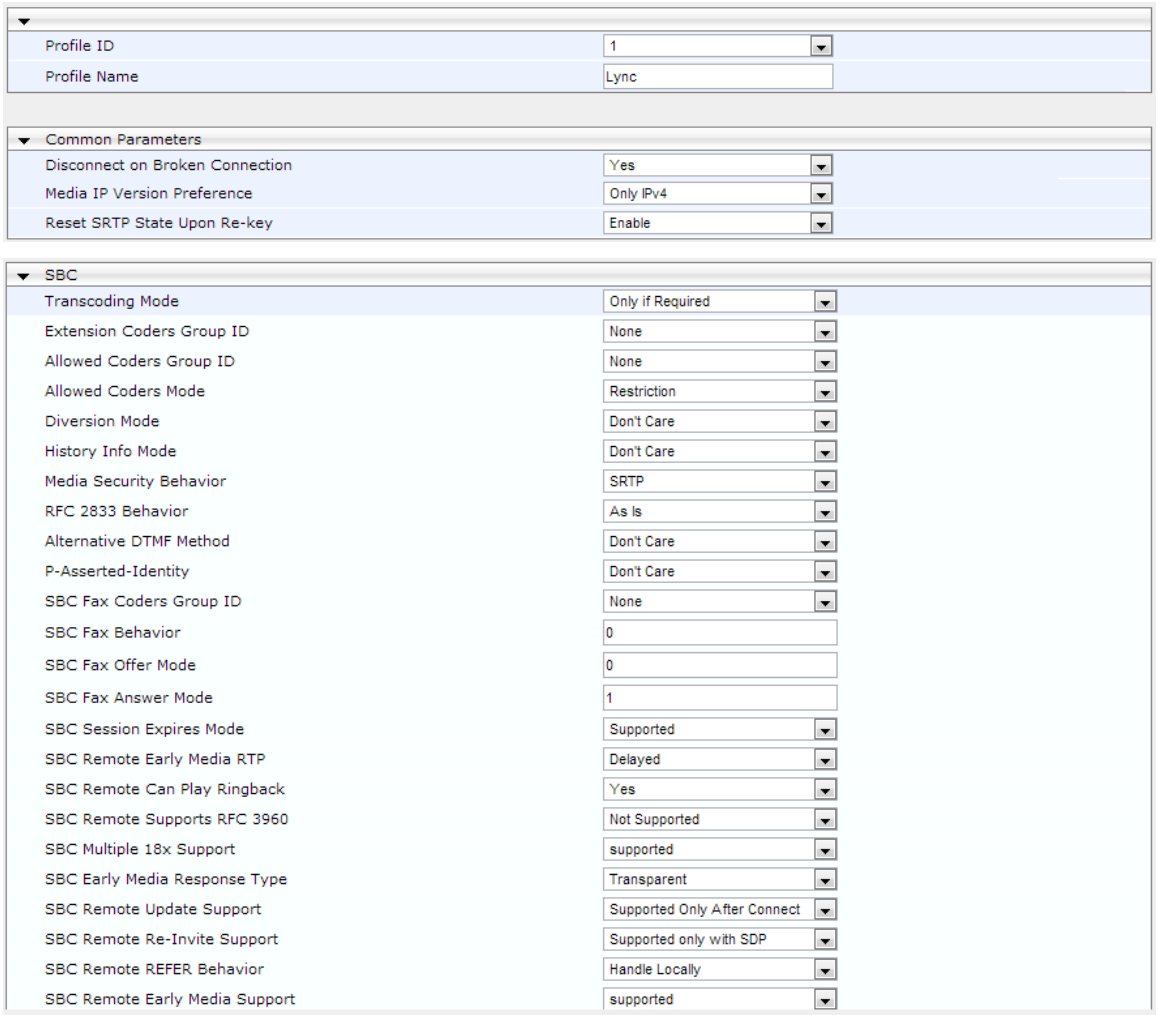
Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 42).

➢ **To configure IP Profiles:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Configure an IP Profile for Lync Server 2010:

Parameter	Value
Profile ID	**1**
Reset SRTP State Upon Re-key	**Enable**
Extension Coders Group ID	**Coders Group 1**
Media Security Behavior	**SRTP**
SBC Session Expires Mode	**Supported**
SBC Remote Early Media RTP	**Delayed** (required, as Lync Server 2010 does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Remote Update Support	**Supported Only After Connect**
SBC Remote Re-Invite Support	**Supported Only With SDP**
SBC Remote Refer Behavior	**Handle Locally** (required, as Lync Server 2010 does not support receipt of SIP REFER)
SBC Remote 3xx Behavior	**Handle Locally** (required, as Lync Server 2010 does not support receipt of SIP 3xx responses)
SBC Remote Delayed Offer Support	**Not Supported**

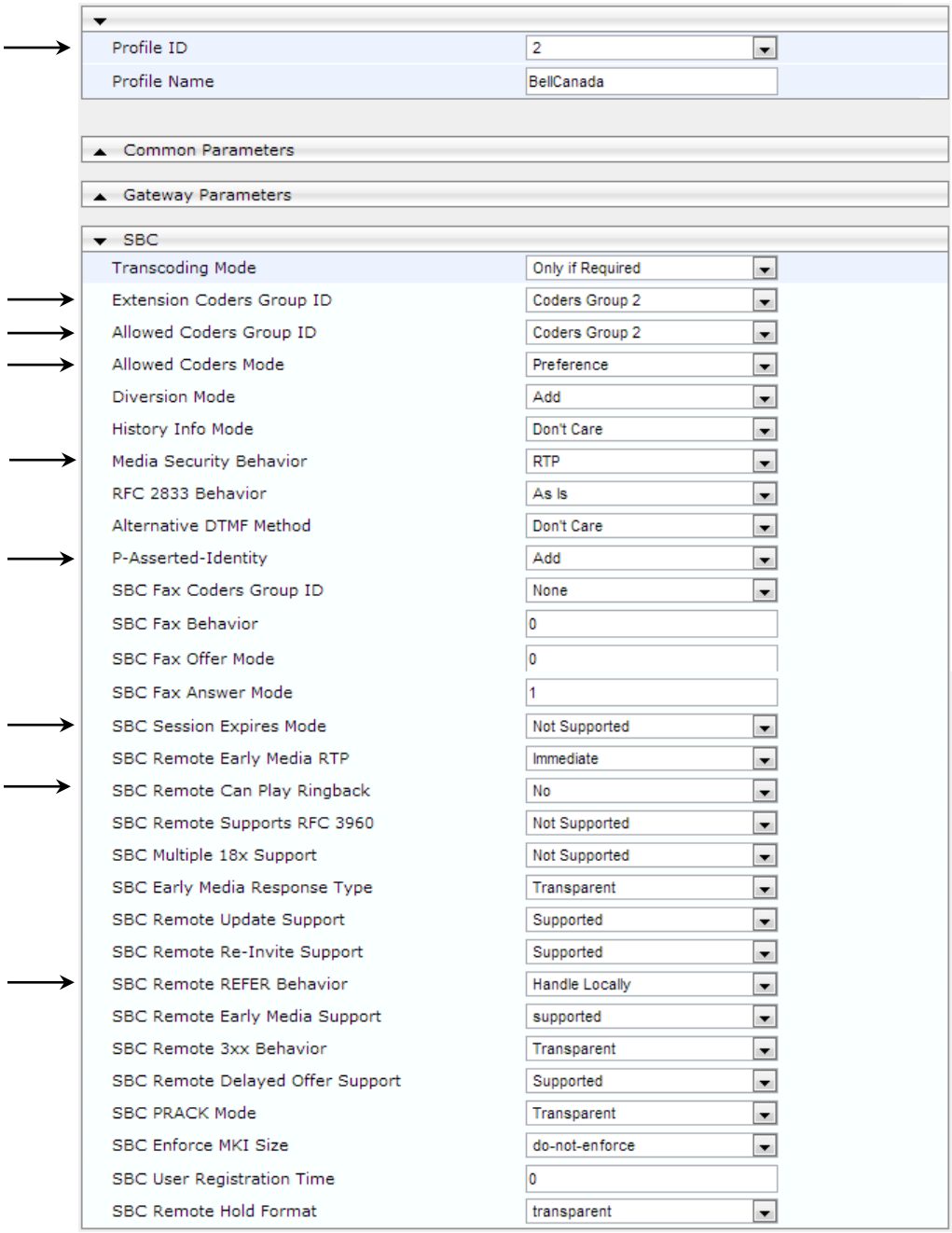
Figure 4-14: Configuring IP Profile for Lync Server 2010



3. Configure an IP Profile for the Bell Canada SIP Trunk:

Parameter	Value
Profile ID	**2**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Preference** (lists Allowed Coders first and then original coders in received SDP offer)
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** (required for anonymous calls)
SBC Session Expires Mode	**Not Supported**
SBC Remote Can Play Ringback	**No** (required, as Lync Server 2010 does not provide a ringback tone for incoming calls)
SBC Remote Refer Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)

Figure 4-15: Configuring IP Profile for Bell Canada SIP Trunk



4.7 Step 7: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Lync Server 2010 supports the G.711 coder while the network connection to Bell Canada SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the Bell Canada SIP Trunk.

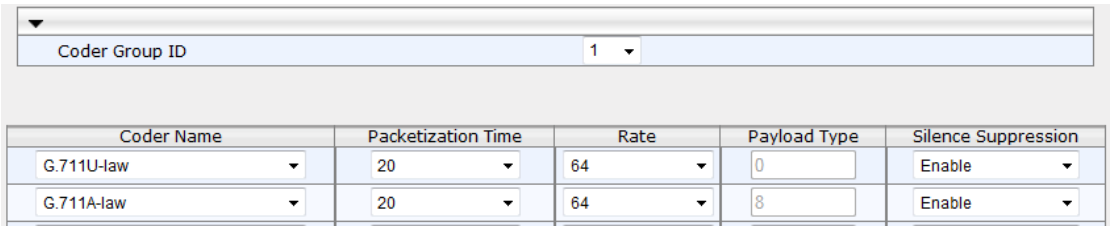
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 44).

➢ **To configure coders:**

1. Open the Coder Group Settings (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**).
2. Configure a Coder Group for Lync Server 2010:

Parameter	Value
Coder Group ID	**1**
Coder Name	▪ **G.711 U-law** ▪ **G.711 A-law**
Silence Suppression	**Enable** (for both coders)

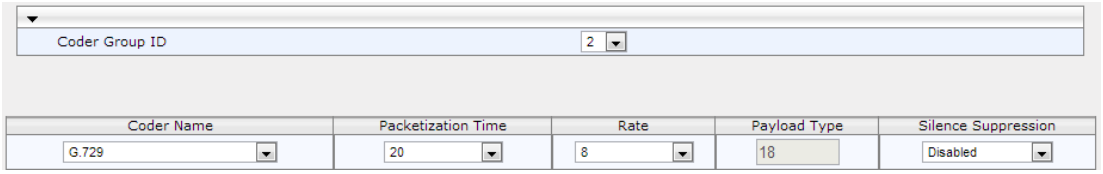
Figure 4-16: Configuring Coder Group for Lync Server 2010



3. Configure a Coder Group for Bell Canada SIP Trunk:

Parameter	Value
Coder Group ID	**2**
Coder Name	**G.729**

Figure 4-17: Configuring Coder Group for Bell Canada SIP Trunk



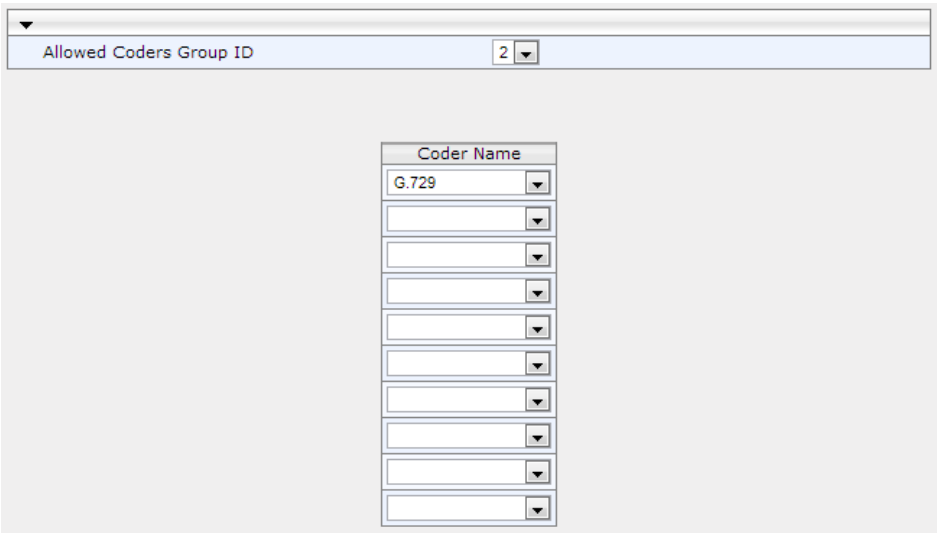
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Bell Canada SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Bell Canada SIP Trunk in the previous step (see Section 4.6 on page 44).

➢ **To set a preferred coder for the Bell Canada SIP Trunk:**

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

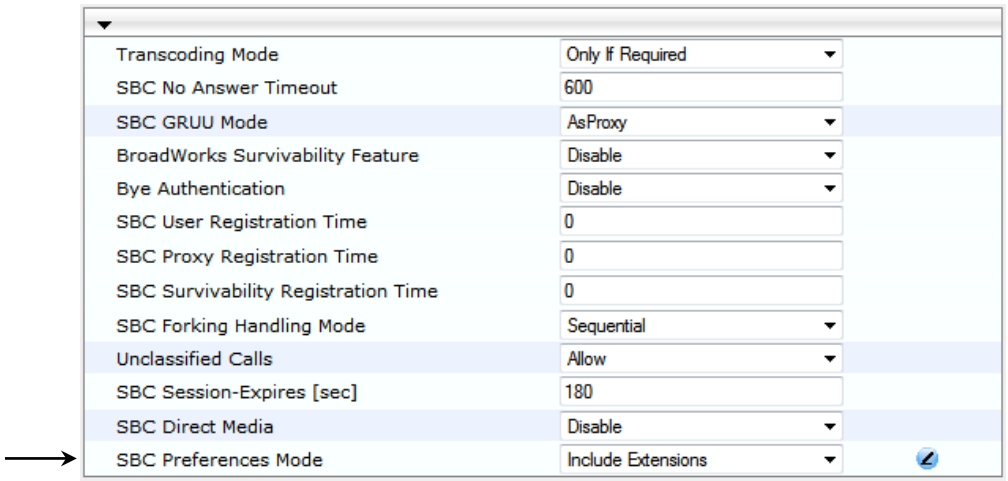
Parameter	Value
Allowed Coders Group ID	**2**
Coder Name	**G.729**

Figure 4-18: Configuring Allowed Coders Group for Bell Canada SIP Trunk



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

Figure 4-19: SBC Preferences Mode



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

4.8 Step 8: SIP TLS Connection Configuration

This section describes how to configure the E-SBC for using a TLS connection with the Lync Server 2010 Mediation Server. This is essential for a secure SIP TLS connection.

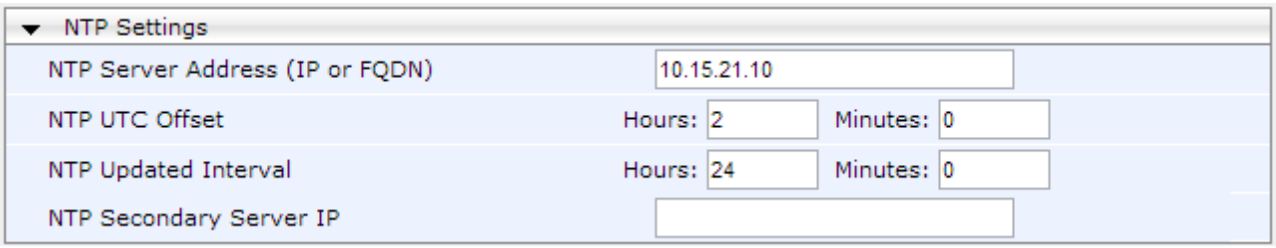
4.8.1 Step 8a: Configure the NTP Server Address

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

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

1. Open the Application Settings page (**Configuration** tab > **System** > **Application Settings**).
2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., **10.15.21.10**).

Figure 4-20: Configuring NTP Server Address



3. Click **Submit**.

4.8.2 Step 8b: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Lync Server 2010.

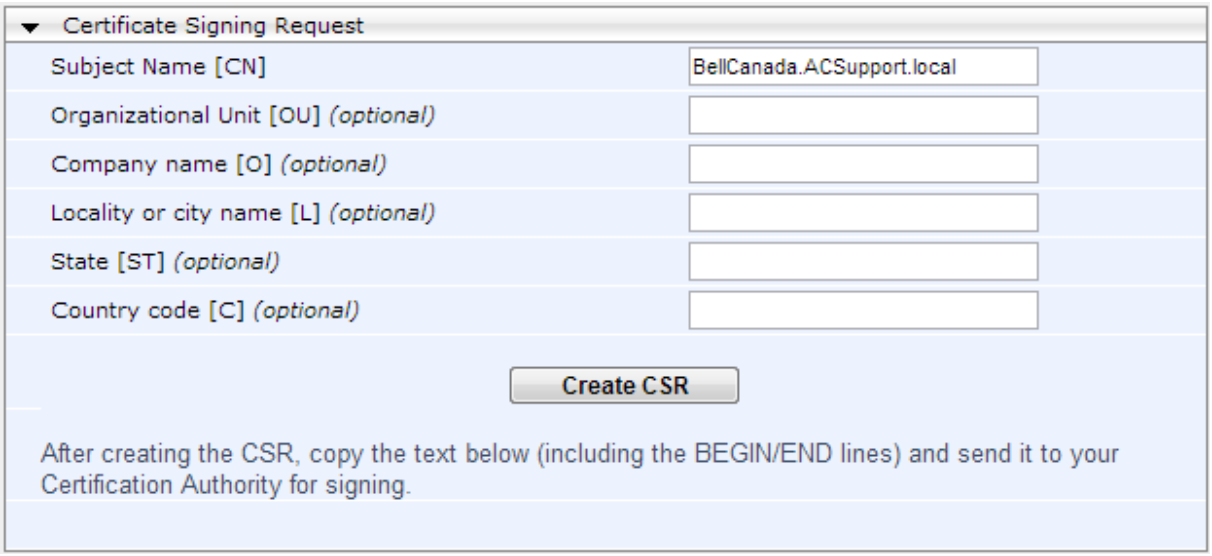
The procedure involves the following main steps:

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

➢ **To configure a certificate:**

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

Figure 4-21: Certificates Page - Creating CSR



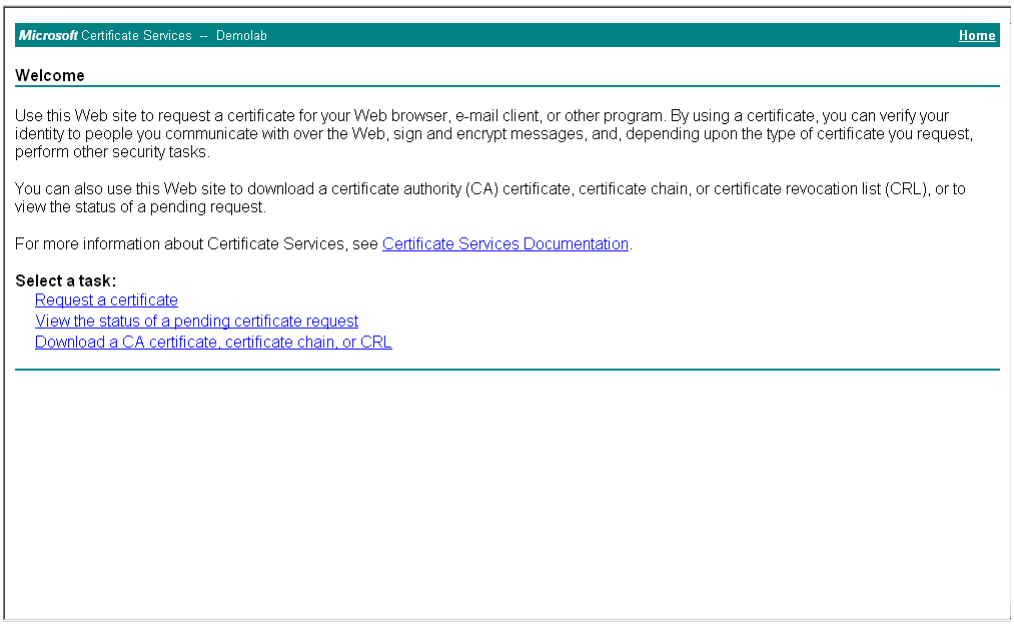
2. In the 'Subject Name' field, enter the media gateway name (e.g., **BellCanada.ACSupport.local**).

Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2010 (see Section 3.1 on page 13).

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

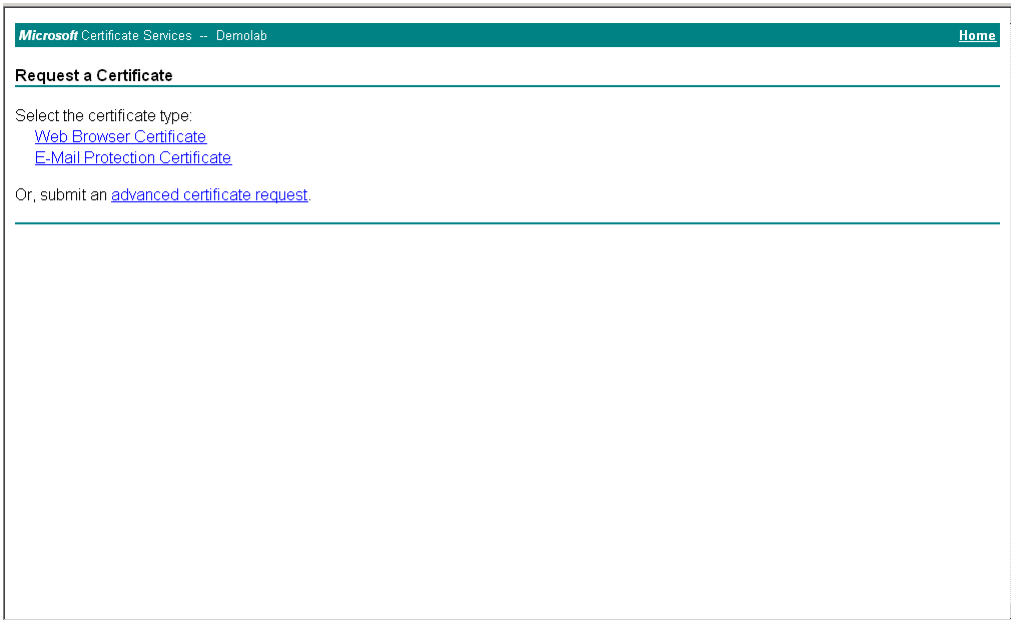
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-22: Microsoft Certificate Services Web Page



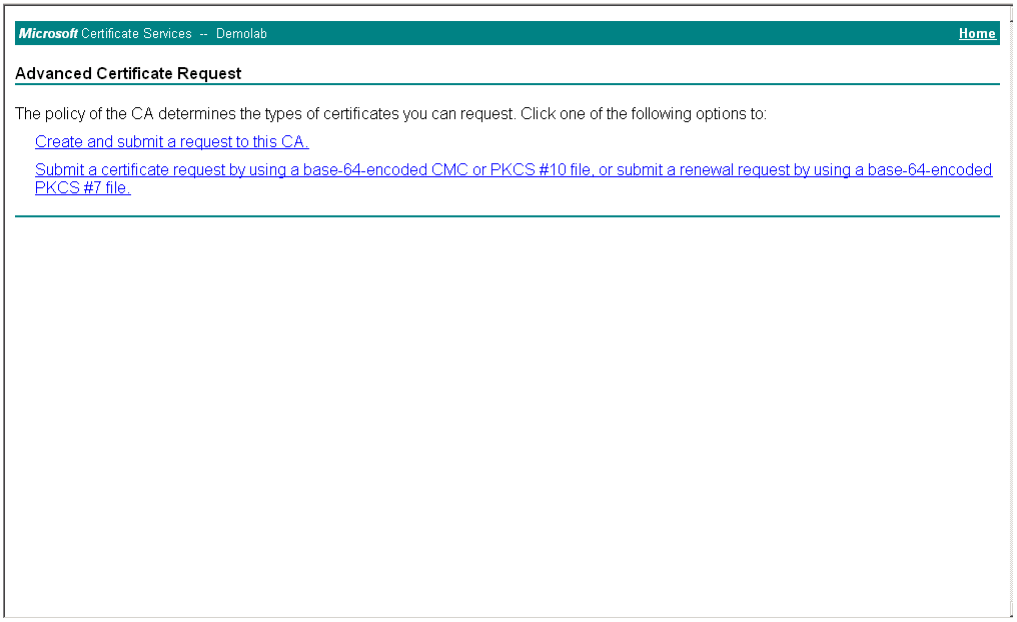
6. Click **Request a certificate**.

Figure 4-23: Request a Certificate Page



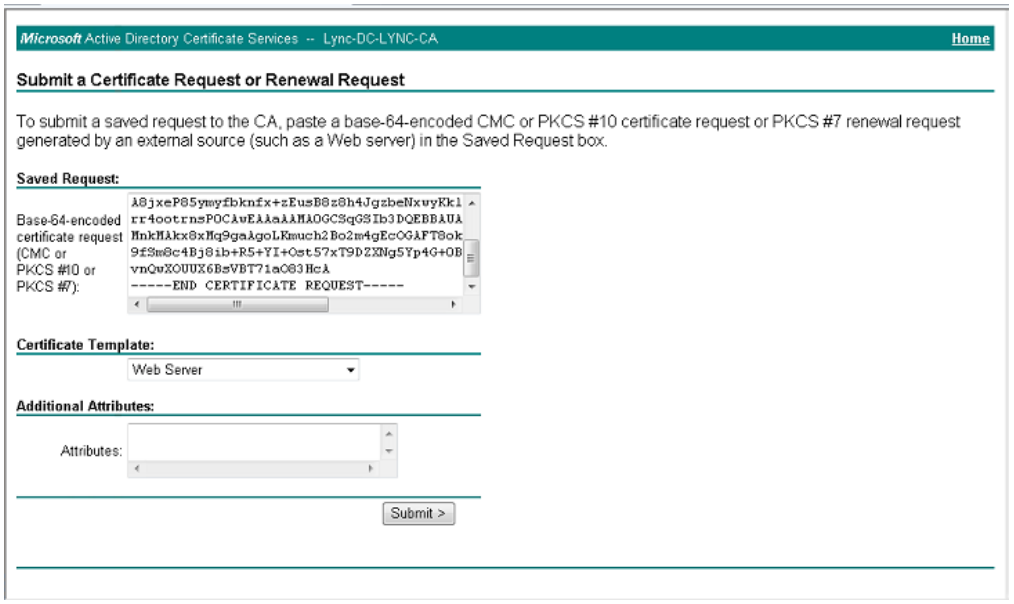
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-24: Advanced Certificate Request Page



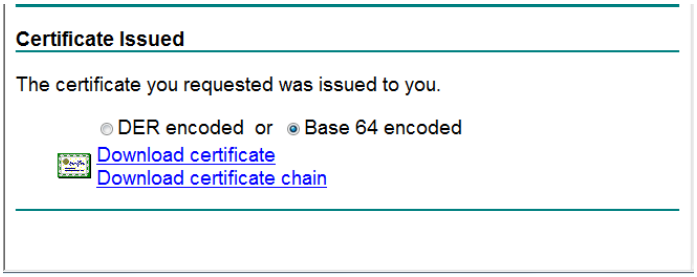
8. Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-25: Submit a Certificate Request or Renewal Request Page



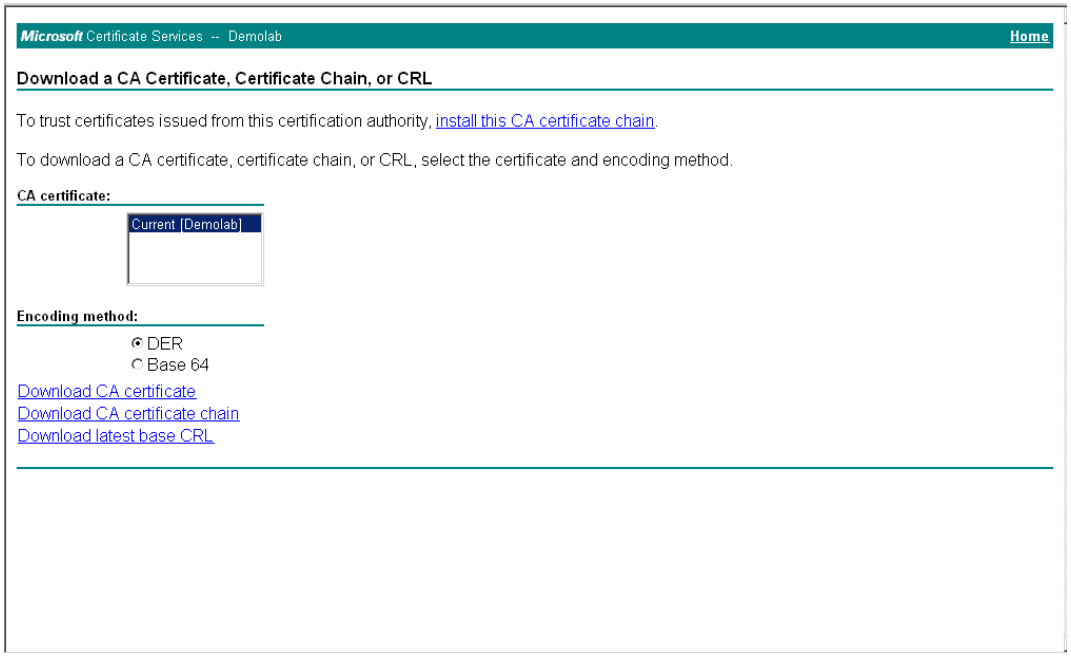
9. Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Saved Request' field.
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-26: Certificate Issued Page



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

Figure 4-27: Download a CA Certificate, Certificate Chain, or CRL Page



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

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

Figure 4-28: Certificates Page (Uploading Certificate)

20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 71).

4.9 Step 9: Configure SRTP

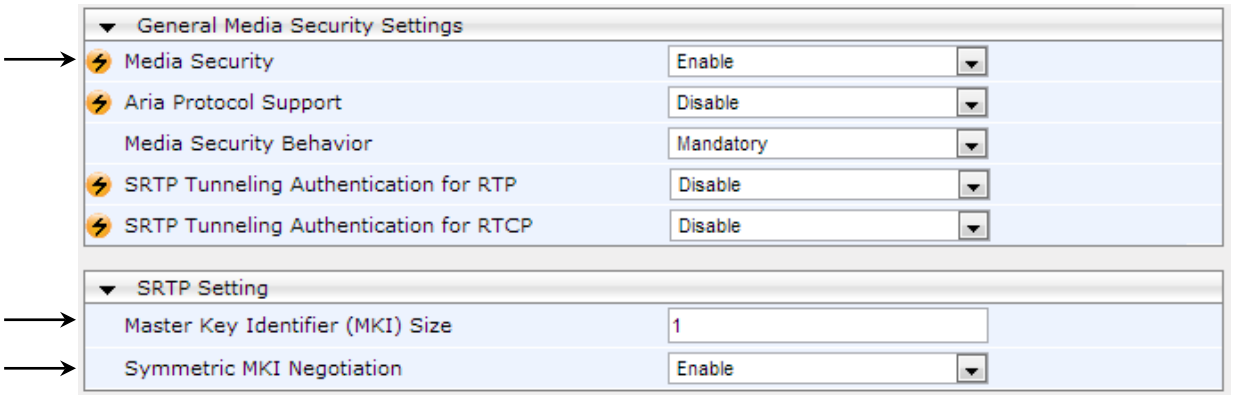
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2010 when you configured an IP Profile for Lync Server 2010 (see Section 4.6 on page 44).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**
Master Key Identifier (MKI) Size	**1**
Symmetric MKI Negotiation	**Enable**

Figure 4-29: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 71).

4.10 Step 10: Configure Maximum IP Media Channels

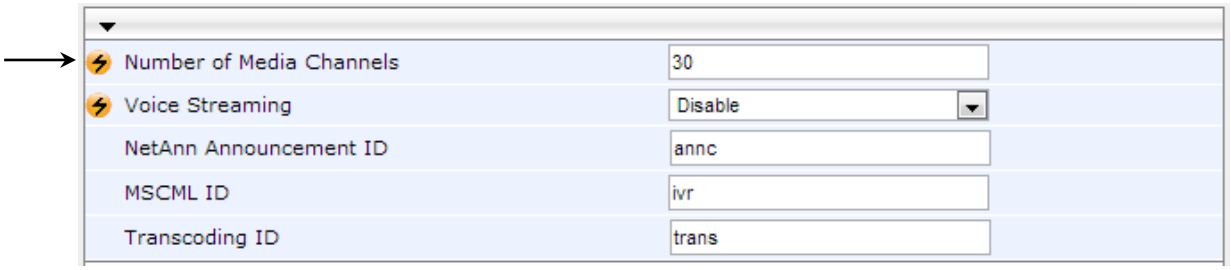
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

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

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

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

Figure 4-30: Configuring Number of IP Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 71).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 42, IP Group 1 represents Lync Server 2010, and IP Group 2 represents Bell Canada SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Lync Server 2010 (LAN) and Bell Canada SIP Trunk (WAN):

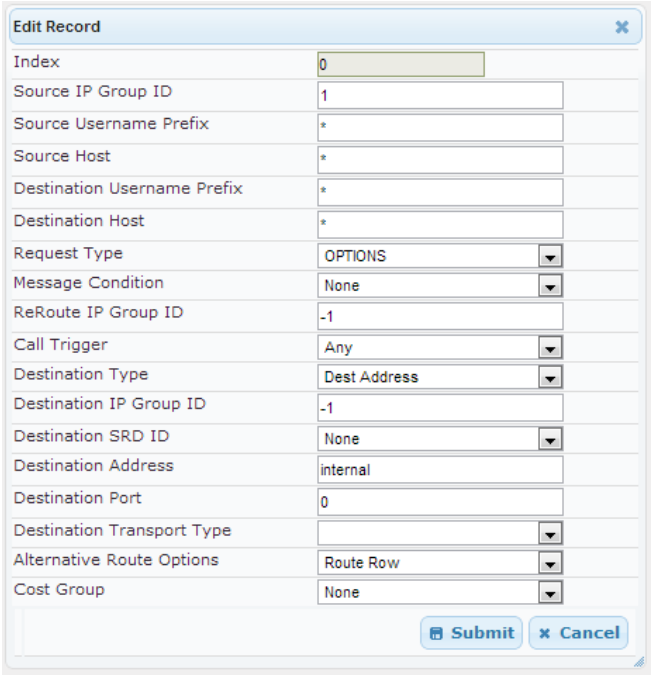
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2010 to Bell Canada SIP Trunk
- Calls from Bell Canada SIP Trunk to Lync Server 2010

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:

Parameter	Value
Index	**0**
Source IP Group ID	**1**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

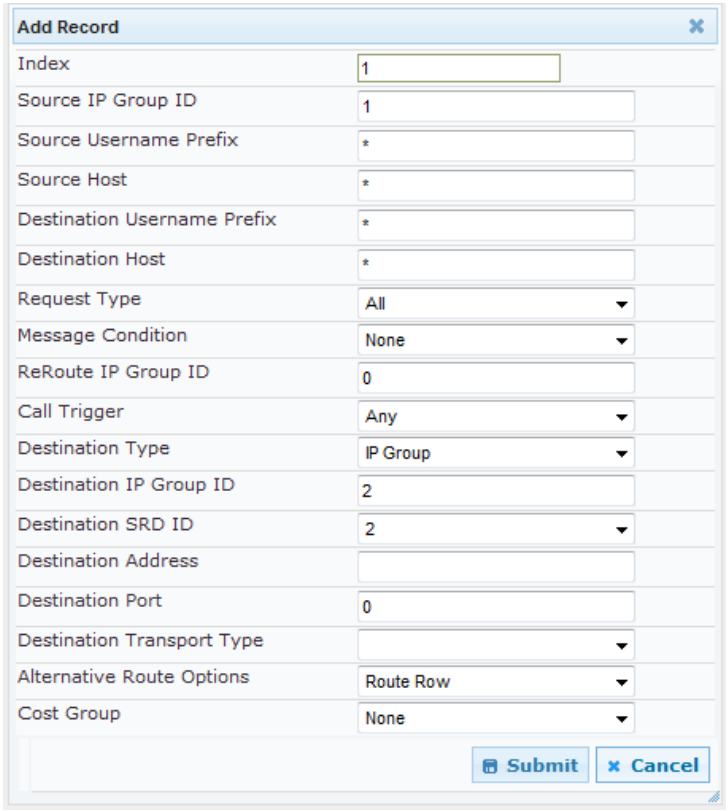
Figure 4-31: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN



3. Configure a rule to route calls from Lync Server 2010 to Bell Canada SIP Trunk:

Parameter	Value
Index	**1**
Source IP Group ID	**1**
Destination Type	**IP Group**
Destination IP Group ID	**2**
Destination SRD ID	**2**

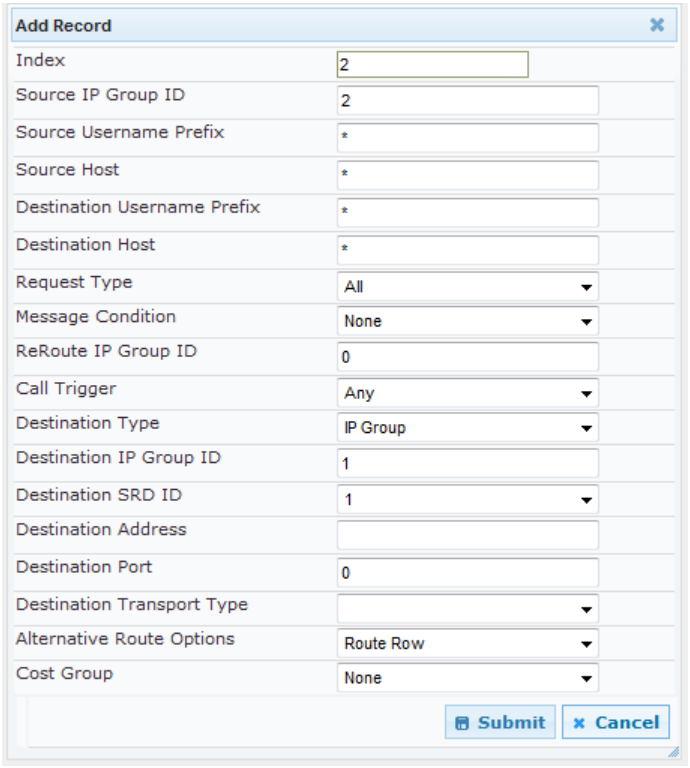
Figure 4-32: Configuring IP-to-IP Routing Rule for LAN to WAN



4. Configure a rule to route calls from Bell Canada SIP Trunk to Lync Server 2010:

Parameter	Value
Index	**2**
Source IP Group ID	**2**
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 4-33: Configuring IP-to-IP Routing Rule for WAN to LAN



The configured routing rules are shown in the figure below:

Figure 4-34: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

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

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

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 42, IP Group 1 represents Lync Server 2010, and IP Group 2 represents Bell Canada SIP Trunk.

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

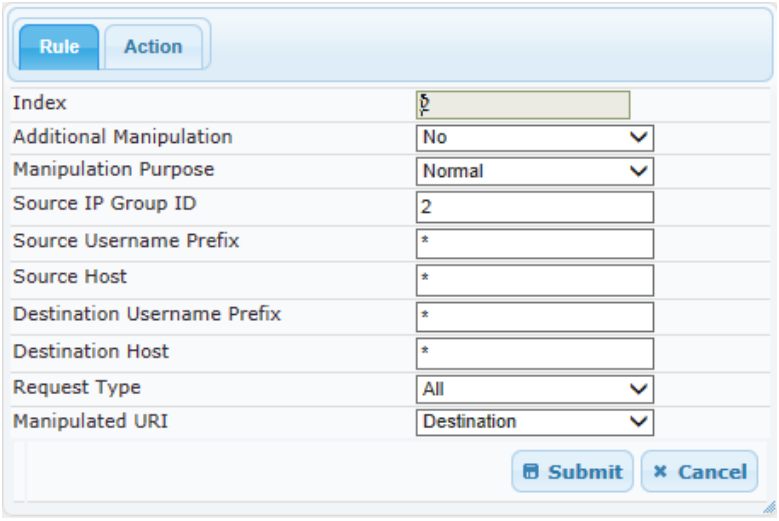
For this interoperability test topology, a manipulation is configured to add the "+1" to the destination number for calls from IP Group 2 (Bell Canada SIP Trunk) to IP Group 1 (i.e., Lync Server 2010) for any destination username prefix.

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

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

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

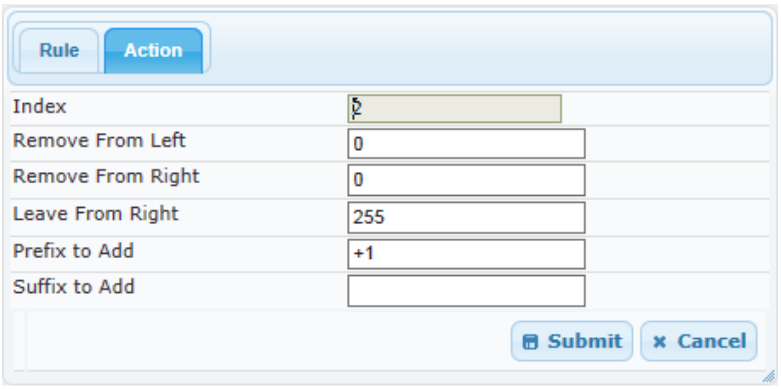
Figure 4-35: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab



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

Parameter	Value
Prefix to Add	**+1**

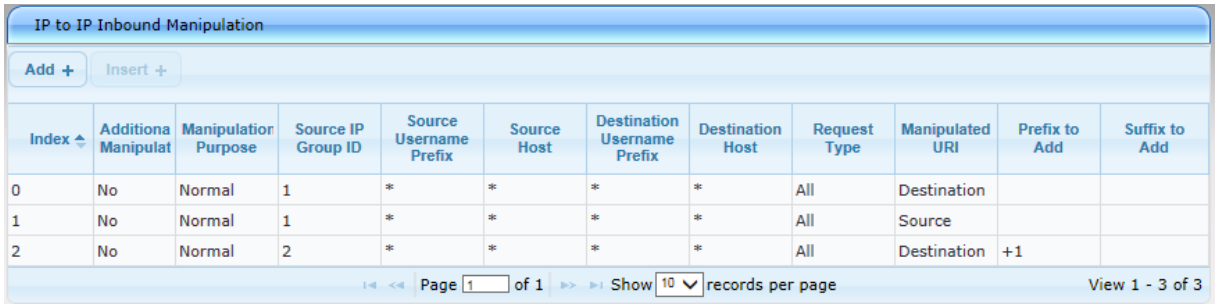
Figure 4-36: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



5. Click **Submit**.

The figure below shows an example of configured IP-to-IP inbound manipulation rules for calls between IP Group 1 (i.e., Lync Server 2010) and IP Group 2 (i.e., Bell Canada SIP Trunk):

Figure 4-37: Example of Configured IP-to-IP Outbound Manipulation Rules



Rule Index	Description
0	Calls from IP Group 1 to IP Group 2 with any destination or source number (*), remove 2 characters from the prefix of the destination number.
1	Calls from IP Group 1 to IP Group 2 with any destination or source number (*), remove 2 characters from the prefix of the source number.
2	Calls from IP Group 2 to IP Group 1 with any destination or source number (*), add "+1" to the prefix of the destination number.

4.13 Step 13: Configure Message Manipulation Rules

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

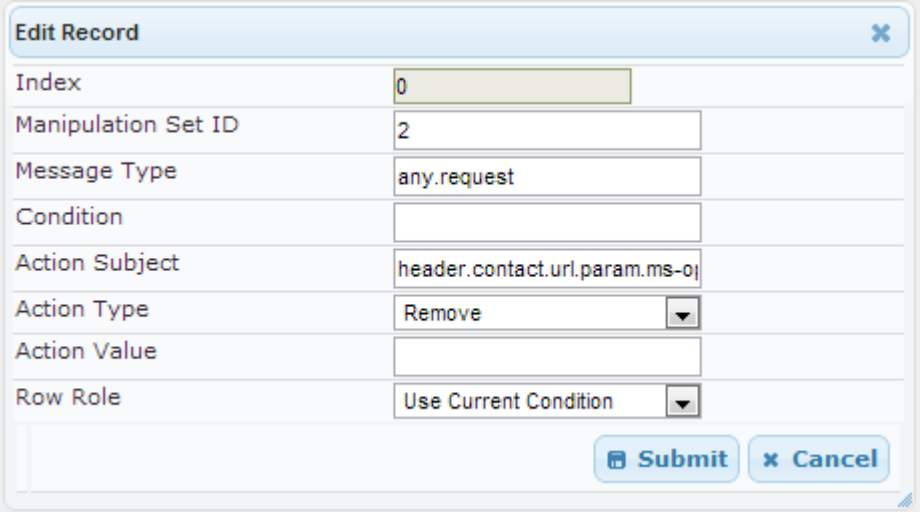
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes 'ms-opaque' parameter from Contact Header.

Parameter	Value
Index	**0**
Manipulation Set ID	**2**
Message Type	**any.request**
Action Subject	**header.contact.url.param.ms-opaque**
Action Type	**Remove**

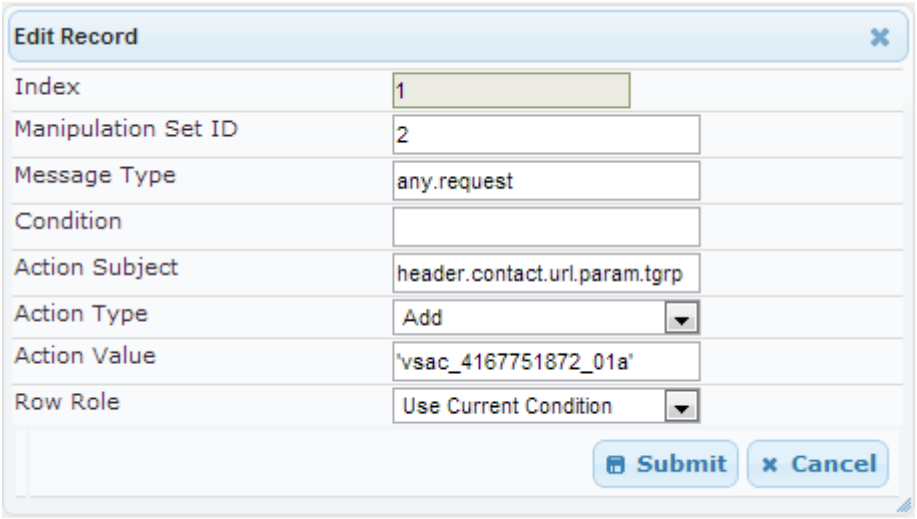
Figure 4-38: Configuring SIP Message Manipulation Rule 0 (for Bell Canada SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This adds 'vsac_4167751872_01a' TGRP parameter to Contact Header.

Parameter	Value
Index	**1**
Manipulation Set ID	**2**
Message Type	**any.request**
Action Subject	**header.contact.url.param.tgrp**
Action Type	**Add**
Action Value	**'vsac_4167751872_01a'**

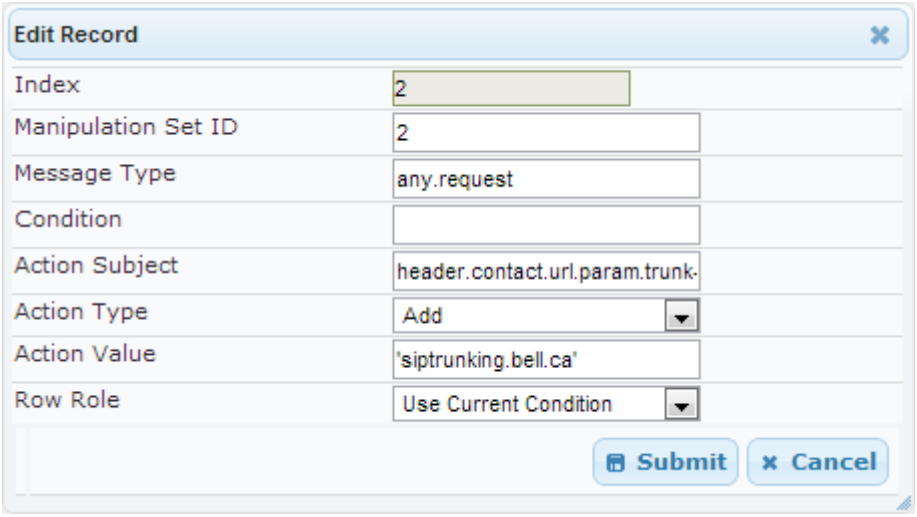
Figure 4-39: Configuring SIP Message Manipulation Rule 1 (for Bell Canada SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This adds 'siptrunking.bell.ca' trunk-context parameter to Contact Header.

Parameter	Value
Index	**2**
Manipulation Set ID	**2**
Message Type	**any.request**
Action Subject	**header.contact.url.param.trunk-context**
Action Type	**Add**
Action Value	**'siptrunking.bell.ca'**

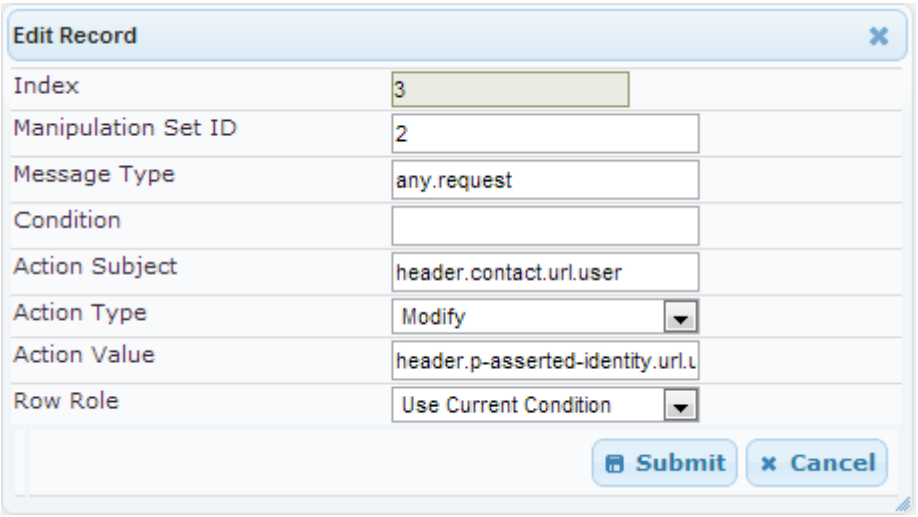
Figure 4-40: Configuring SIP Message Manipulation Rule 2 (for Bell Canada SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This replaces the user part of Contact Header with value from P-Asserted Identity Header.

Parameter	Value
Index	**3**
Manipulation Set ID	**2**
Message Type	**any.request**
Action Subject	**header.contact.url.user**
Action Type	**Modify**
Action Value	**header.p-asserted-identity.url.user**

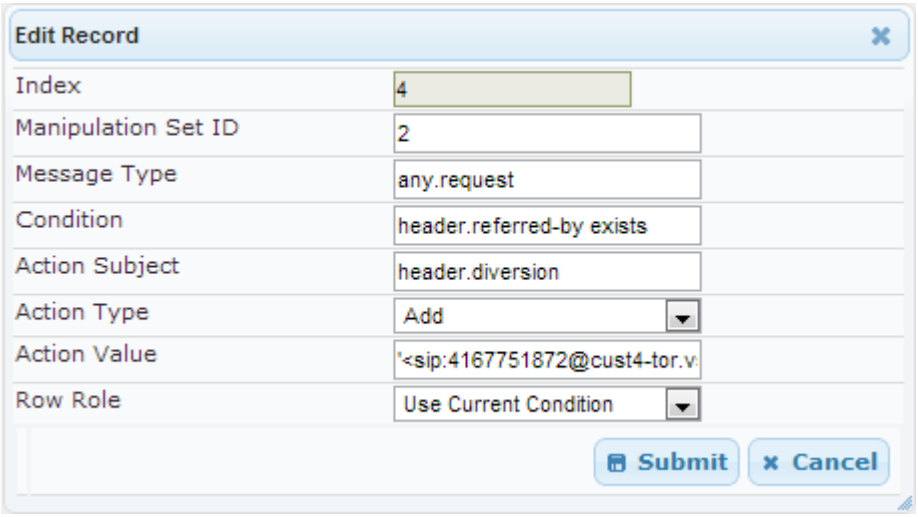
Figure 4-41: Configuring SIP Message Manipulation Rule 3 (for Bell Canada SIP Trunk)



6. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Call Transfer initiated by the Lync Server 2010 (IP Group 1).
This adds '<sip:4167751872@cust4-tor.vsac.bell.ca>' string to Diversion Header in case that Referred-By Header exists. Where 4167751872 is trunk main line.

Parameter	Value
Index	**4**
Manipulation Set ID	**2**
Message Type	**any.request**
Condition	**header.referred-by exists**
Action Subject	**header.diversion**
Action Type	**Add**
Action Value	**'<sip:4167751872@cust4-tor.vsac.bell.ca>'**

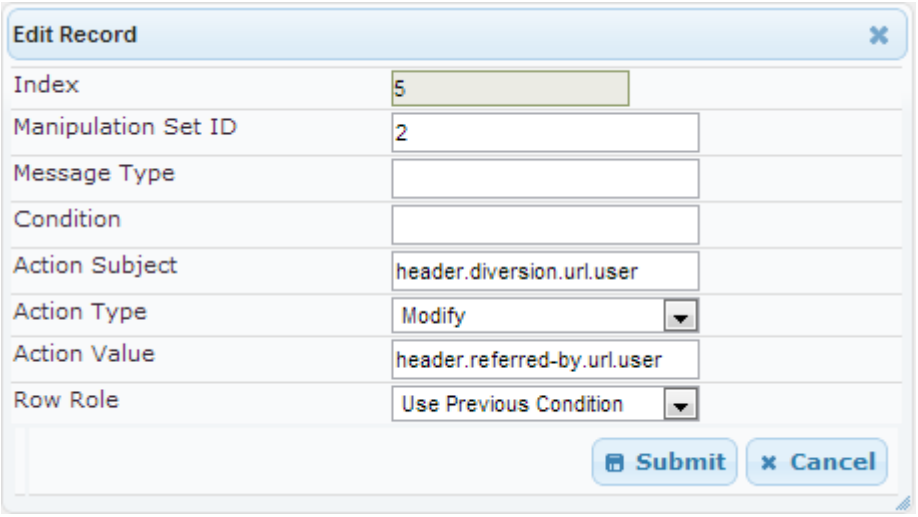
Figure 4-42: Configuring SIP Message Manipulation Rule 4 (for Bell Canada SIP Trunk)



7. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) based on previous rule condition. This replaces the user part of Diversion Header with value from Referred-By Header.

Parameter	Value
Index	**5**
Manipulation Set ID	**2**
Action Subject	**header.diversion.url.user**
Action Type	**Modify**
Action Value	**header.referred-by.url.user**
Row Role	**Use Previous Condition**

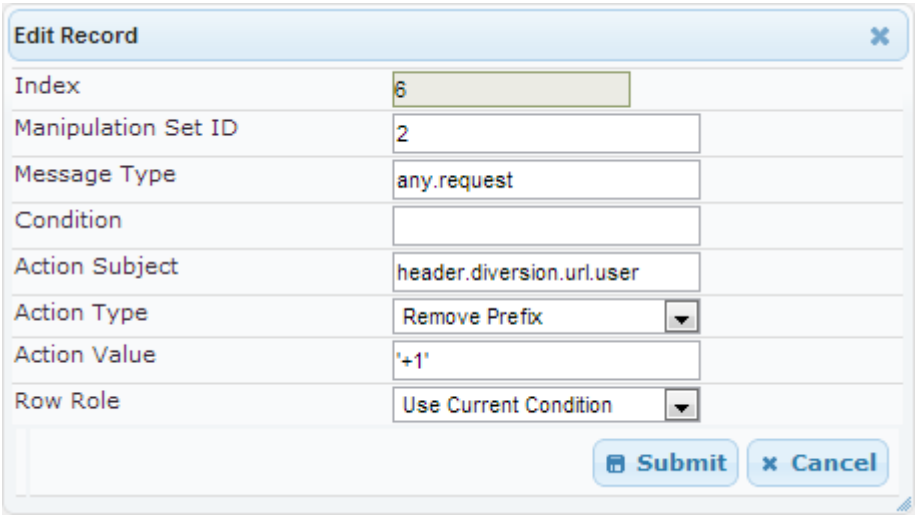
Figure 4-43: Configuring SIP Message Manipulation Rule 5 (for Bell Canada SIP Trunk)



8. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes '+1' prefix from the user part of Diversion Header.

Parameter	Value
Index	**6**
Manipulation Set ID	**2**
Message Type	**any.request**
Action Subject	**header.diversion.url.user**
Action Type	**Remove Prefix**
Action Value	**'+1'**

Figure 4-44: Configuring SIP Message Manipulation Rule 6 (for Bell Canada SIP Trunk)



9. Configure another manipulation rule (Manipulation Set 2) for Bell Canada SIP Trunk. This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Rejected Calls initiated by the Lync Server 2010 (IP Group 1). This replaces the method type '603' with the value '486', because Bell Canada SIP Trunk not recognizes '603' method type.

Parameter	Value
Index	**7**
Manipulation Set ID	**2**
Message Type	**invite.response.603**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'486'**

Figure 4-45: Configuring SIP Message Manipulation Rule 7 (for Bell Canada SIP Trunk)

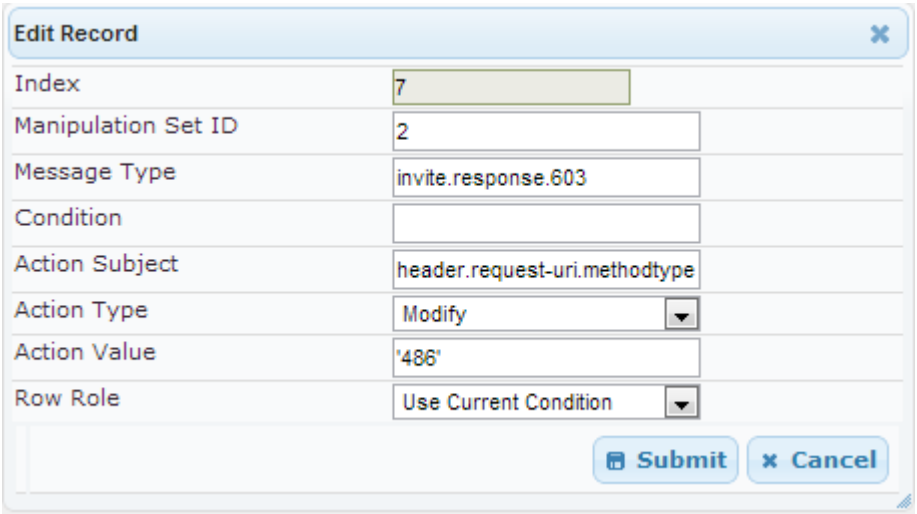
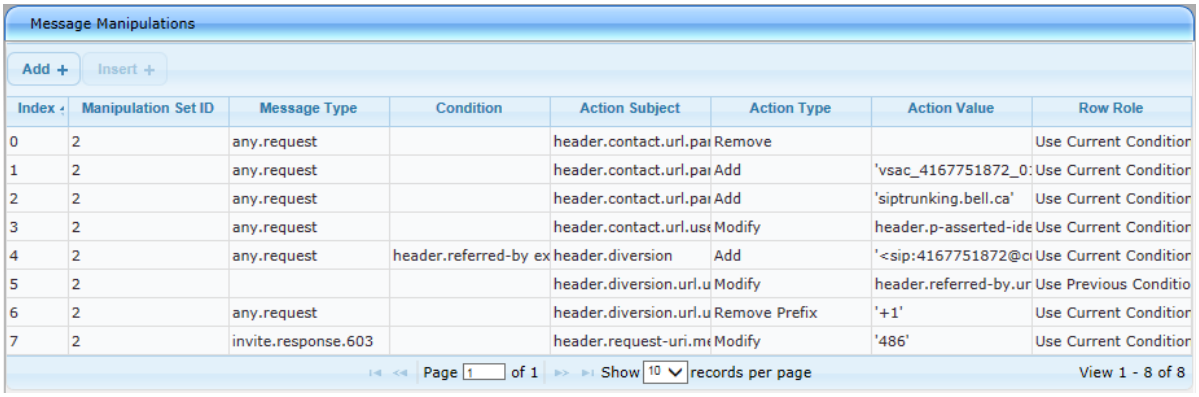


Figure 4-46: Example of Configured SIP Message Manipulation Rules



Message Manipulations

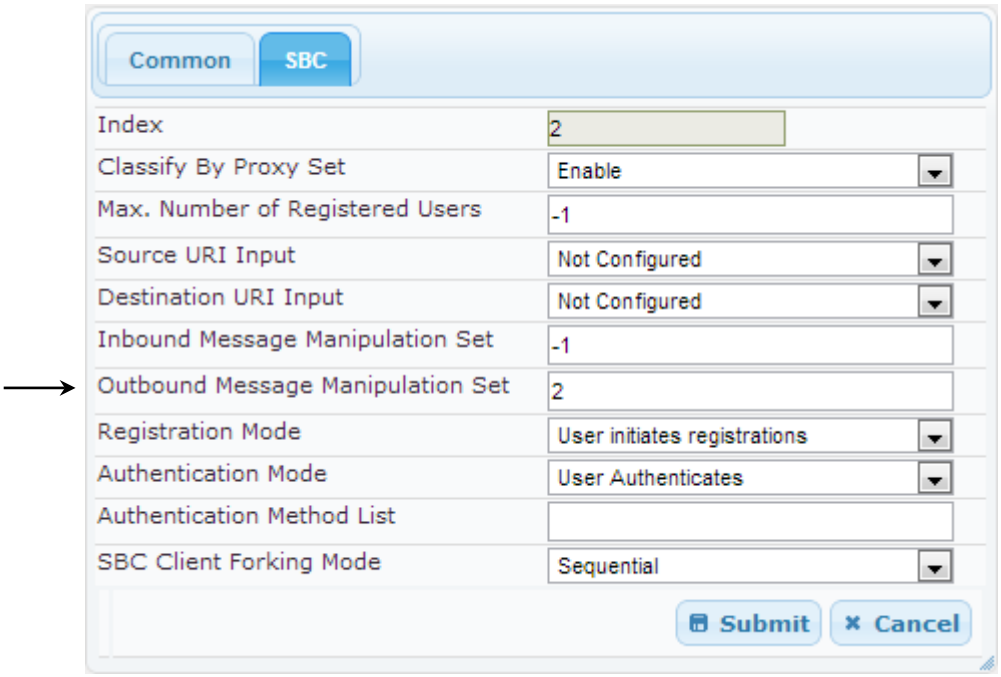
Add + | Insert +

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	2	any.request		header.contact.url.pa	Remove		Use Current Condition
1	2	any.request		header.contact.url.pa	Add	'vsac_4167751872_0	Use Current Condition
2	2	any.request		header.contact.url.pa	Add	'siptrunking.bell.ca'	Use Current Condition
3	2	any.request		header.contact.url.us	Modify	header.p-asserted-ide	Use Current Condition
4	2	any.request	header.referred-by ex	header.diversion	Add	'<sip:4167751872@c	Use Current Condition
5	2			header.diversion.url.u	Modify	header.referred-by.ur	Use Previous Conditio
6	2	any.request		header.diversion.url.u	Remove Prefix	'+1'	Use Current Condition
7	2	invite.response.603		header.request-uri.m	Modify	'486'	Use Current Condition

Page 1 of 1 | Show 10 records per page | View 1 - 8 of 8

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

Figure 4-47: Assigning Manipulation Set 2 to IP Group 2



Common | SBC

Index	2
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Source URI Input	Not Configured
Destination URI Input	Not Configured
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	2
Registration Mode	User initiates registrations
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential

Submit | Cancel

    e. Click **Submit**.

4.14 Step 14: Configure Registration Accounts

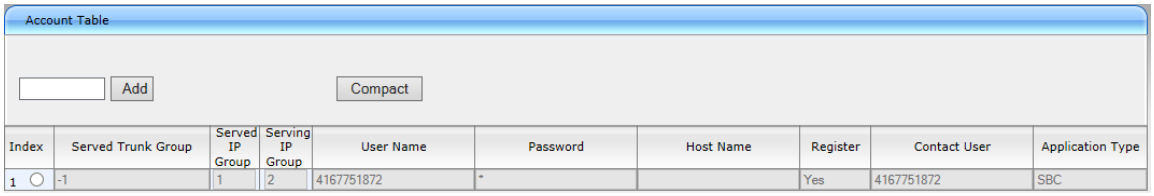
This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the Bell Canada SIP Trunk on behalf of Lync Server 2010. The Bell Canada SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Lync Server 2010 (IP Group 1) and the Serving IP Group is Bell Canada SIP Trunk (IP Group 2).

➢ **To configure a registration account:**

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

Figure 4-48: Configuring SIP Registration Account



2. Enter an index number (e.g., "0"), and then click **Add**.
3. Configure the account according to the provided information from Bell Canada, for example:

Parameter	Value
Served IP Group	**1** (Lync Server 2010)
Serving IP Group	**2** (Bell Canada SIP Trunk)
Username	As provided by Bell Canada
Password	As provided by Bell Canada
Host Name	**207.236.237.203**
Register	**Yes**
Contact User	**4167751872** (trunk main line)
Application Type	**SBC**

4. Click **Apply**.

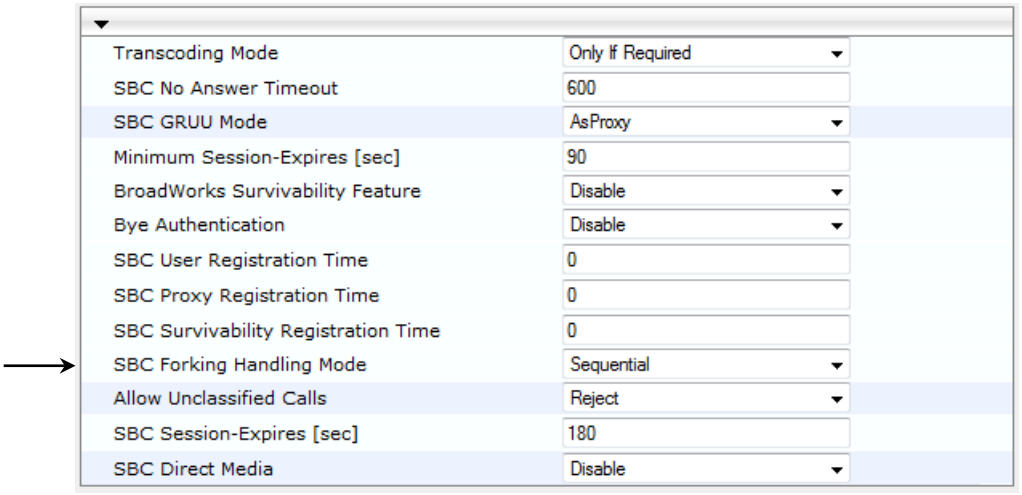
4.15 Step 15: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if 18x with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if 180 response without SDP is received. It's mandatory to set this field for the Lync Server 2010 environment.

➢ **To configure call forking:**

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

Figure 4-49: Configuring Forking Mode



3. Click **Submit**.

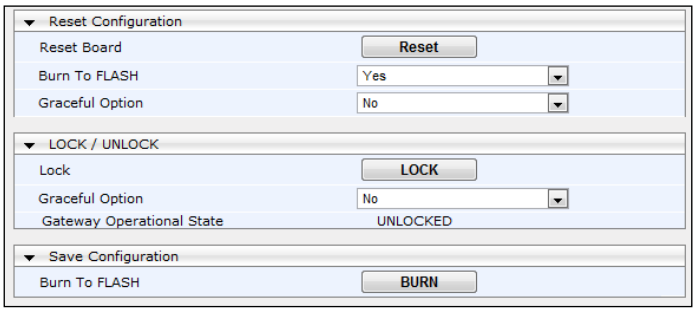
4.16 Step 16: Reset the E-SBC

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

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

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

Figure 4-50: Resetting the E-SBC



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

Reader's Notes

A AudioCodes INI File

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

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

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

;Board: Mediant 4000
;Board Type: 70
;Serial Number: 4773101
;Slot Number: 1
;Software Version: 6.60A.235.010
;DSP Software Version: 5039AE3_R => 660.22
;Board IP Address: 10.15.17.70
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 2048M   Flash size: 252M
;Num of DSP Cores: 24  Num DSP Channels: 30
;Num of physical LAN ports: 8
;Profile: NONE
;Key features:;Board Type: Mediant 4000 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;Coders: G723 G729 G728 NETCODER
GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711
MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB ;E1Trunks=0
;T1Trunks=0 ;DSP Voice features: IpmDetector RTCP-XR ;Channel Type: RTP
DspCh=30 IPMediaDspCh=30 ;Control Protocols: MSFT CLI TRANSCODING=10
FEU=10 TestCall=10 MGCP SIP SASurvivability SBC=120 ;Default
features:;Coders: G711 G726;

;------ Mediant 4000 HW components------
;
; Slot # : Module type : # of ports
;---------------------------------------------
;      1 : DSM         : 0
;      2 : CSM         : 0
;      3 : LSM         : 4
;      4 : DSM         : 0
;      5 : Empty
;      6 : LSM         : 4
;---------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.15.17.200
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
```

```
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '10.15.21.10'
LDAPSEARCHDNSINPARALLEL = 0

[BSP Params]

PCMLawSelect = 3

[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

[Voice Engine Params]

RFC2833TxPayloadType = 101
RFC2833RxPayloadType = 101
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1

[WEB Params]

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

[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
MEDIASECURITYBEHAVIOUR = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1

[IPsec Params]


[SNMP Params]
```

```
[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "GE_5", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "GE_6", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "GE_7", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "GE_8", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, GE_1, GE_2;
EtherGroupTable 1 = "GROUP_2", 2, GE_3, GE_4;
EtherGroupTable 2 = "GROUP_3", 2, GE_5, GE_6;
EtherGroupTable 3 = "GROUP_4", 2, GE_7, GE_8;

[ \EtherGroupTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 6, 10, 10.15.17.70, 16, 10.15.0.1, 1, "Lync",
10.15.21.10, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 195.189.192.153, 25, 195.189.192.129, 2,
"BellCanada", 80.179.52.100, 80.179.55.100, GROUP_2;

[ \InterfaceTable ]


[ DspTemplates ]

;
```

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

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault;
CpMediaRealm 1 = "MRLan", Lync, , 6000, 10, 6090, 1;
CpMediaRealm 2 = "MRWan", BellCanada, , 7000, 10, 7090, 0;

[ \CpMediaRealm ]


[ SRD ]

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

[ \SRD ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "LyncS.ACSupport.local:5067", 2, 1;
ProxyIp 1 = "siptrunking.bell.ca:5060", 0, 2;

[ \ProxyIp ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
```

```
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_SBCPlayHeldTone, IpProfile_SBCRemoteHoldFormat;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, -1, 1, 1, 0, 0, 0, 0,
8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3, 1, 1, 0, 3, 2, 1, 0, 1, 0, 0, 0,
1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0;
IpProfile 2 = "BellCanada", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, 2, 1, 2, 0, 0,
1, 0, 8, 300, 400, 1, 0, 0, -1, 0, 0, 1, 3, 2, 2, 2, 1, 3, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0;

[ \IpProfile ]


[ 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, 1, 0, -1;
ProxySet 2 = 1, 60, 0, 0, 2, 0, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "Lync", 1, "cust4-tor.vsac.bell.ca", "", 0, -1, -1, 0, -1,
1, "MRLan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "BellCanada", 2, "siptrunking.bell.ca", "", 0, -1, -1, 0,
-1, 2, "MRWan", 1, 2, -1, -1, 2, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]
```

```
[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup,
Account_ServingIPGroup, Account_Username, Account_Password,
Account_HostName, Account_Register, Account_ContactUser,
Account_ApplicationType;
Account 0 = -1, 1, 2, "4167751872", *, "207.236.237.203", 1,
"4167751872", 2;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_CostGroup;
IP2IPRouting 0 = 1, "*", "*", "*", "*", 6, , -1, 0, 1, -1, , "internal",
0, -1, 0, ;
IP2IPRouting 1 = 1, "*", "*", "*", "*", 0, , -1, 0, 0, 2, , "", 0, -1, 0,
;
IP2IPRouting 2 = 2, "*", "*", "*", "*", 0, , -1, 0, 0, 1, , "", 0, -1, 0,
;

[ \IP2IPRouting ]


[ SIPInterface ]

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

[ \SIPInterface ]


[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index =
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
```

```
IPInboundManipulation 0 = 0, 0, 1, "*", "*", "*", "*", 0, 1, 2, 0, 255,
"", "";
IPInboundManipulation 1 = 0, 0, 1, "*", "*", "*", "*", 0, 0, 2, 0, 255,
"", "";
IPInboundManipulation 2 = 0, 0, 2, "*", "*", "*", "*", 0, 1, 0, 0, 255,
"+1", "";

[ \IPInboundManipulation ]


[ CodersGroup0 ]

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

[ \CodersGroup0 ]


[ CodersGroup1 ]

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

[ \CodersGroup1 ]


[ CodersGroup2 ]

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

[ \CodersGroup2 ]


[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = 2, "any.request", "",
"header.contact.url.param.ms-opaque", 1, "", 0;
MessageManipulations 1 = 2, "any.request", "",
"header.contact.url.param.tgrp", 0, "'vsac_4167751872_01a'", 0;
MessageManipulations 2 = 2, "any.request", "",
"header.contact.url.param.trunk-context", 0, "'siptrunking.bell.ca'", 0;
```

```
MessageManipulations 3 = 2, "any.request", "", "header.contact.url.user",
2, "header.p-asserted-identity.url.user", 0;
MessageManipulations 4 = 2, "any.request", "header.referred-by exists",
"header.diversion", 0, "'<sip:4167751872@cust4-tor.vsac.bell.ca>'", 0;
MessageManipulations 5 = 2, "", "", "header.diversion.url.user", 2,
"header.referred-by.url.user", 1;
MessageManipulations 6 = 2, "any.request", "",
"header.diversion.url.user", 6, "'+1'", 0;
MessageManipulations 7 = 2, "invite.response.603", "", "header.request-
uri.methodtype", 2, "'486'", 0;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com