Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2013 & Bell Canada SIP Trunk using Mediant E-SBC

Microsoft Partner
Gold Communications

Lync

Bell

AudioCodes

Version 6.8

February 2015

Document # LTRT-39233

Table of Contents

This page is intentionally left blank.

Notice

This document shows how to connect the Microsoft Lync Server 2013 and Bell Canada's SIP Trunk using AudioCodes Mediant E-SBC product series.

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

Date Published: February-5-2015

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 services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Document Revision Record

LTRT	Description
39232	Initial document release
39233	Added Dynamic ONND feature configuration

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

This note describes how to set up AudioCodes Enterprise Session Border Controller (referred to in this document as *E-SBC*) for interworking between Bell Canada's SIP Trunk and Microsoft's Lync Server 2013 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 2013 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 SBC
Software Version	SIP_6.80A.256
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 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

Vendor	Microsoft
Model	Microsoft Lync
Software Version	Release 2013 5.0.8308.0
Protocol	SIP
Additional Notes	None

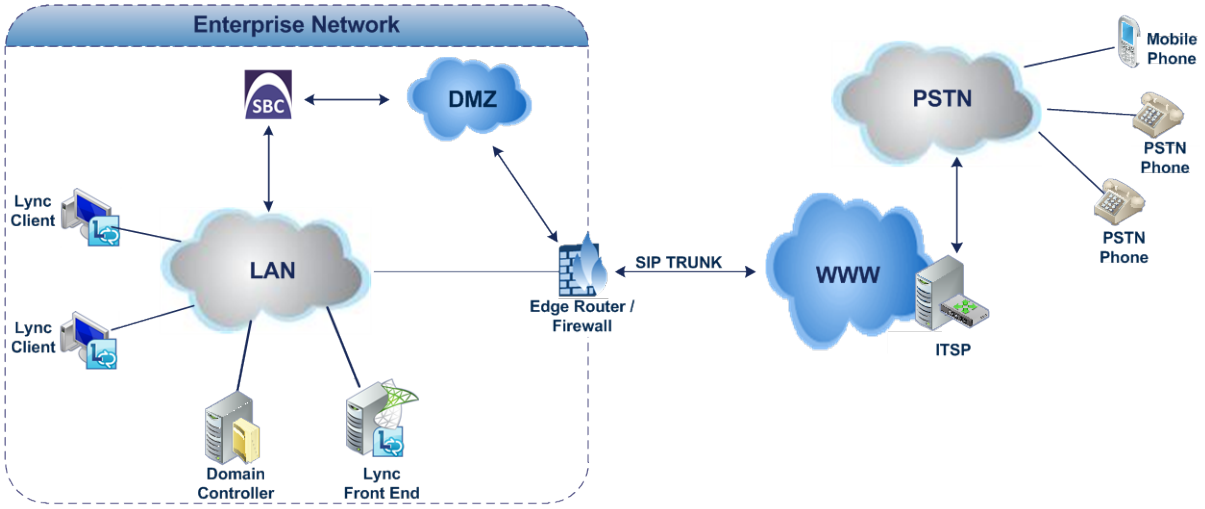
2.4 Interoperability Test Topology

Interoperability testing between AudioCodes' E-SBC and Bell Canada's SIP Trunk with Lync 2013 was performed using this topology:

- The enterprise deployed Microsoft Lync Server 2013 in its private network for enhanced communication within the enterprise.
- The enterprise wants to offer its employees enterprise-voice capabilities and to connect the enterprise to the PSTN network using 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 IP-based Session Initiation Protocol (SIP)
  - Border: IP-to-IP network border between the Lync Server 2013 network in the enterprise LAN, and Bell Canada's SIP Trunk located in the public network

Figure 2-1 illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Lync with Bell Canada's 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 2013 environment is located on the enterprise's LAN ▪ Bell Canada's SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2013 operates with SIP-over-TLS transport type ▪ Bell Canada's SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders ▪ Bell Canada's SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ Microsoft Lync Server 2013 operates with SRTP media type ▪ Bell Canada's SIP Trunk operates with RTP media type

2.4.2 Known Limitations

The following limitation was observed in the Interoperability tests performed for AudioCodes' E-SBC interworking between Microsoft Lync Server 2013 and Bell Canada's SIP Trunk:

1. If, following a “603 Decline”, an Error Response is sent from the Lync server, Bell Canada's SIP Trunk continues to send re-INVITEs and does not disconnect the call. To resolve this and disconnect the call correctly, a message manipulation rule is used to replace the Error Response with a “486 Busy Here” (see Section 4.13 on page 71).
2. In all outgoing calls (Lync to PSTN), Bell Canada’s SIP Trunk waits for RTP packets in order to ring a ‘Ring Back Tone’. Lync does not send these packets because it does not recognize comfort noise as an RTP stream. To resolve this issue, the force transcoding feature must be enabled in the E-SBC's Bell Canada IP Profile (see the 'Transcoding Mode' parameter under Section 4.6 on page 46).
3. In a Park Call scenario, when Lync transfers a call to the parking lot (puts the call on park), two INVITEs are sent, the first with a=inactive and another after that with a=sendonly. The second Invite is responded to by Bell Canada with a=inactive instead of a=recvonly. This causes a situation in which the parked party is on hold without hearing anything (Lync usually sends Music on Hold to the parked party). The main functionality is not impacted.

This page is intentionally left blank.

3 Configuring Lync Server 2013

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

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

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

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

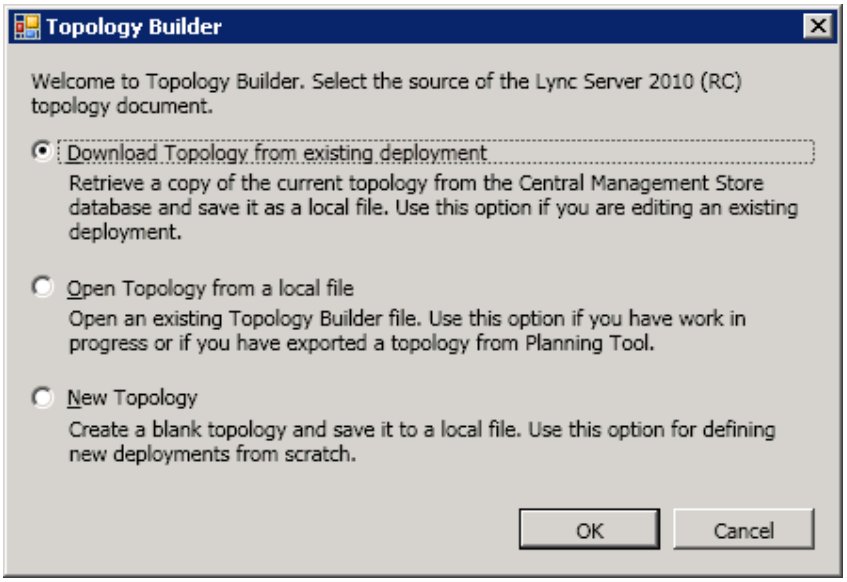
➢ **To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:**

1. On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows **Start** menu > **All Programs** > **Lync Server Topology Builder**), as shown below:

Figure 3-1: Starting the Lync Server Topology Builder

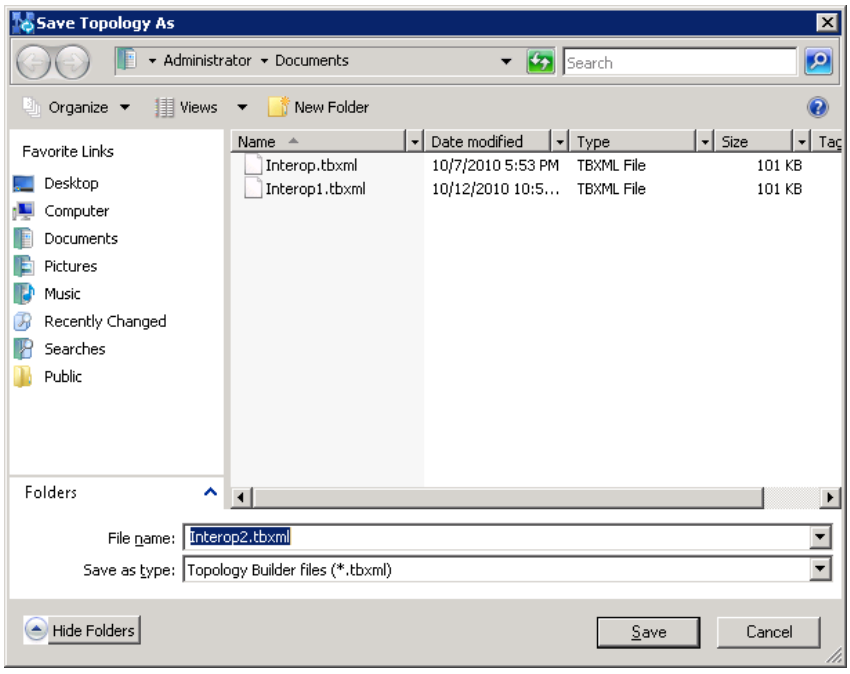
The following is displayed:

Figure 3-2: Topology Builder



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

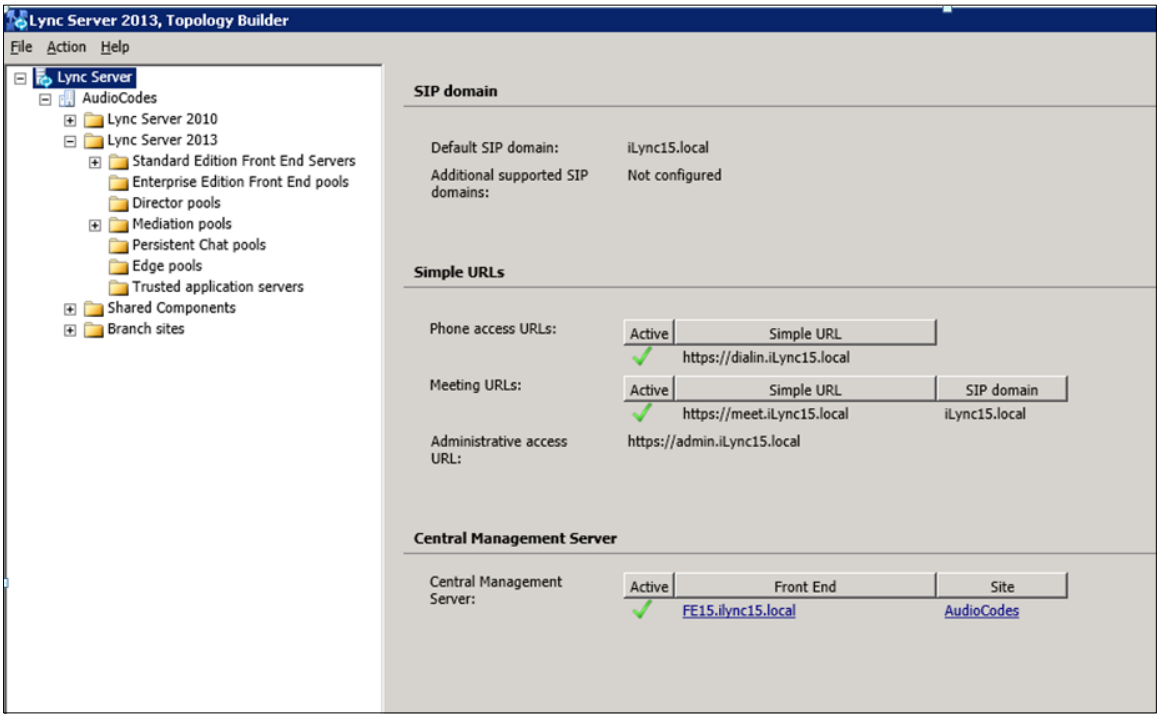
Figure 3-3: Save Topology



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.

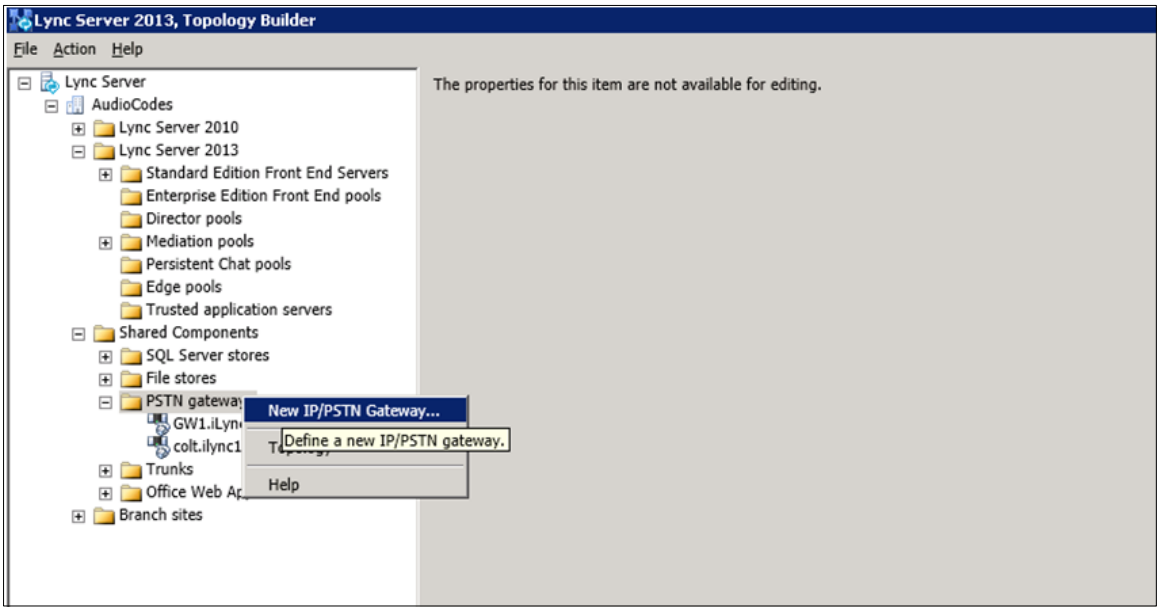
   The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



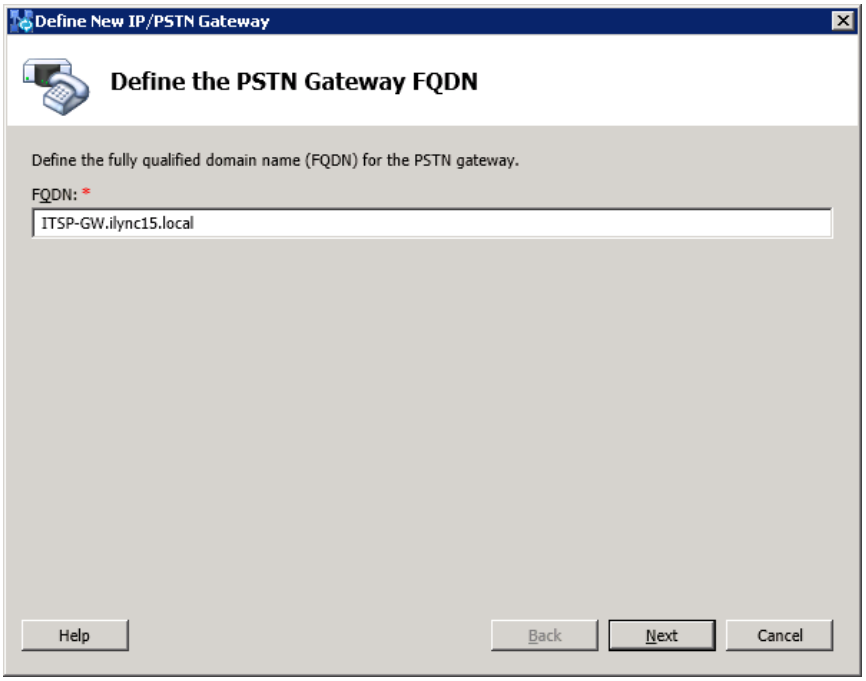
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



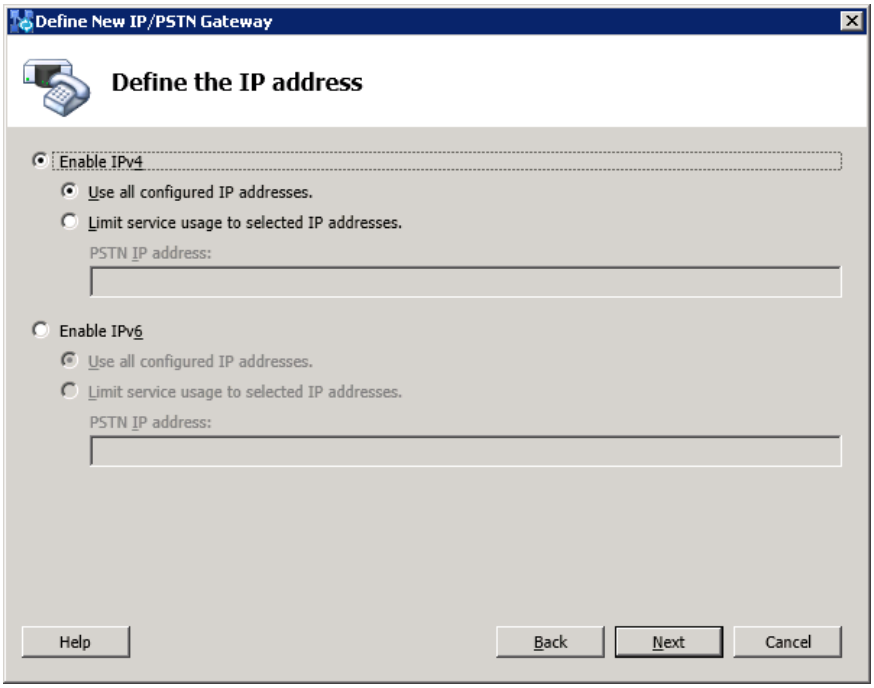
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP-GW.ilync15.local**). Update this FQDN in the relevant DNS record, and then click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



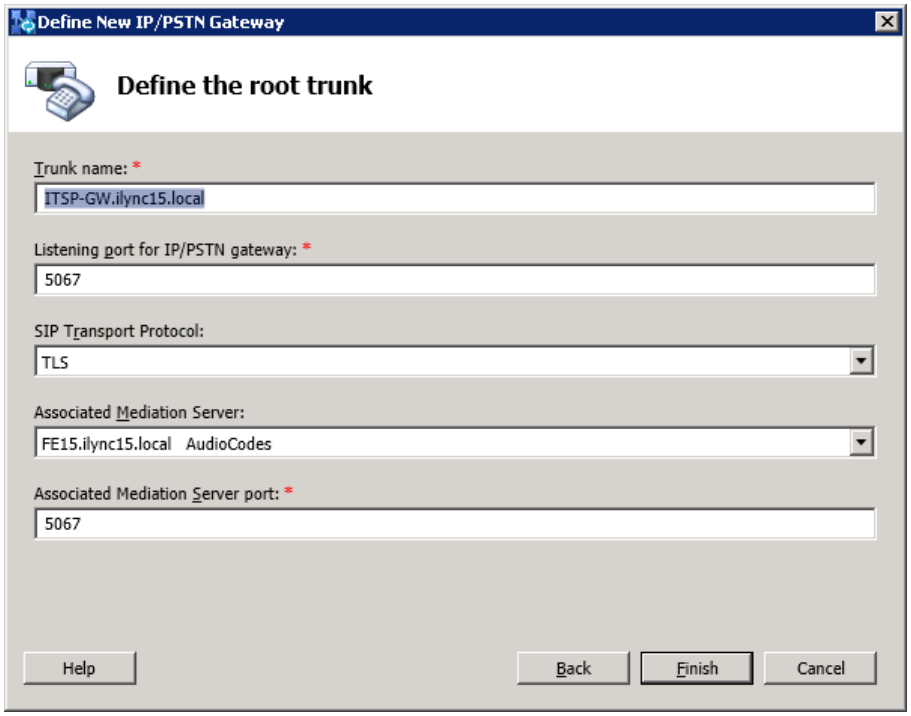
6. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

7. Define a *root trunk* for the PSTN gateway. A trunk is a logical connection between the Mediation Server and a gateway uniquely identified by the following combination: Mediation Server FQDN, Mediation Server listening port (TLS or TCP), gateway IP and FQDN, and gateway listening port.

Notes:

- When defining a PSTN gateway in Topology Builder, you must define a root trunk to successfully add the PSTN gateway to your topology.
- The root trunk cannot be removed until the associated PSTN gateway is removed.

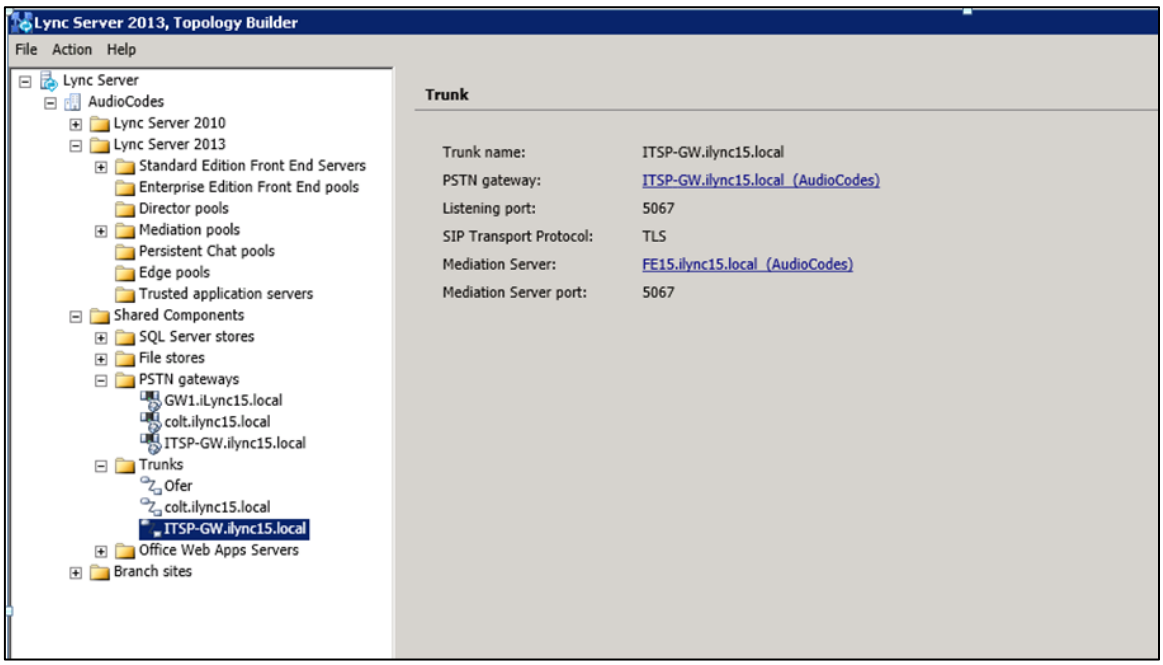
Figure 3-8: Define the Root Trunk



a. In the 'Listening Port for IP/PSTN Gateway' field, enter the listening port that the E-SBC will use for SIP messages from the Mediation Server that will be associated with the root trunk of the PSTN gateway (e.g., **5067**).
b. In the 'SIP Transport Protocol' field, select the transport type (e.g., **TLS**) that the trunk uses.
c. In the 'Associated Mediation Server' field, select the Mediation Server pool to associate with the root trunk of this PSTN gateway.
d. In the 'Associated Mediation Server Port' field, enter the listening port that the Mediation Server will use for SIP messages from the SBC (e.g., **5067**).
e. Click **Finish**.

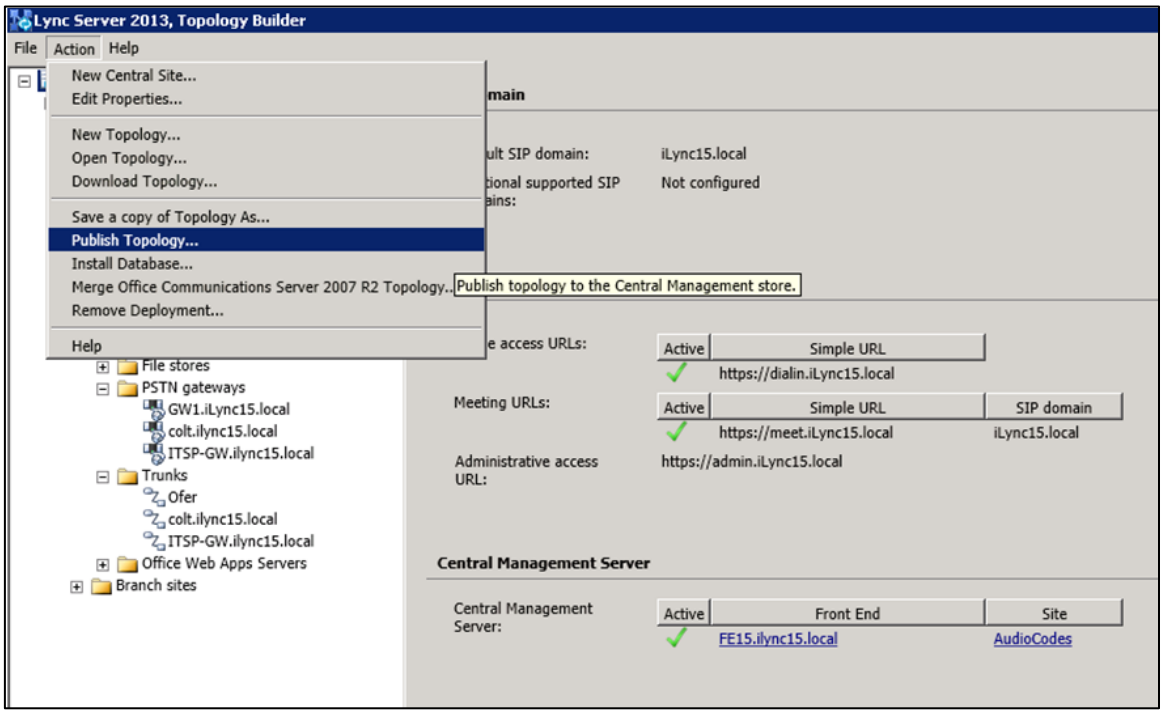
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



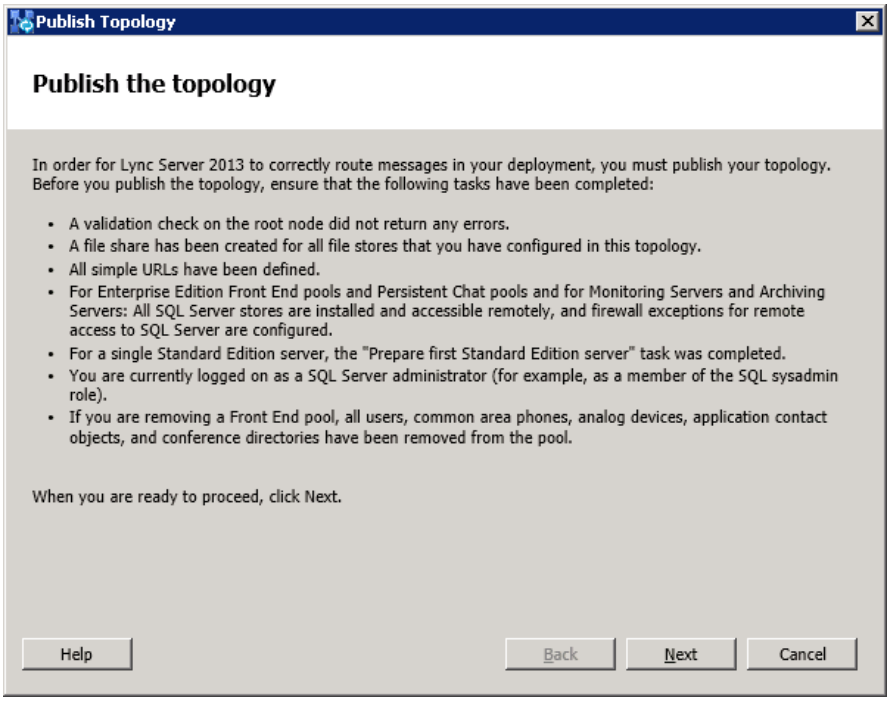
8. Publish the Topology: In the main tree, select the root node **Lync Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



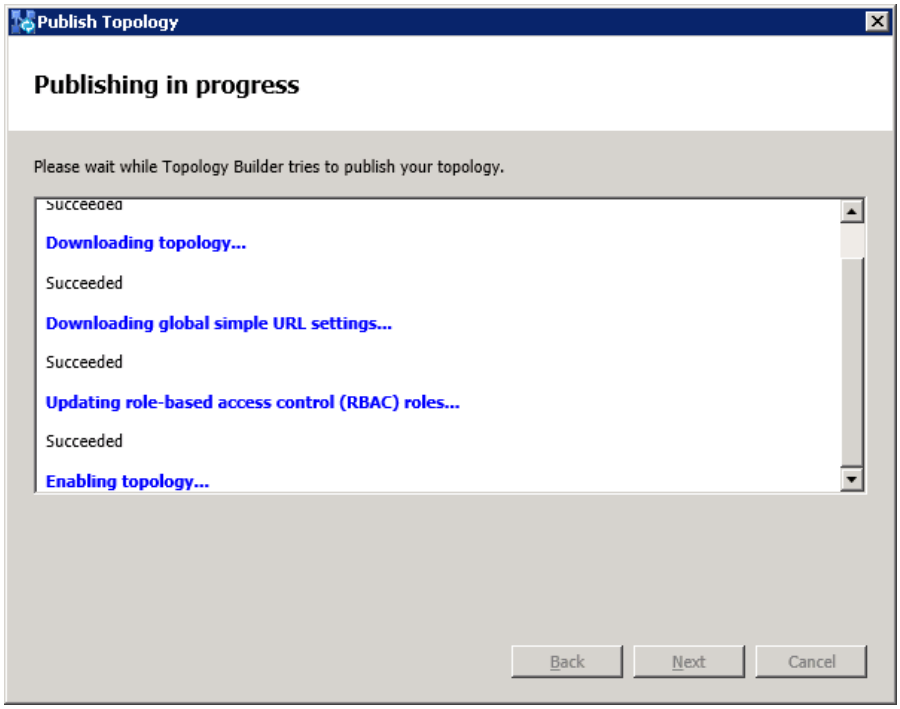
The following is displayed:

Figure 3-11: Publish the Topology



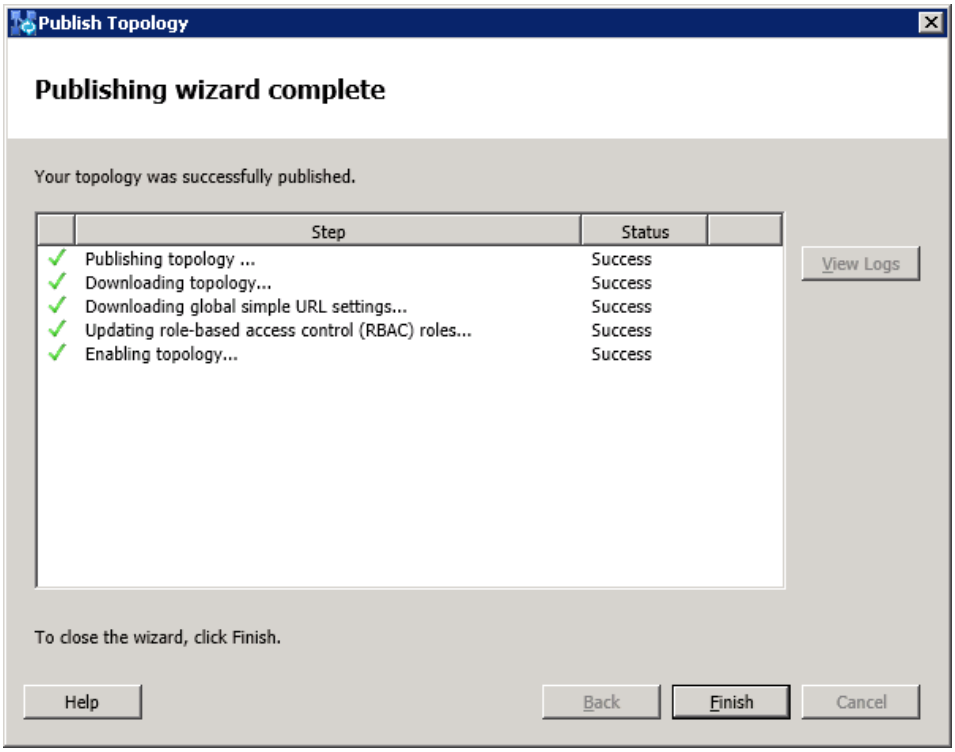
9. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



11. Click **Finish**.

3.2 Configuring the "Route" on Lync Server 2013

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

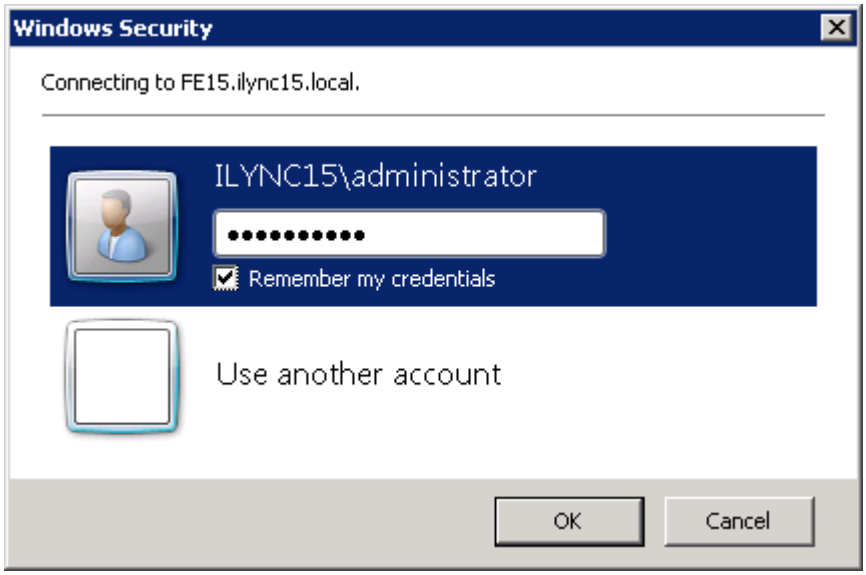
➢ **To configure the "route" on Lync Server 2013:**

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

Figure 3-14: Opening the Lync Server Control Panel

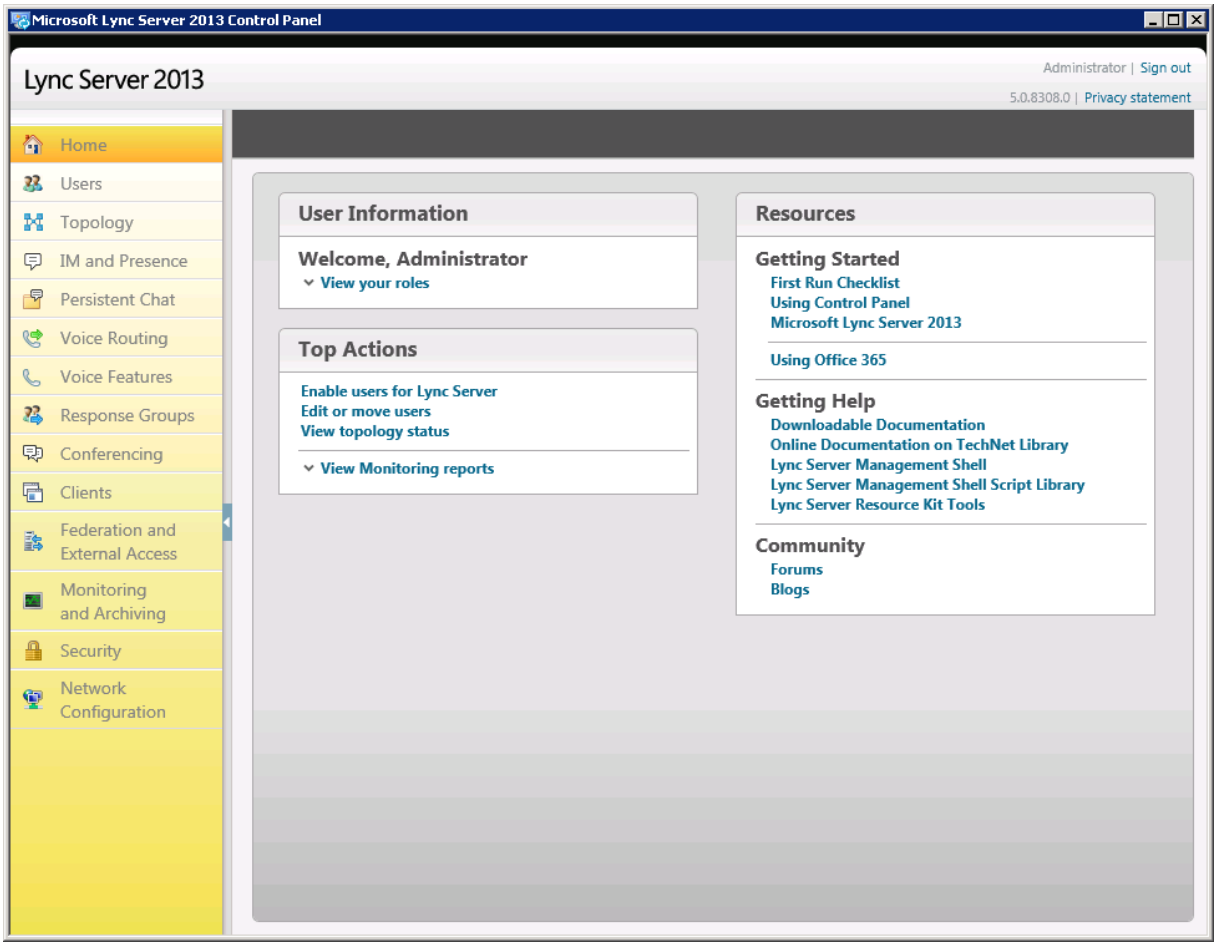
You're prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials



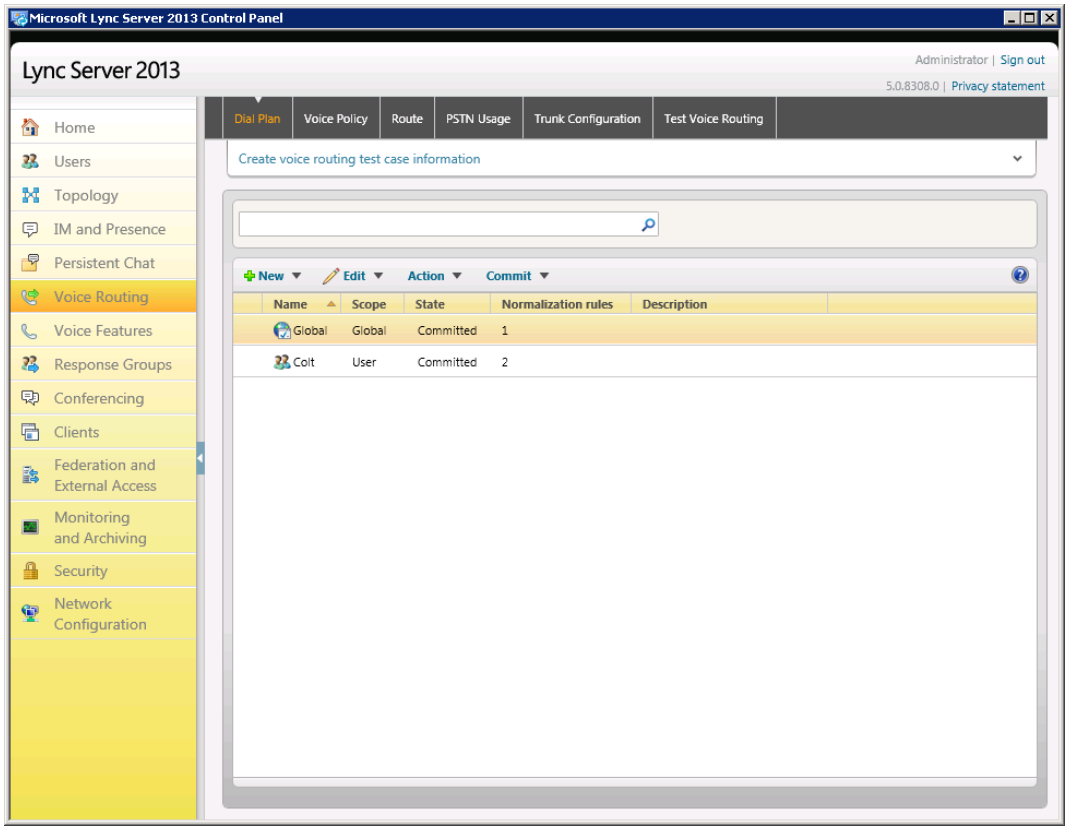
2. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

Figure 3-16: Microsoft Lync Server 2013 Control Panel



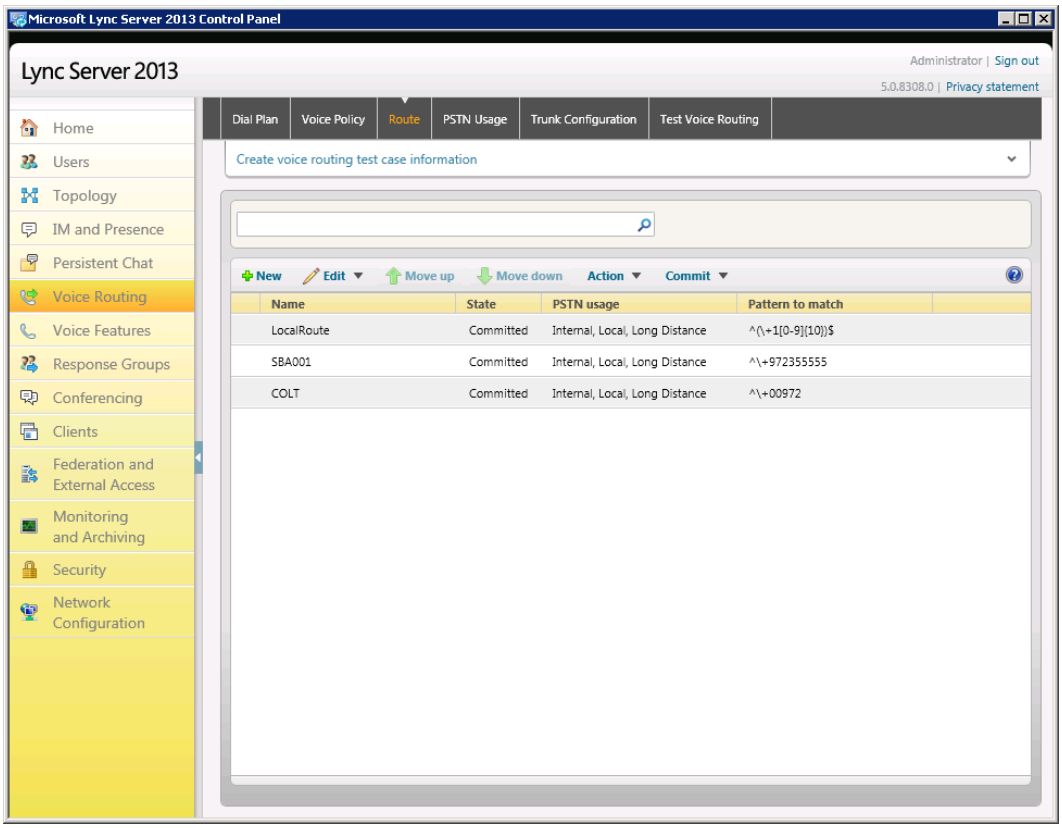
3. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



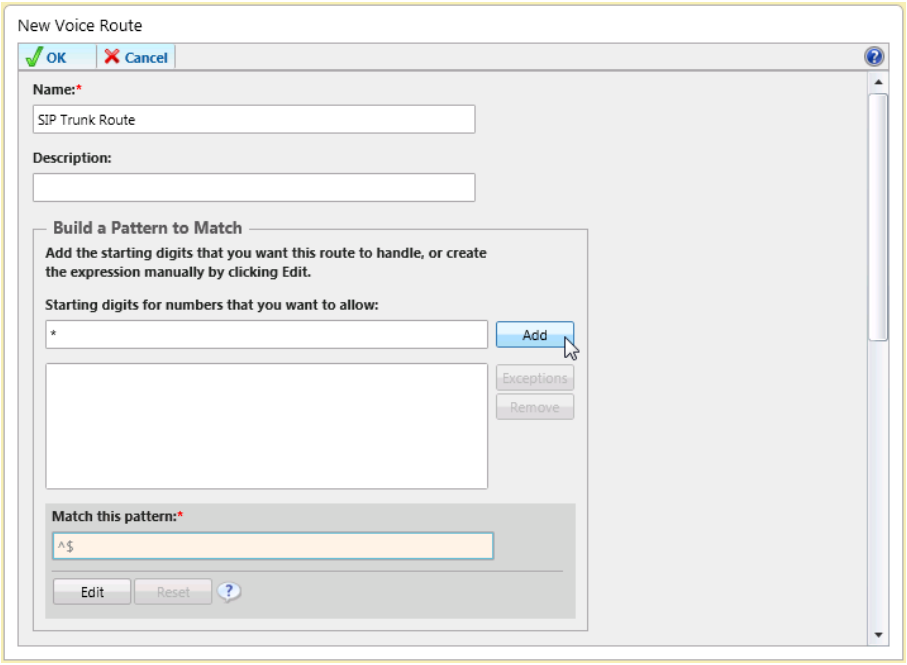
4. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



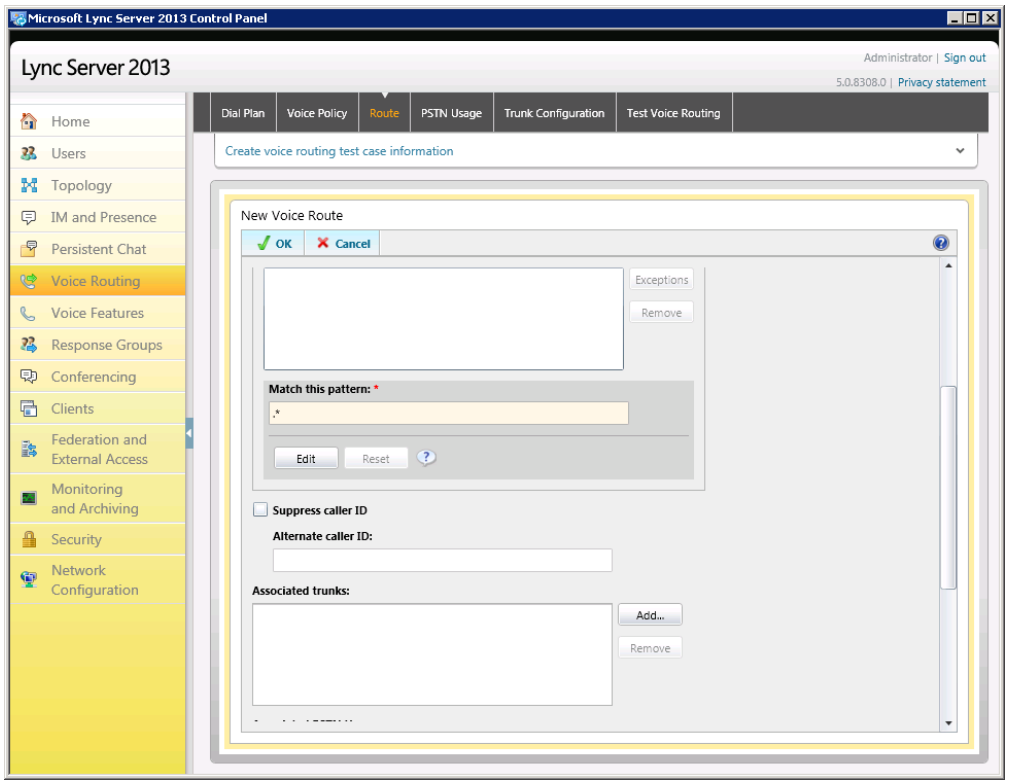
5. Click **New**; the New Voice Route page appears:

Figure 3-19: Adding New Voice Route



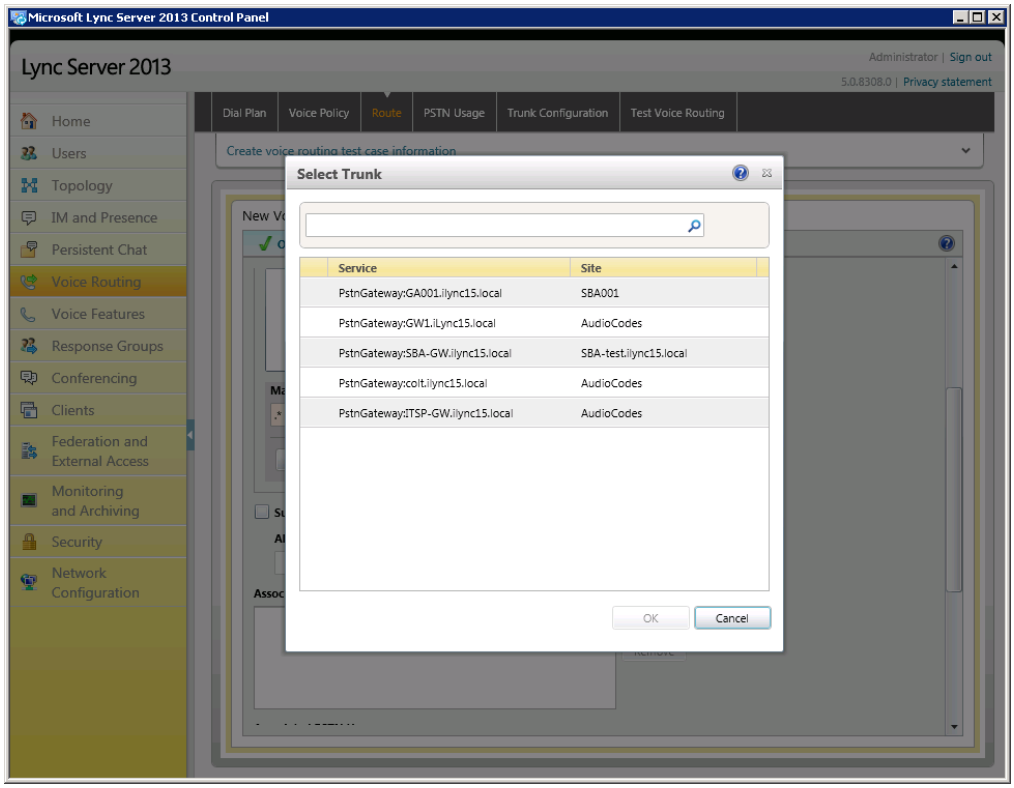
6. In the 'Name' field, enter a name for this route (e.g., **SIP Trunk Route**).
7. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., ***** to match all numbers), and then click **Add**.

Figure 3-20: Adding New Trunk



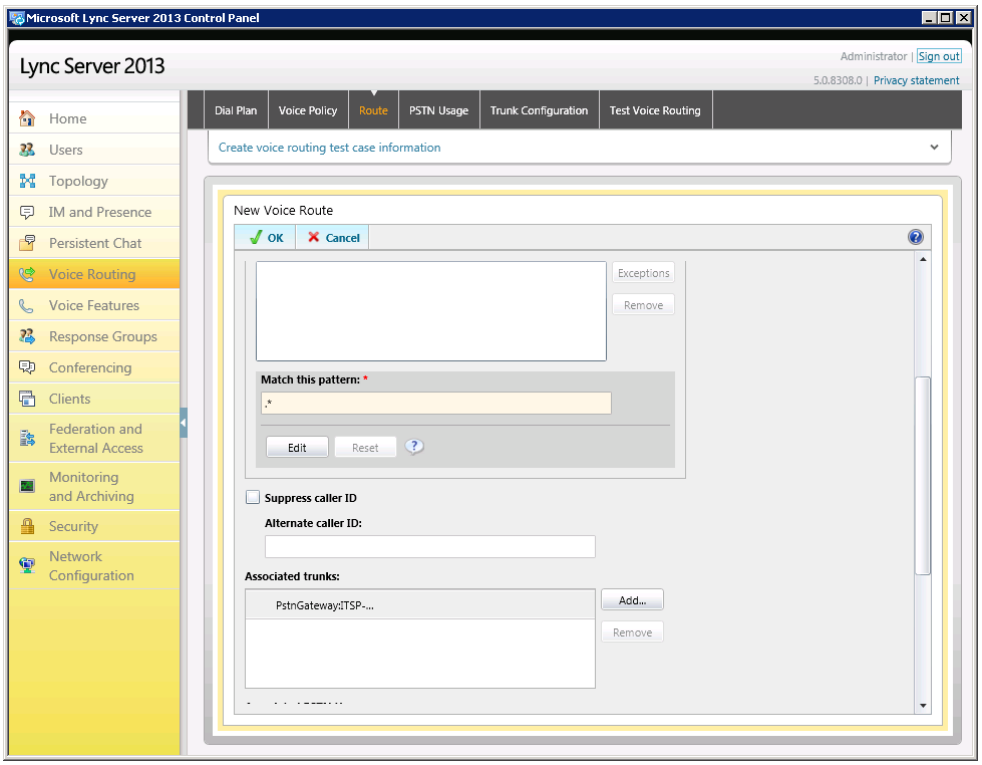
8. Associate the route with the E-SBC Trunk that you created:
   a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-21: List of Deployed Trunks



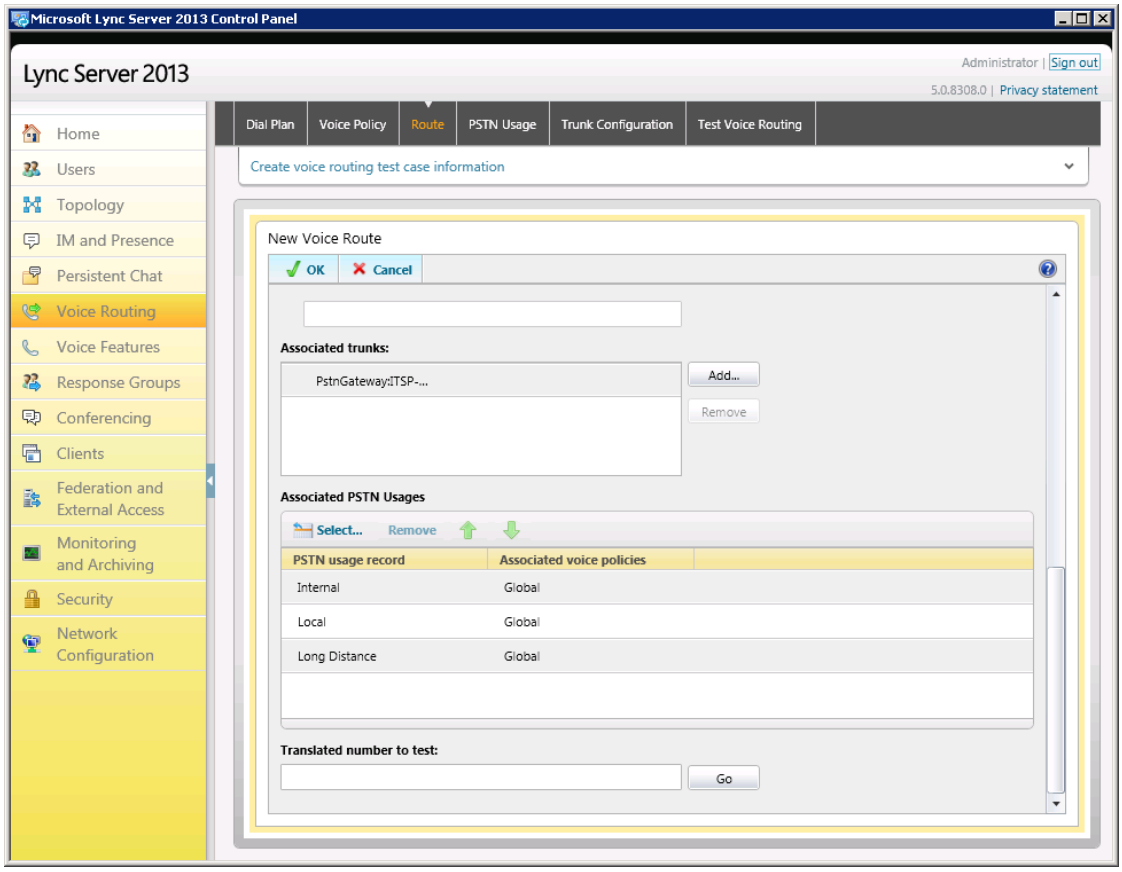
   b. Select the E-SBC Trunk you created, and then click **OK**; the trunk is added to the 'Associated Trunks' group list:

Figure 3-22: Selected E-SBC Trunk



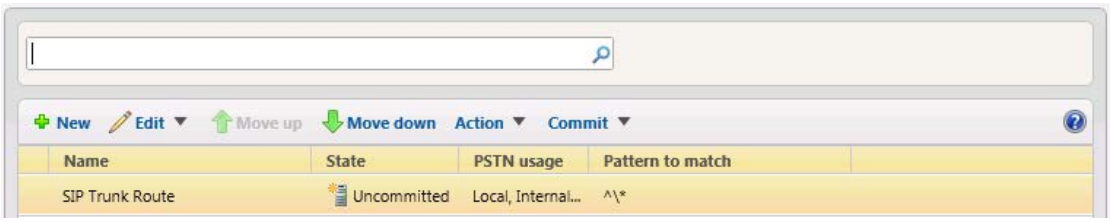
9. Associate a PSTN Usage with this route:
   a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-23: Associating PSTN Usage to Route



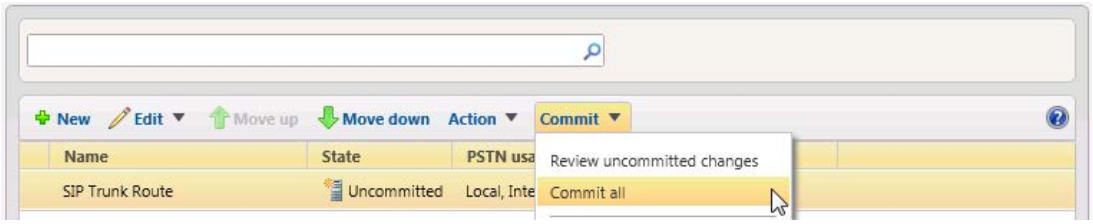
10. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed:

Figure 3-24: Confirmation of New Voice Route



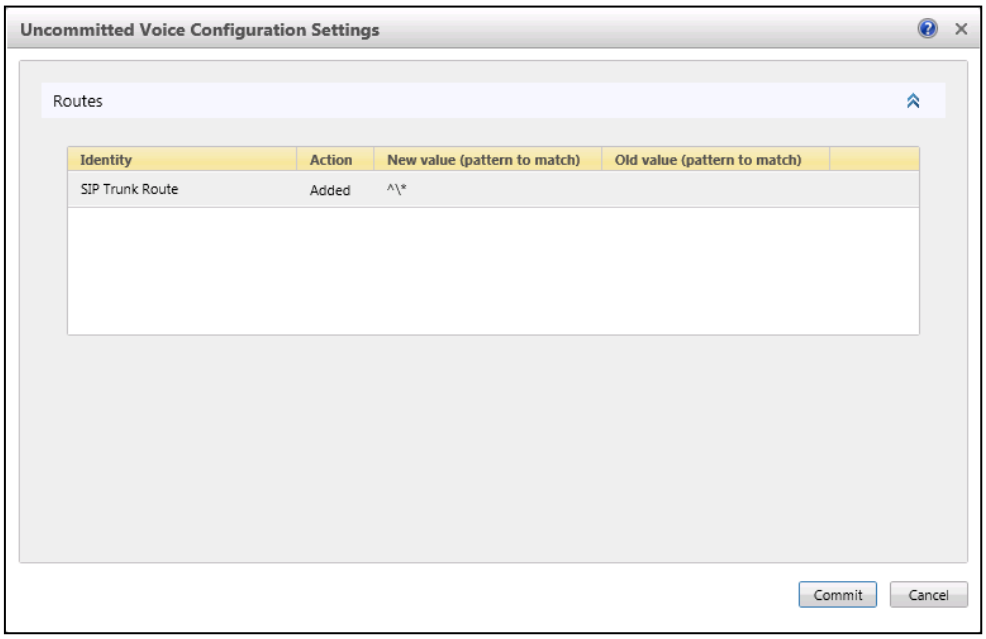
11. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-25: Committing Voice Routes



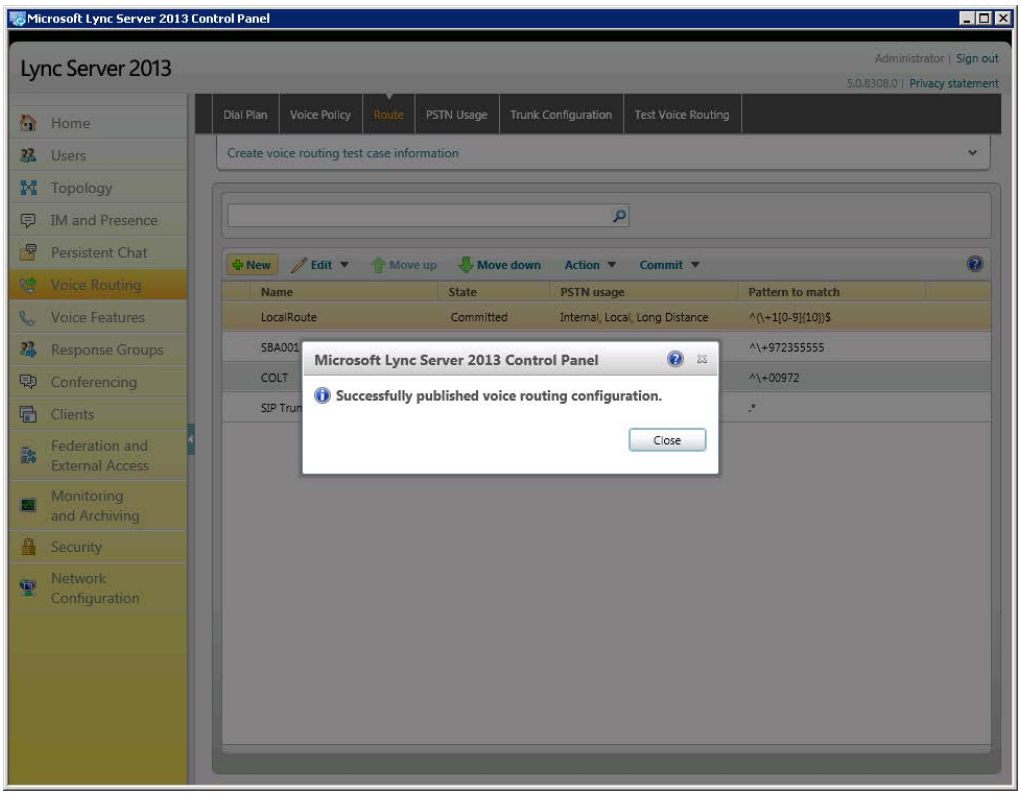
The Uncommitted Voice Configuration Settings page appears:

Figure 3-26: Uncommitted Voice Configuration Settings



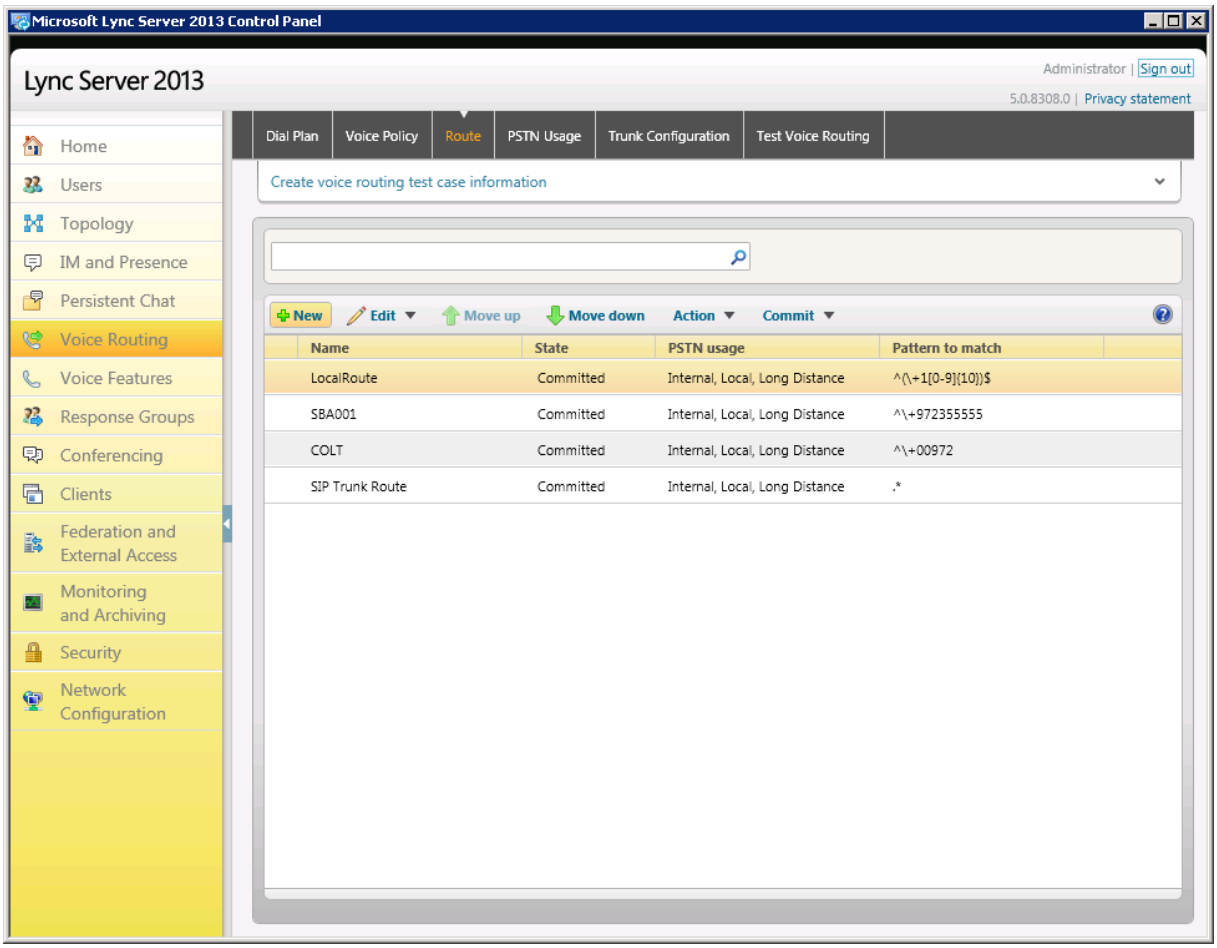
12. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-27: Confirmation of Successful Voice Routing Configuration



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

Figure 3-28: Voice Routing Screen Displaying Committed Routes

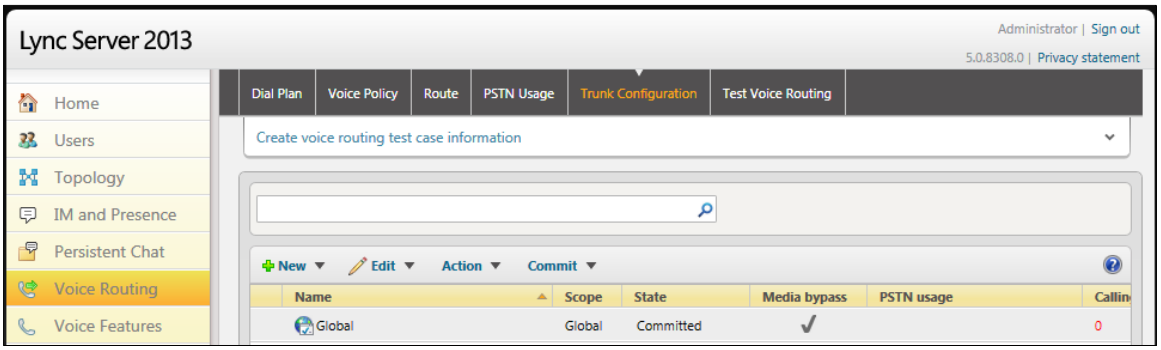


14. For ITSPs that implement a call identifier, continue with the following steps:

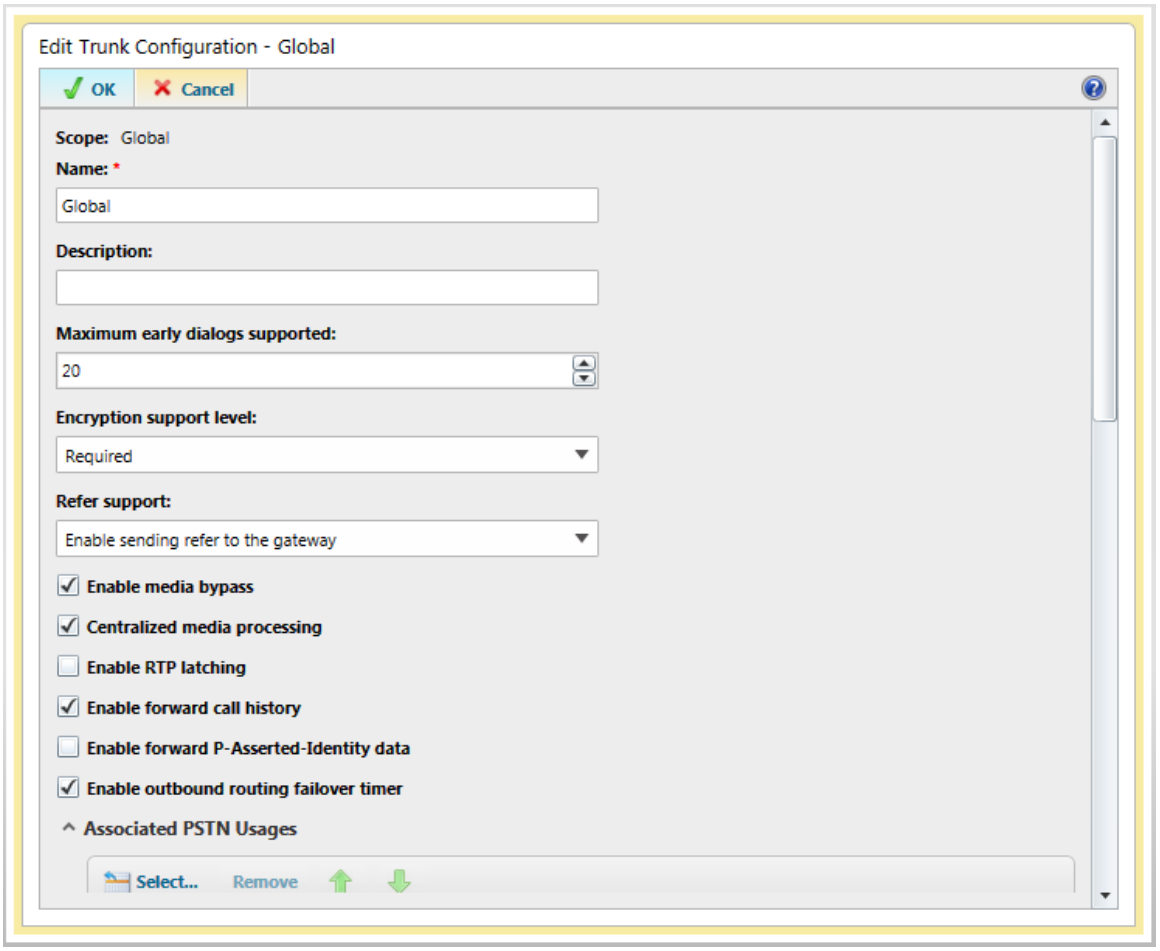
Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Lync user number). This ID is required by Bell Canada's SIP Trunk in the P-Asserted-Identity header. Using a Message Manipulation rule (see Section 4.13 on page 71), the device adds this ID to the P-Asserted-Identity header in the sent INVITE message.

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

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



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



c. Select the **Enable forward call history** option, and then click **OK**.

d. Repeat Steps 11 through 13 to commit your settings.

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This section shows how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 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 include the following main areas:

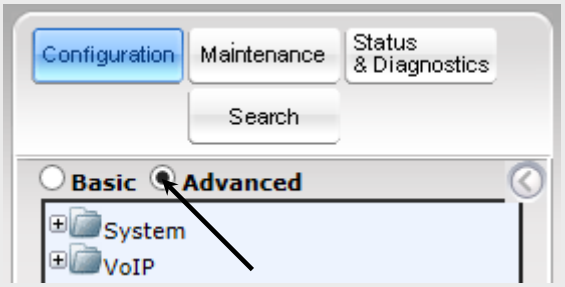
- E-SBC WAN interface - Bell Canada SIP Trunking environment
- E-SBC LAN interface - Lync Server 2013 environment

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

Notes:

- For implementing Microsoft Lync and Bell Canada's 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, make sure that the E-SBC's Web interface navigation tree is in **Advanced** display mode. To do this, select the **Advanced** option, as shown below:



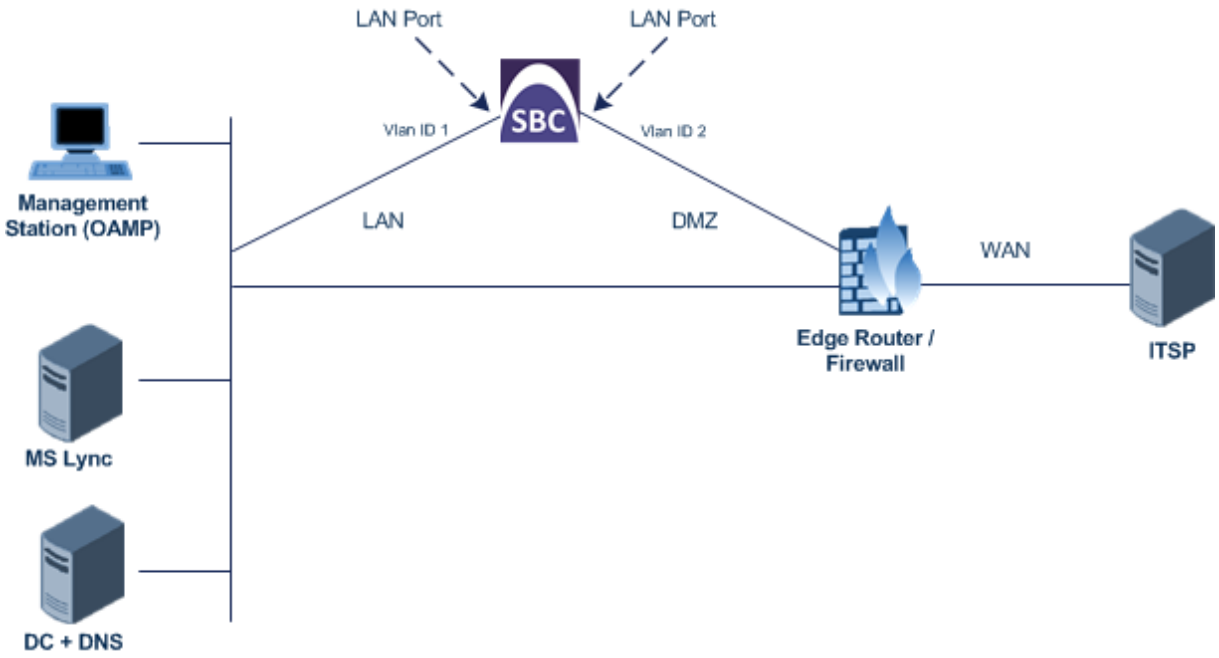
Note that when the E-SBC is reset, the navigation tree reverts to **Basic** display mode.

4.1 Step 1: Configure IP Network Interfaces

This step shows how to configure the E-SBC's IP network interfaces. There are several methods of deploying the E-SBC but the interoperability test topology employs this 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 VLANs

This step shows how to define VLANs for each of the following interfaces:

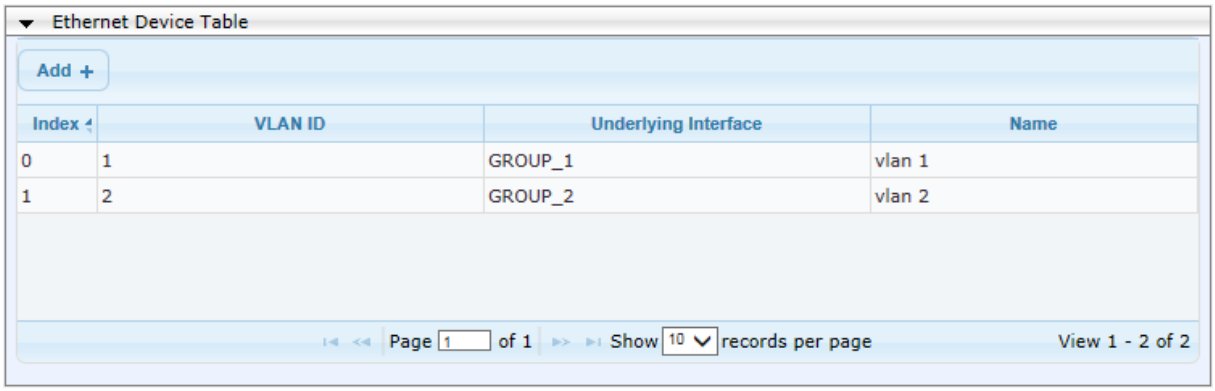
- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "WANSP")

➢ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
2. There will be one existing row for VLAN ID 1 and an underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	**1**
VLAN ID	**2**
Underlying Interface	**GROUP_2** (Ethernet port group)
Name	**vlan 2**

Figure 4-2: Configured VLAN IDs in Ethernet Device Table



4.1.2 Step 1b: Configure Network Interfaces

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

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

➢ **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	**10.15.45.101** (E-SBC IP address)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.25.1**
Underlying Device	**vlan 1**

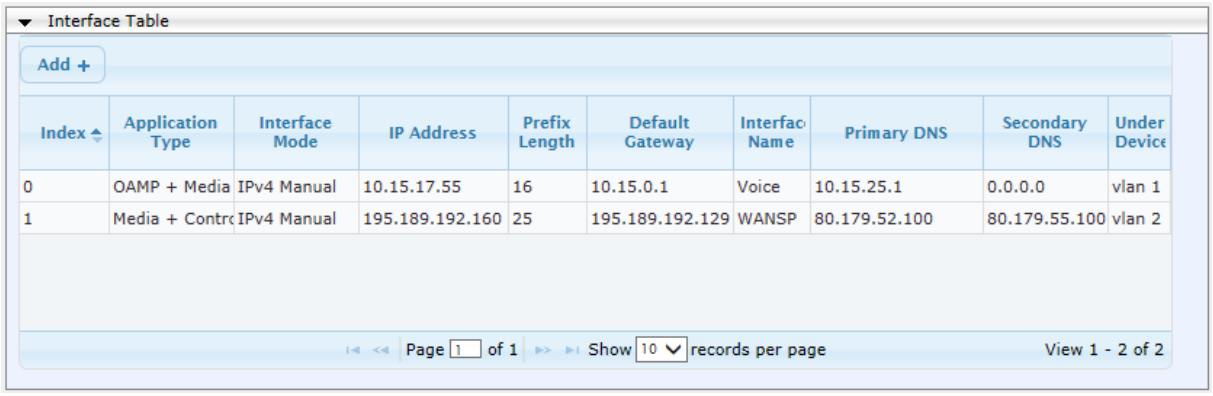
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.189.192.156** (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	**WANSP**
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Device	**vlan 2**

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

Figure 4-3 shows the configured IP network interfaces:

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



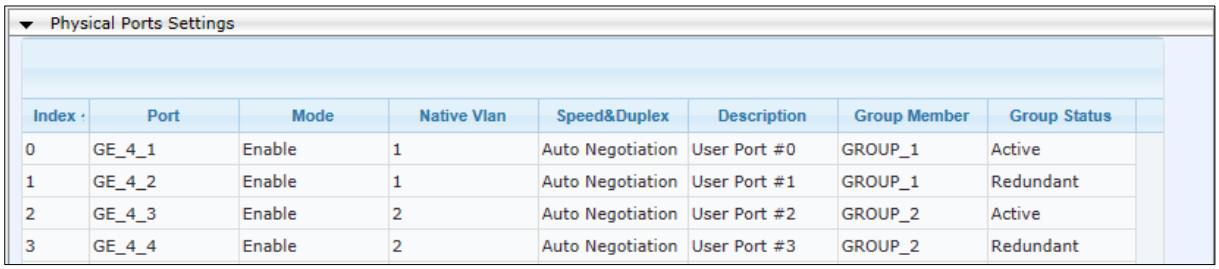
4.1.3 Step 1c: Configure the Native VLAN ID

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

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

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

Figure 4-4: Configured Port Native VLAN


Physical Ports Settings

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_4_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
2	GE_4_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
3	GE_4_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

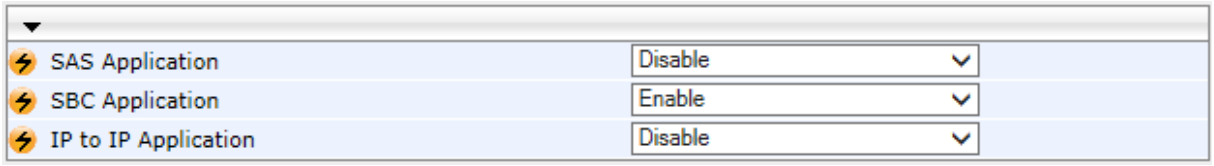
4.2 Step 2: Enable the SBC Application

This step shows how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-5: Enabling SBC Application



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 87).

4.3 Step 3: Configure Signaling Routing Domains

This step shows 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.

The SRD comprises:

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

4.3.1 Step 3a: Configure Media Realms

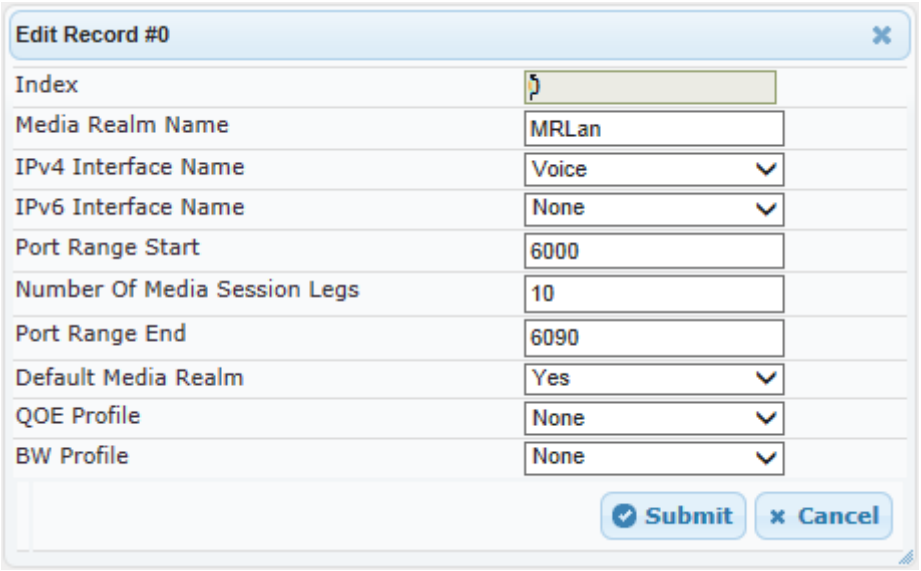
This step shows how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and the other for external (WAN) traffic.

➢ **To configure Media Realms:**

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

Parameter	Value
Index	**0**
Media Realm Name	**MRLan** (descriptive name)
IPv4 Interface Name	**Voice**
Port Range Start	**6000** (represents the lowest UDP port number used for media on the LAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	**1**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**WANSP**
Port Range Start	**7000** (represents the lowest UDP port number used for media on the WAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

Figure 4-7: Configuring Media Realm for WAN

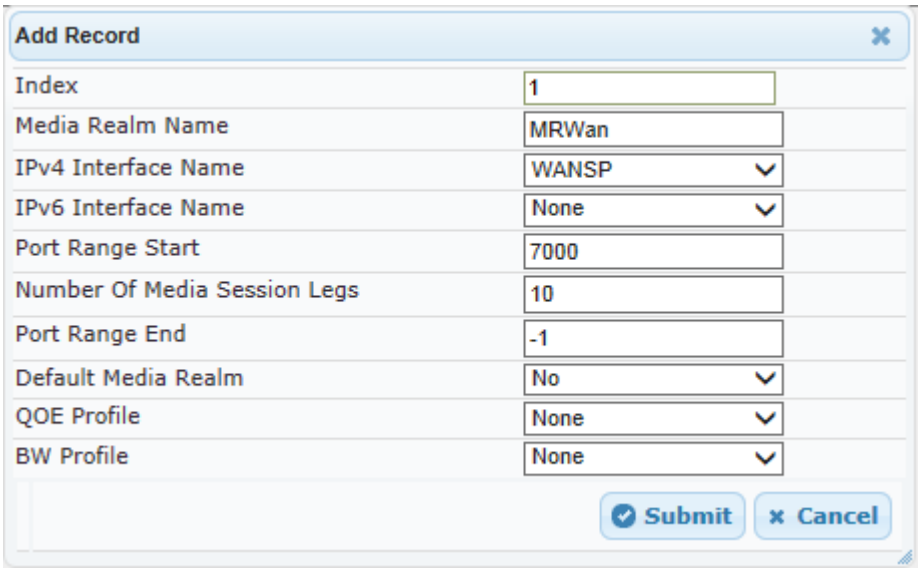
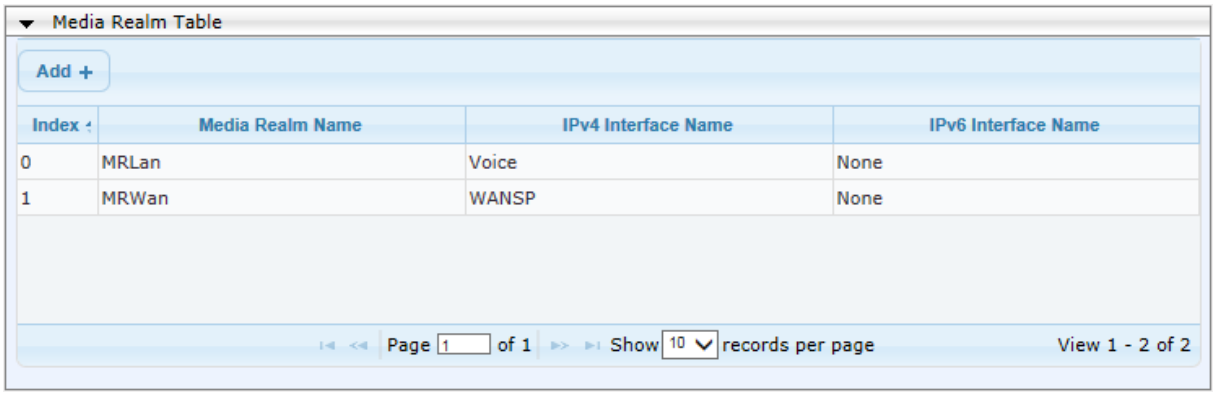


Figure 4-8 shows the configured Media Realms:

Figure 4-8: Configured Media Realms in Media Realm Table



4.3.2 Step 3b: Configure SRDs

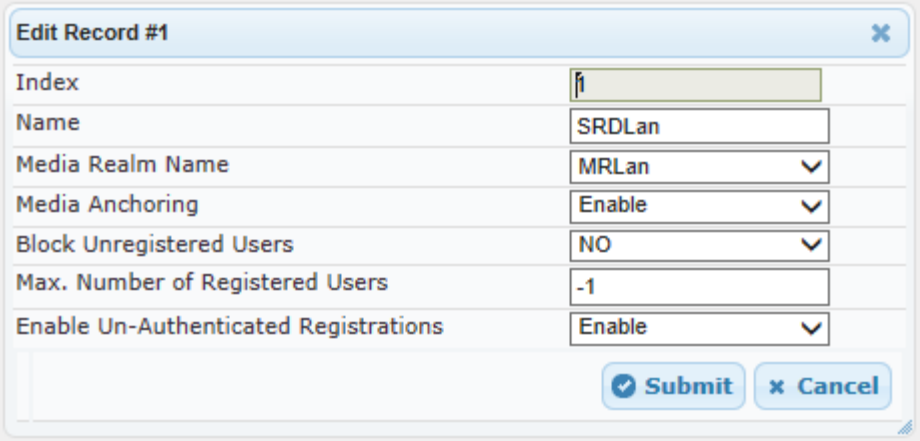
This step shows how to configure the SRDs.

➢ **To configure SRDs:**

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

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

Figure 4-9: Configuring LAN SRD



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

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

Figure 4-10: Configuring WAN SRD

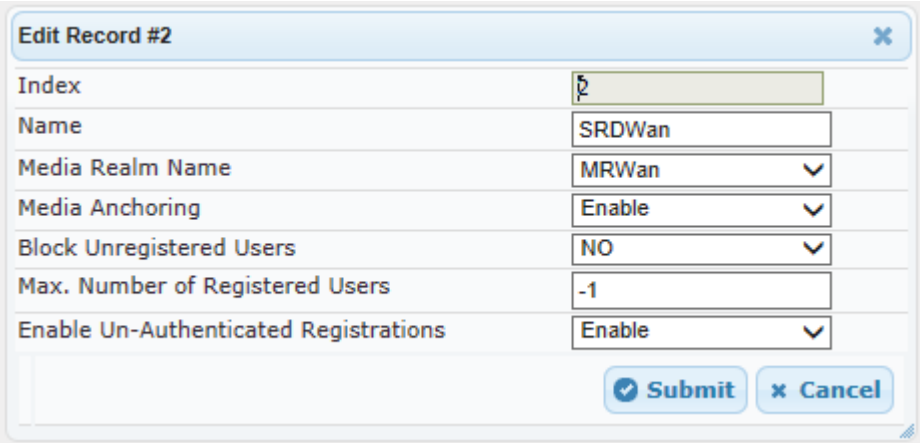
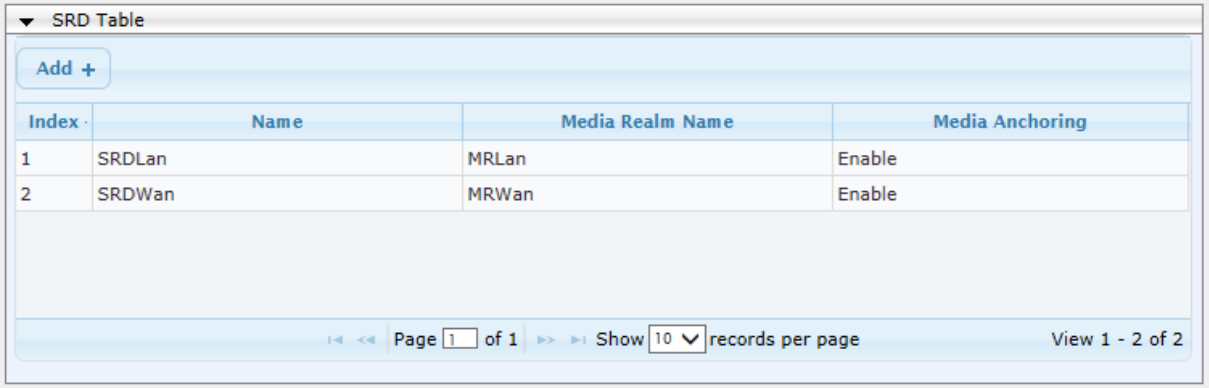


Figure 4-11 shows the configured SRDs:

Figure 4-11: Configured SRDs in SRD Table



4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

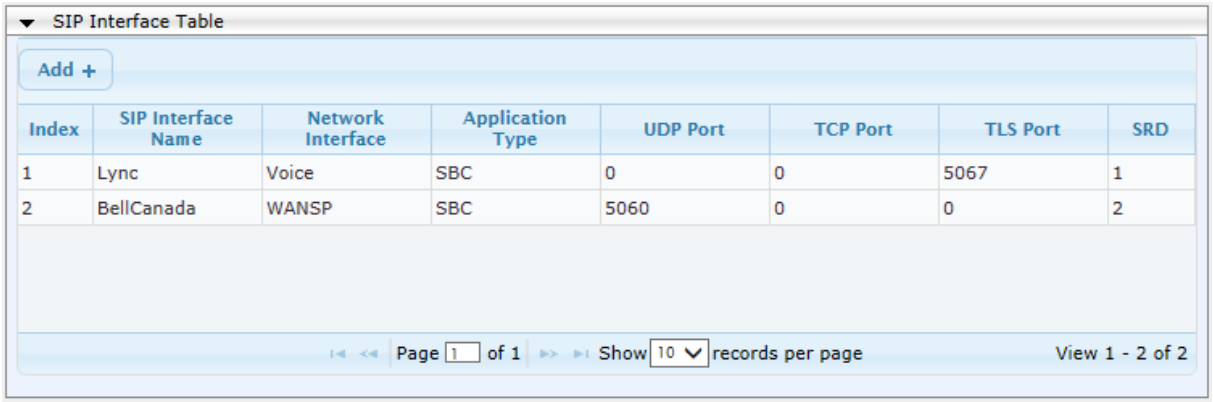
Parameter	Value
Index	**1**
Interface Name	**Lync** (arbitrary descriptive name)
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**1**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
Interface Name	**BellCanada** (arbitrary descriptive name)
Network Interface	**WANSP**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	**0**
SRD	**2**

Figure 4-12 shows the configured SIP Interfaces:

Figure 4-12: Configured SIP Interfaces in SIP Interface Table



4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Lync Server 2013
- Bell Canada's SIP Trunk

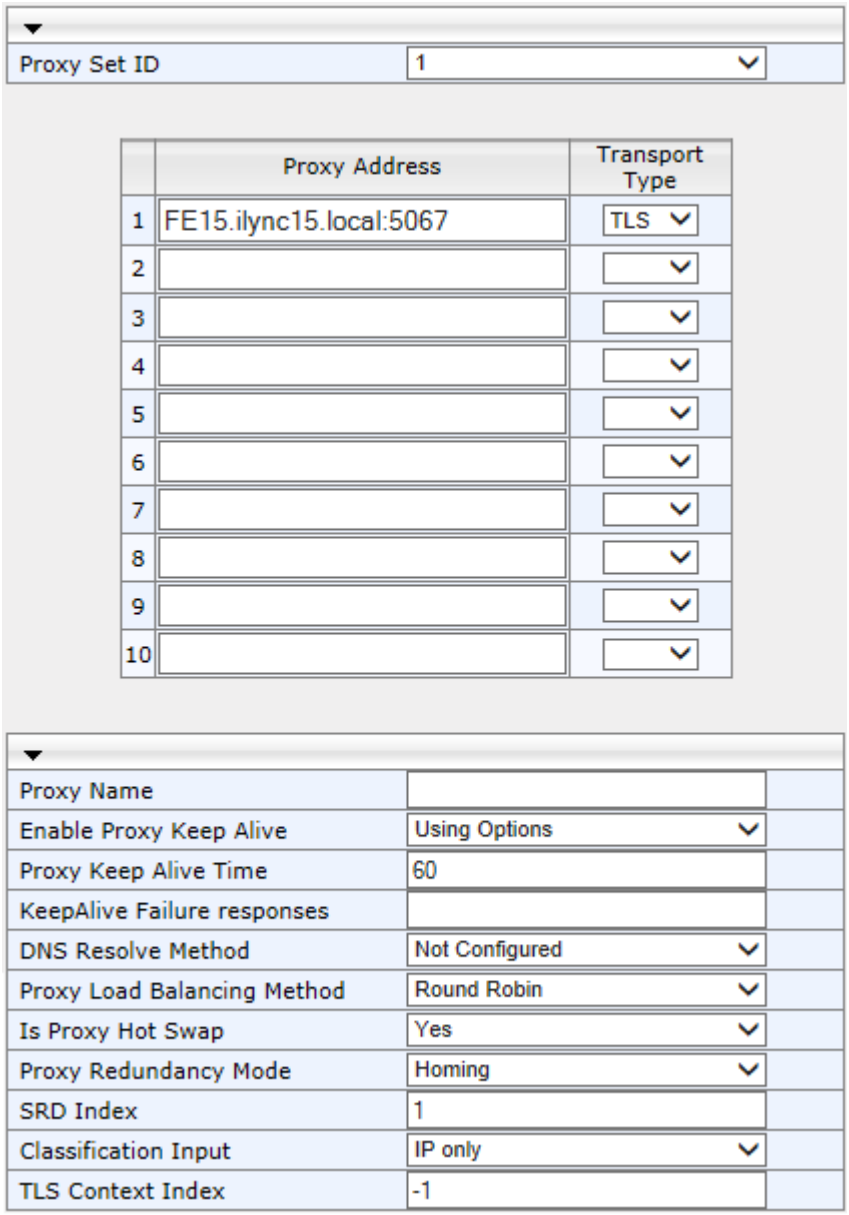
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

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

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**FE15.ilync15.local:5067** (Lync Server 2013 IP address / FQDN and destination port)
Transport Type	**TLS**
Proxy Name	**Lync** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	**1**

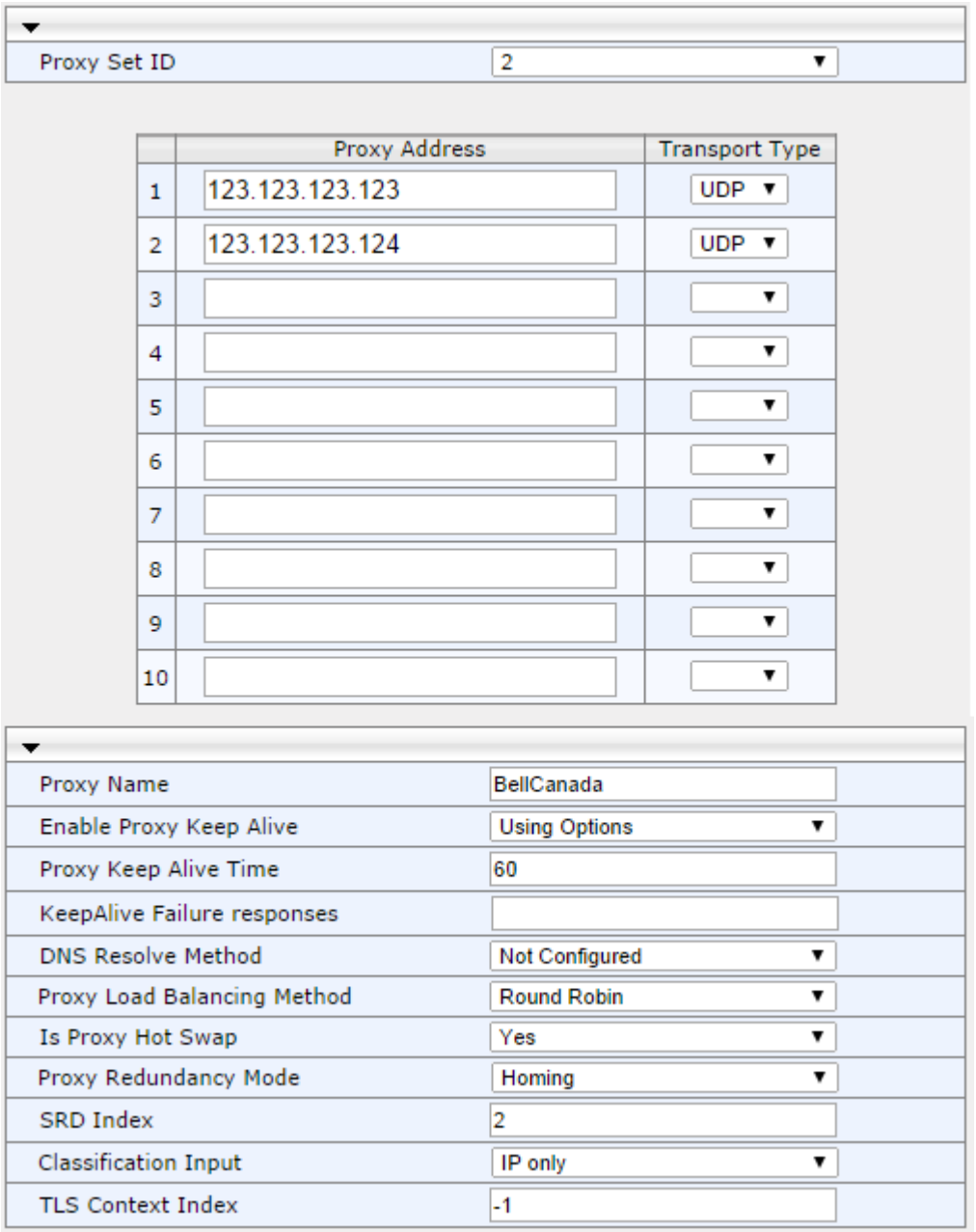
Figure 4-13: Configuring Proxy Set for Microsoft Lync Server 2013



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

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**123.123.123.123** (Bell Canada IP address / FQDN and destination port). *For Load Balancing, enter the Load Balancer IP address.*
Proxy Address	**123.123.123.124**
Transport Type	**UDP**
Proxy Name	**BellCanada** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	**2**

Figure 4-14: Configuring Proxy Set for Bell Canada's SIP Trunk



4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.16 on page 87).

4.5 Step 5: Configure IP Groups

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

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

- Lync Server 2013 (Mediation Server) located on LAN
- Bell Canada's SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Configure an IP Group for the Lync Server 2013 Mediation Server:

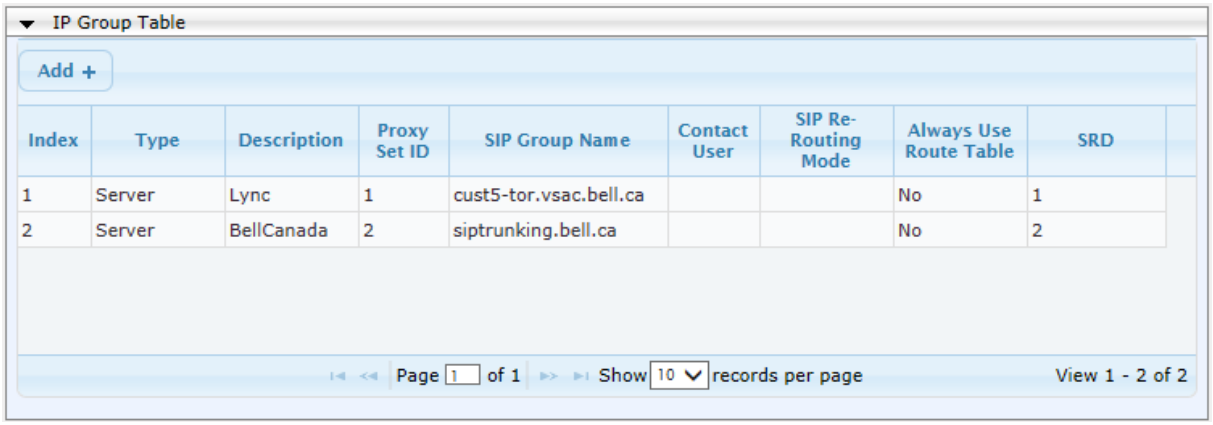
Parameter	Value
Index	**1**
Type	**Server**
Description	**Lync** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**cust5-tor.vsac.bell.ca** (according to ITSP requirement)
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

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

Parameter	Value
Index	**2**
Type	**Server**
Description	**BellCanada** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**siptrunking.bell.ca** (according to ITSP requirement)
SRD	**2**
Media Realm Name	**MRWan**
IP Profile ID	**2**
Classify By Proxy Set	**Disable** (*For Load Balancing configuration only. Classification is done according to the Classification Table; see Section 4.15.1 on page 83*)

The figure below shows the configured IP Groups:

Figure 4-15: Configured IP Groups in IP Group Table


IP Group Table

Add +

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	Lync	1	cust5-tor.vsac.bell.ca			No	1
2	Server	BellCanada	2	siptrunking.bell.ca			No	2

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

4.6 Step 6: Configure IP Profiles

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

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

- Microsoft Lync Server 2013 - to operate in secure mode using SRTP and TLS
- Bell Canada's SIP Trunk - to operate in non-secure mode using RTP and UDP

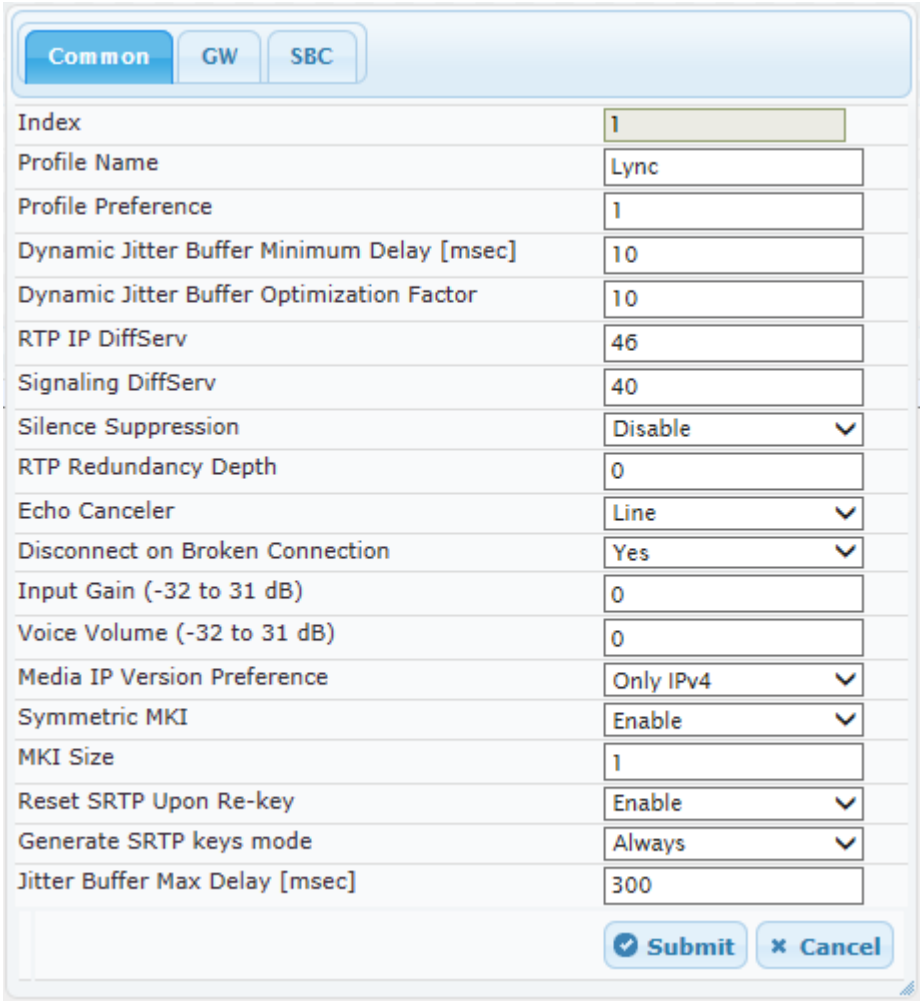
Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 4.5 on page 44).

➢ **To configure IP Profiles:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Profile Name	**Lync** (arbitrary descriptive name)
Symmetric MKI	**Enable**
MKI Size	**1**
Reset SRTP State Upon Re-key	**Enable**
Generate SRTP keys mode:	**Always**

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

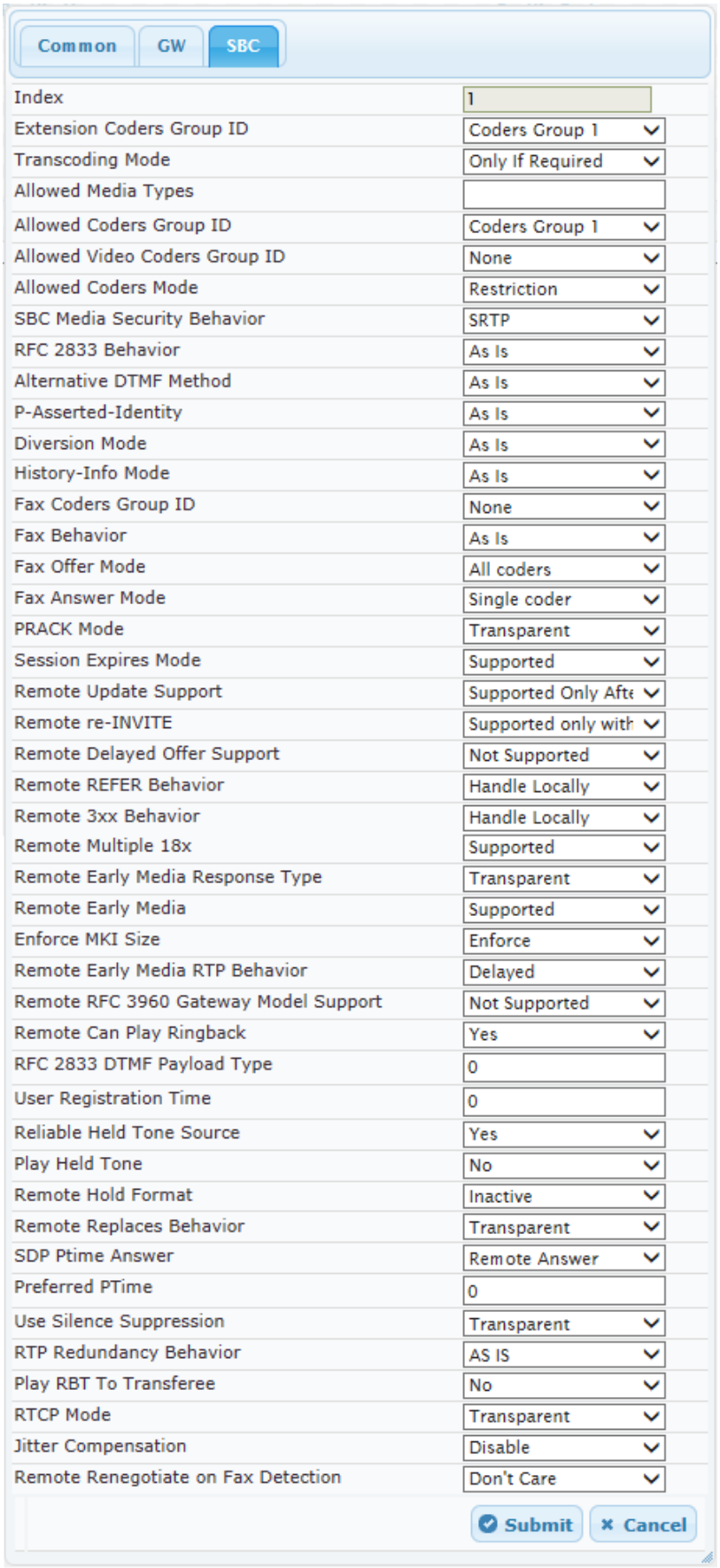


4. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Extension Coders Group ID	**Coders Group 1**
Allowed Coders Group ID	**Coders Group 1**
Allowed Coders Mode	**Restriction** (only Allowed Coders will be introduced in SDP offer)
Media Security Behavior	**SRTP**
Session Expires Mode	**Supported** (required because Bell Canada's SIP Trunk does not support Session Timer, so SBC should negotiate it with Lync)
Remote Update Support	**Supported Only After Connect**
Remote Re-Invite Support	**Supported Only With SDP**
Remote Delayed Offer Support	**Not Supported**
Remote Refer Behavior	**Handle Locally** (required because Lync Server 2013 does not support receipt of SIP REFER)

Parameter	Value
Remote 3xx Behavior	**Handle Locally** (required because Lync Server 2013 does not support receipt of SIP 3xx responses)
Enforce MKI Size	**Enforce**
Remote Early Media RTP Behavior	**Delayed** (required because Lync Server 2013 does not send an RTP immediately to the remote side when it sends a SIP 18x response)
Remote Hold Format	**Inactive** (required because Bell Canada's SIP Trunk sends 0.0.0.0 for Hold but Lync Server 2013 does not recognize that format)

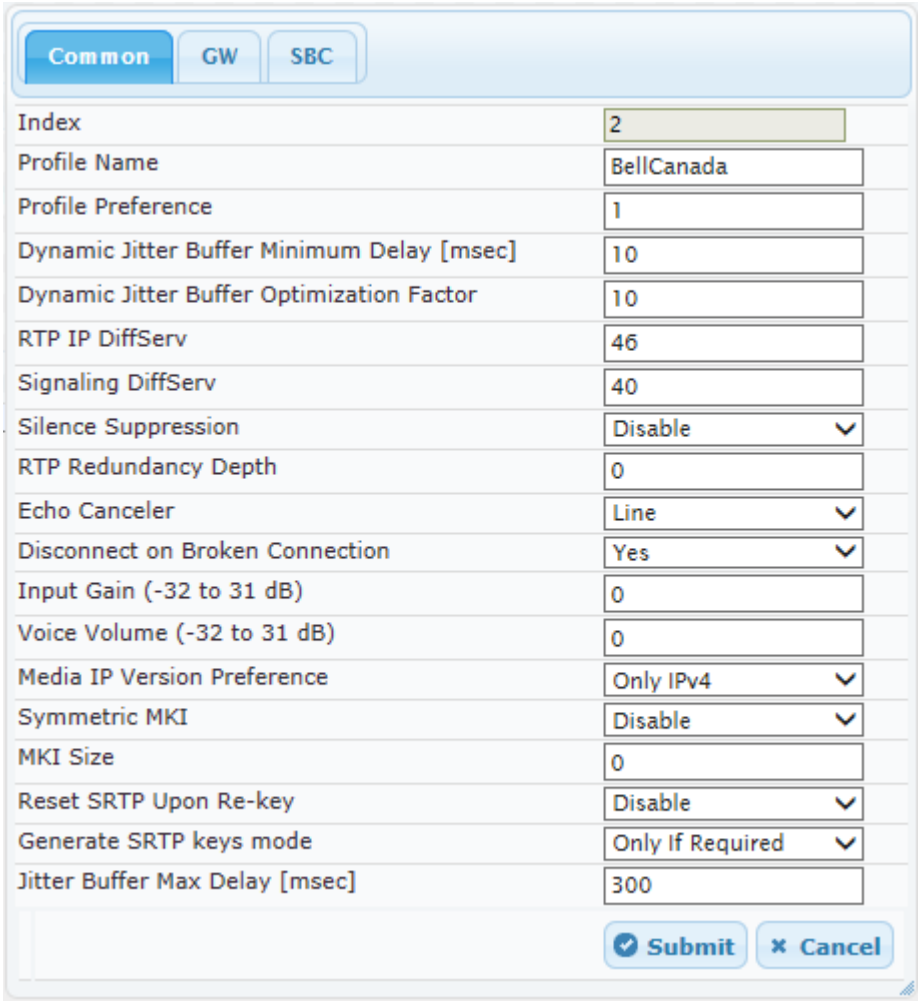
Figure 4-17: Configuring IP Profile for Lync Server 2013 – SBC Tab



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

Parameter	Value
Index	**2**
Profile Name	**BellCanada** (arbitrary descriptive name)

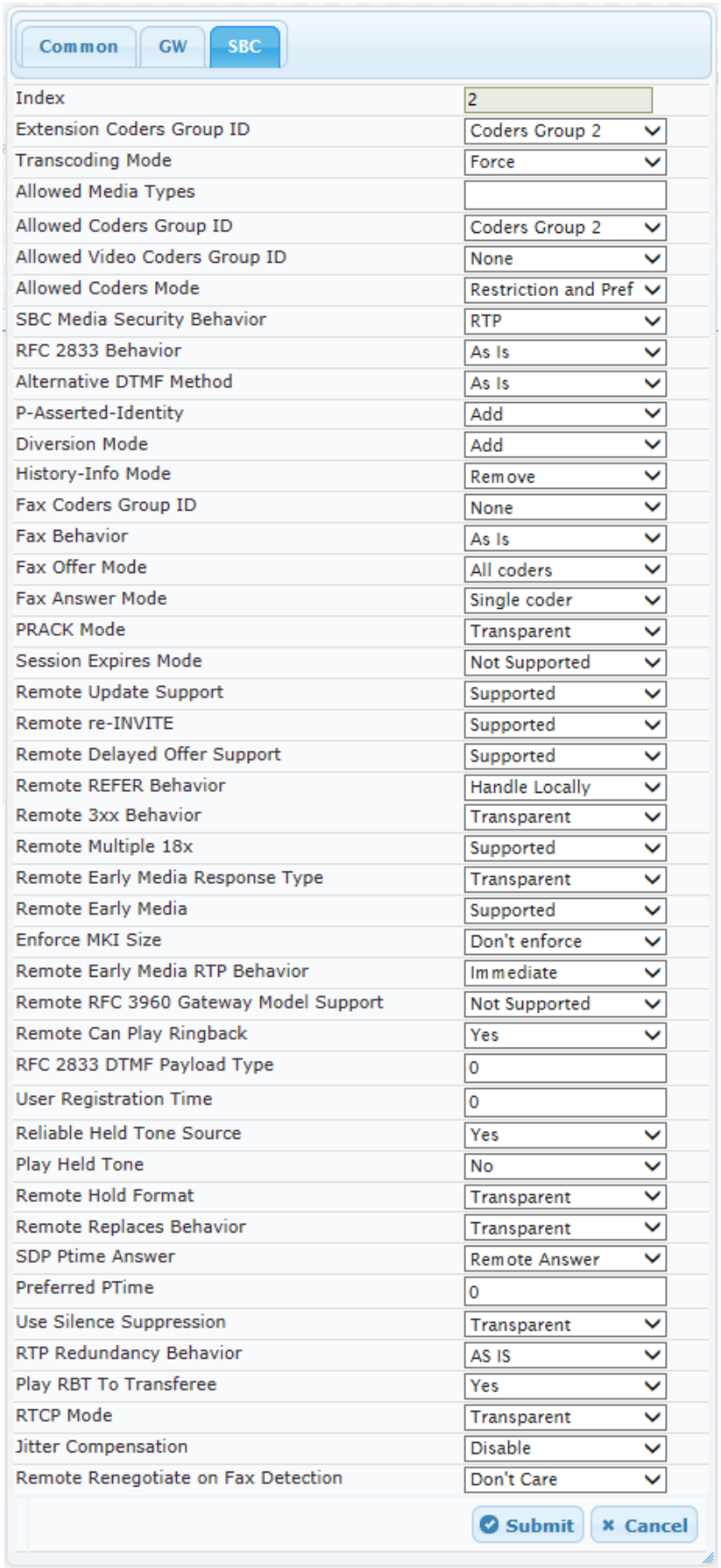
Figure 4-18: Configuring IP Profile for Bell Canada's SIP Trunk – Common Tab



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

Parameter	Value
Profile ID	**2**
Extension Coders Group ID	**Coders Group 2**
Transcoding Mode	**Force** (required for fixing Ring Back Tone issue, mentioned under 'Known Limitations')
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Restriction and Preference** (lists Allowed Coders first and then original coders in received SDP offer)
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** (required for anonymous calls)
Diversion Mode	**Add** (required for transferred calls)
History-Info Mode	**Remove**
SBC Session Expires Mode	**Not Supported**
Remote REFER Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to the SIP Trunk)
Play RBT To Transferee	**Yes**

Figure 4-19: Configuring IP Profile for Bell Canada's SIP Trunk – SBC Tab



4.7 Step 7: Configure Coders

This step shows how to configure coders (termed *Coder Group*). As Lync Server 2013 supports the G.711 coder while the network connection to Bell Canada's 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.

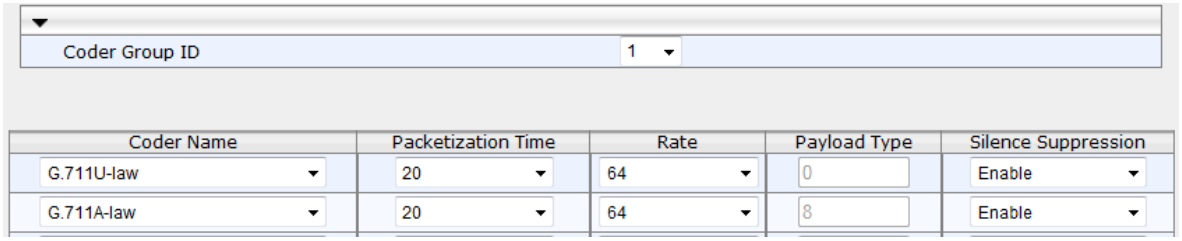
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 46).

➢ **To configure coders:**

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

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

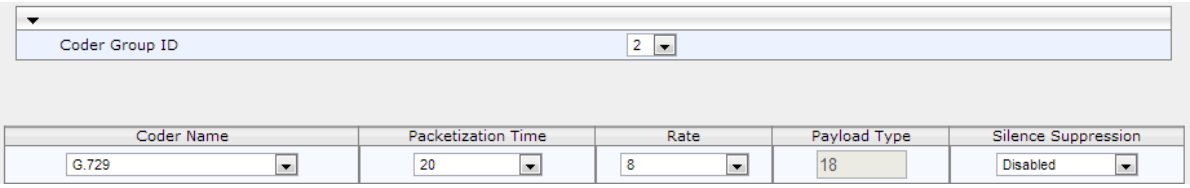
Figure 4-20: Configuring Coder Group for Lync Server 2013



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

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

Figure 4-21: Configuring Coder Group for Bell Canada's SIP Trunk



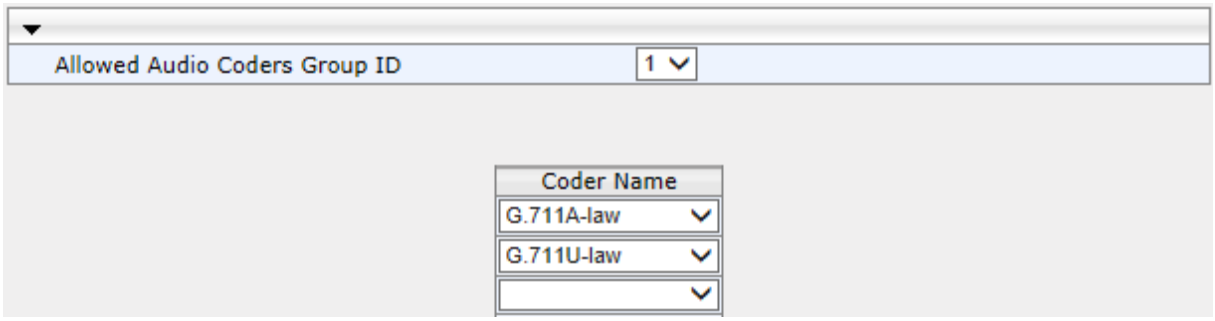
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Bell Canada SIP Trunk uses the G.729 coder *whenever possible*. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Bell Canada SIP Trunk in the previous step (see Section 4.6 on page 46).

➢ **To set a preferred coders:**

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

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

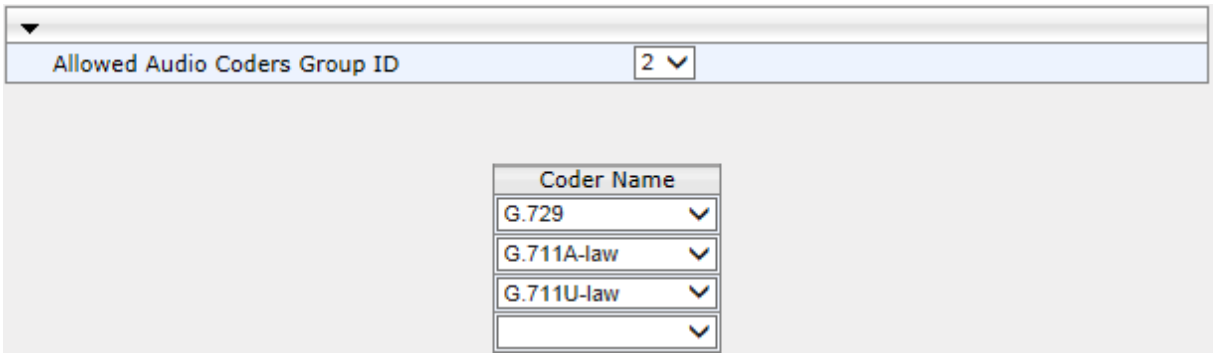
Figure 4-22: Configuring Allowed Coders Group for Lync



3. Configure an Allowed Coders for Bell Canada's SIP Trunk as follows:

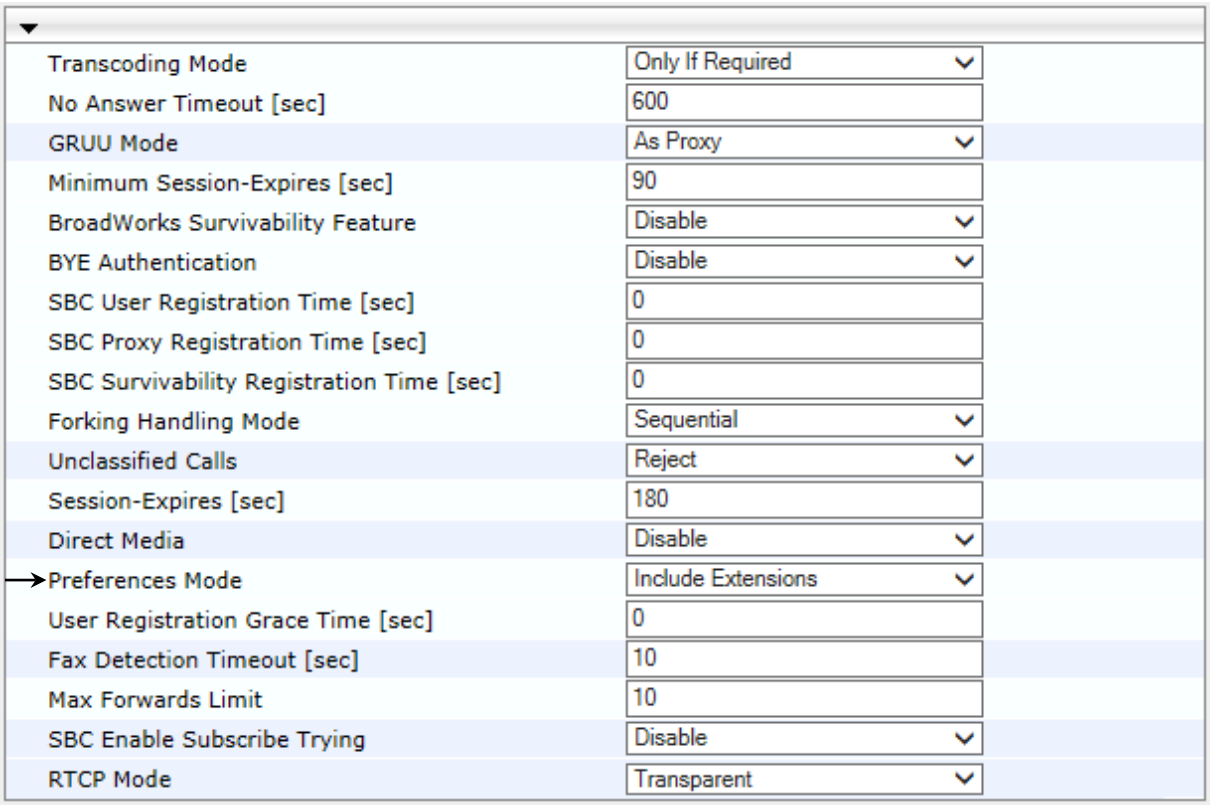
Parameter	Value
Allowed Coders Group ID	**2**
Coder Name	**G.729**
Coder Name	**G.711A-law**
Coder Name	**G.711U-law**

Figure 4-23: Configuring Allowed Coders Group for Bell Canada's SIP Trunk



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

Figure 4-24: SBC Preferences Mode



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

4.8 Step 8: Configure SIP TLS Connection

This section shows how to configure the E-SBC for using a TLS connection with the Lync Server 2013 Mediation Server. This is essential for a secure SIP TLS connection.

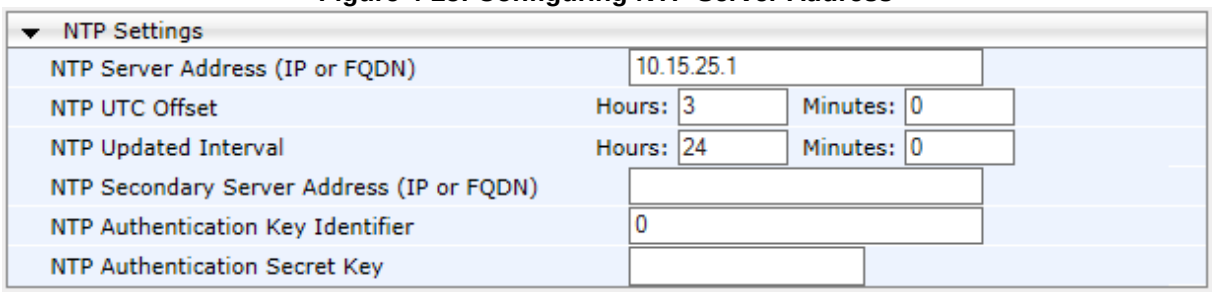
4.8.1 Step 8a: Configure the NTP Server Address

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

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

1. Open the Application Settings page (**Configuration** tab > **System** > **Application Settings**).
2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., **10.15.25.1**).

Figure 4-25: Configuring NTP Server Address



3. Click **Submit**.

4.8.2 Step 8b: Configure a Certificate

This step shows how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Lync Server 2013.

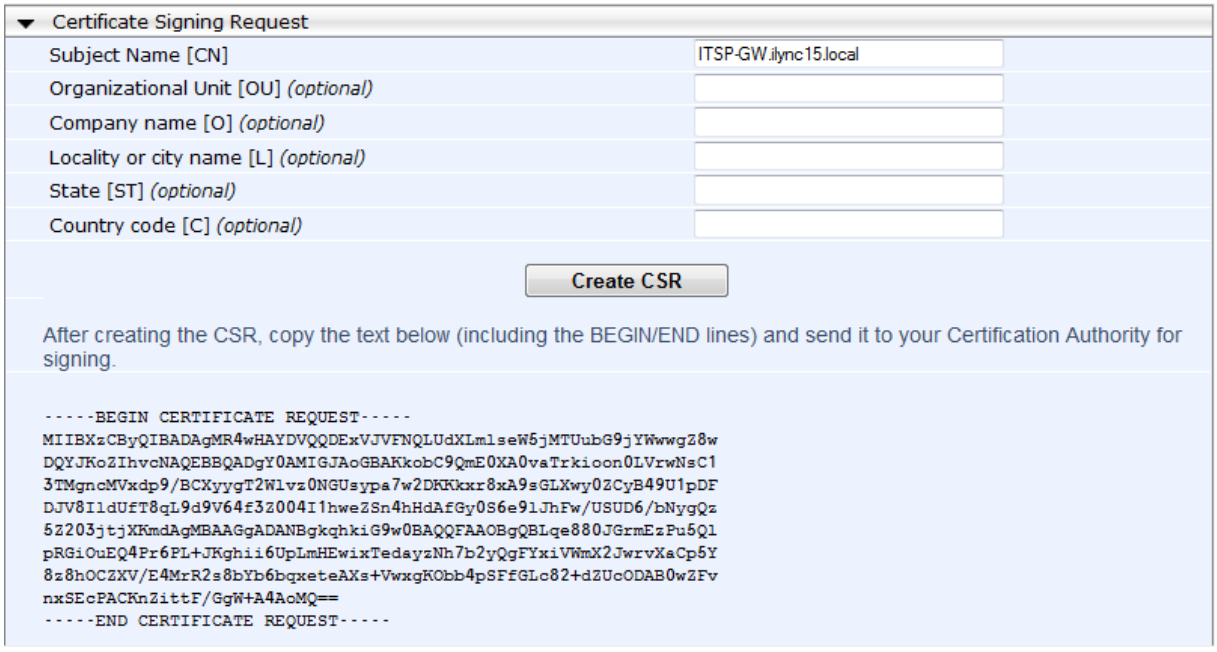
The procedure involves the following main steps:

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 TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row, and then click the **Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP-GW.ilync15.local**).
   b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-26: Certificate Signing Request – Creating CSR

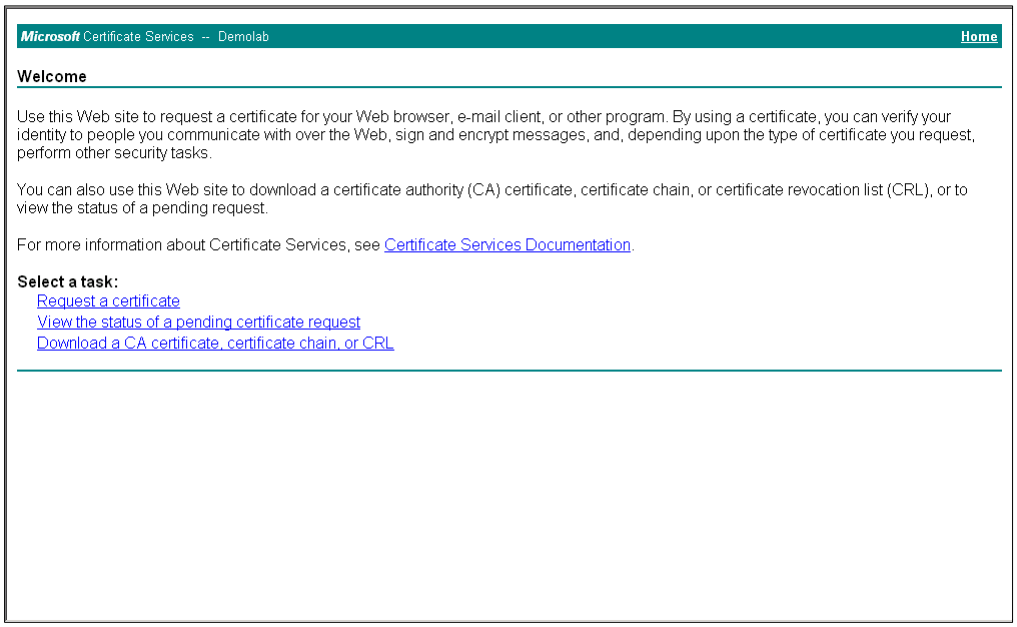


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13.

5. 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*.

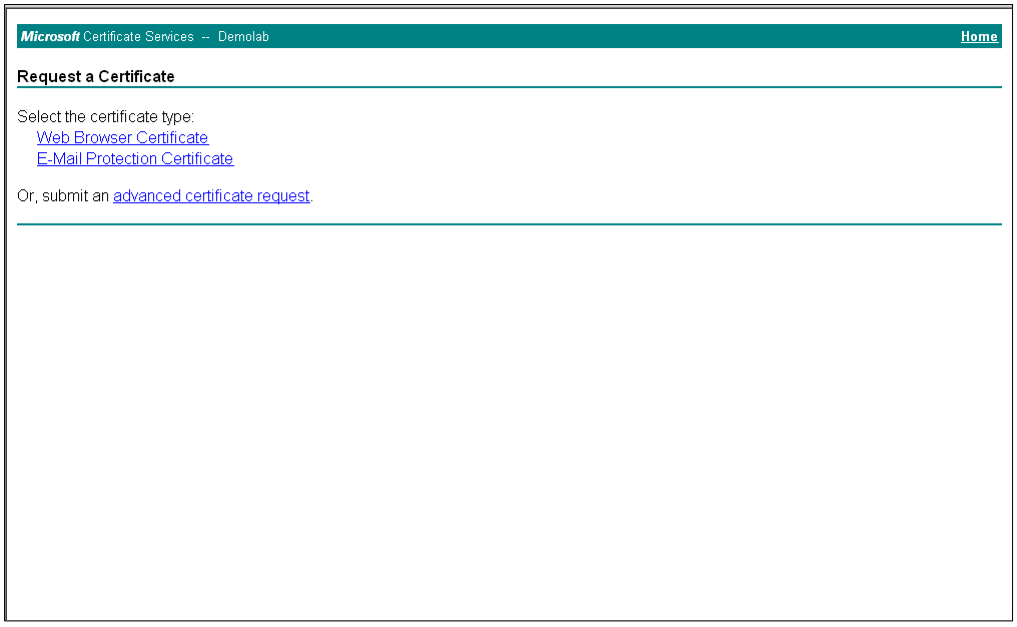
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-27: Microsoft Certificate Services Web Page



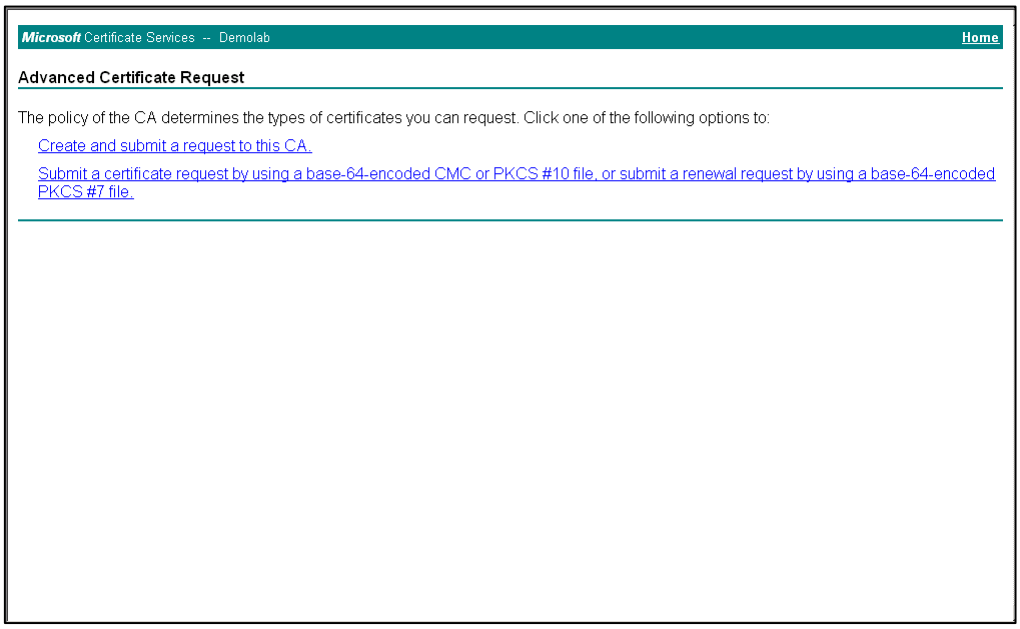
7. Click **Request a certificate**.

Figure 4-28: Request a Certificate Page



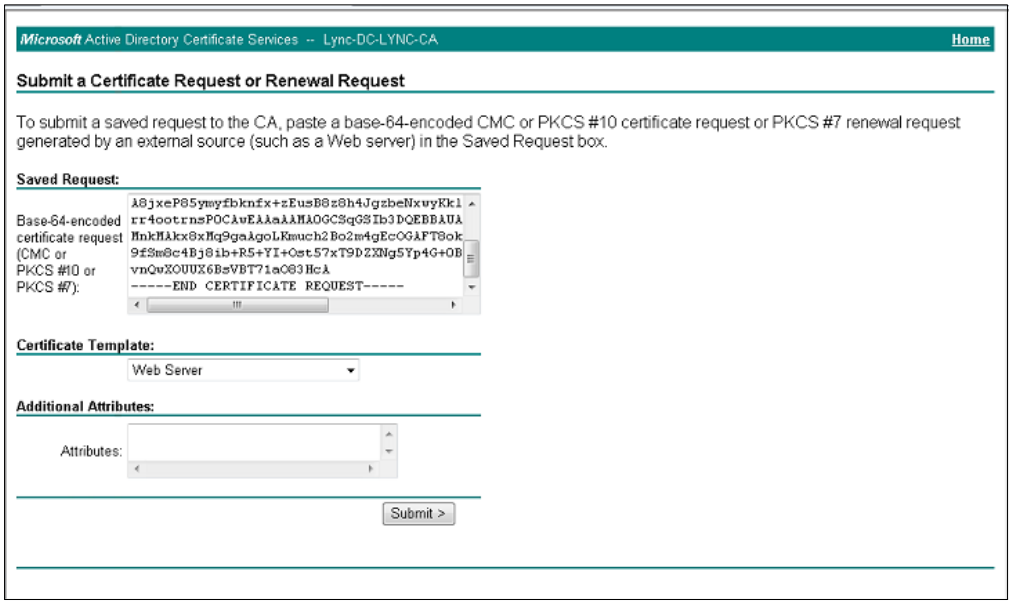
8. Click **advanced certificate request**, and then click **Next**.

Figure 4-29: Advanced Certificate Request Page



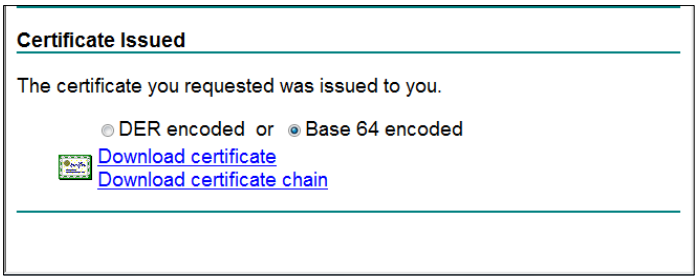
9. Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-30: Submit a Certificate Request or Renewal Request Page



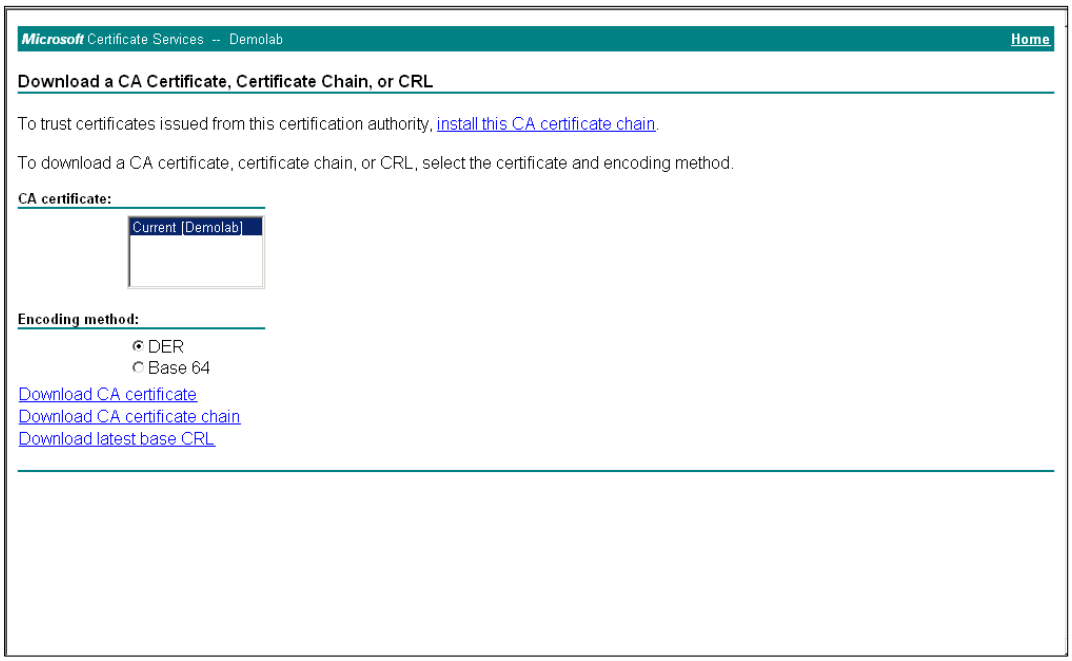
10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 4-31: Certificate Issued Page



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

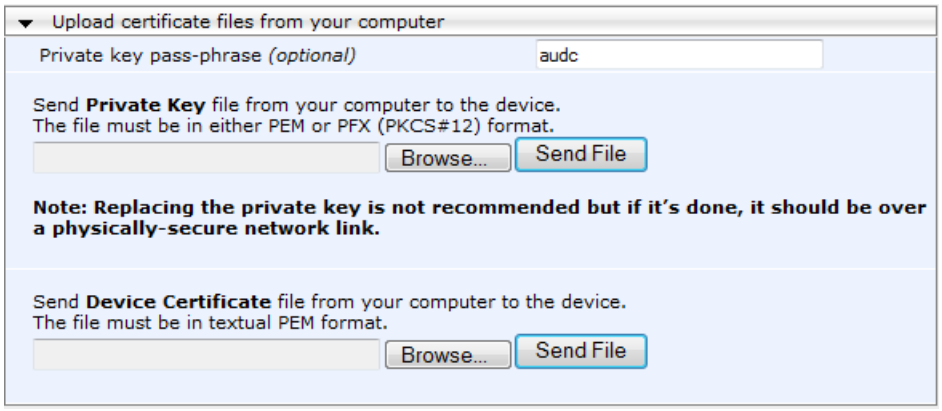
Figure 4-32: Download a CA Certificate, Certificate Chain, or CRL Page



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

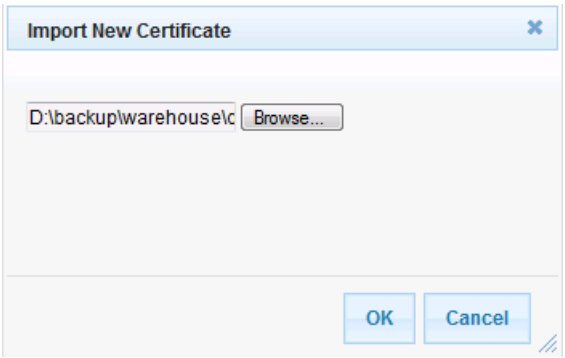
20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
    a. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-33: Upload Device Certificate Files from your Computer Group



    b. In the E-SBC's Web interface, return to the **TLS Contexts** page.
    c. In the TLS Contexts table, select the required TLS Context index row, and then click the **TLS Context Trusted-Roots Certificates** button, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
    d. Click the **Import** button, and then select the certificate file to load.

Figure 4-34: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 87).

4.9 Step 9: Configure SRTP

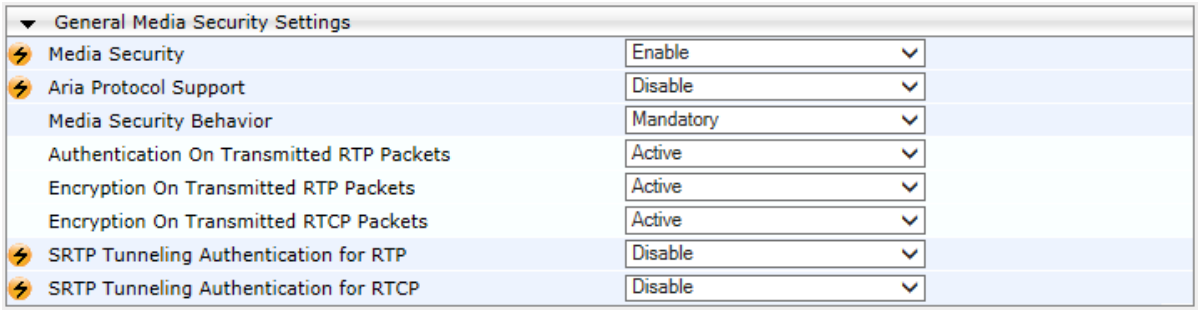
This step shows how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you must configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 46).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**

Figure 4-35: 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 87).

4.10 Step 10: Configure Maximum IP Media Channels

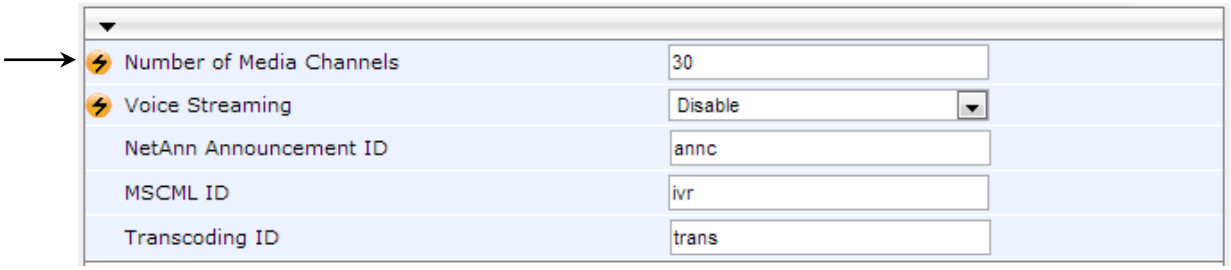
This step shows how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

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

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

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

Figure 4-36: 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 87).

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

This step shows how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 44, IP Group 1 represents Lync Server 2013, and IP Group 2 represents Bell Canada's SIP Trunk.

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

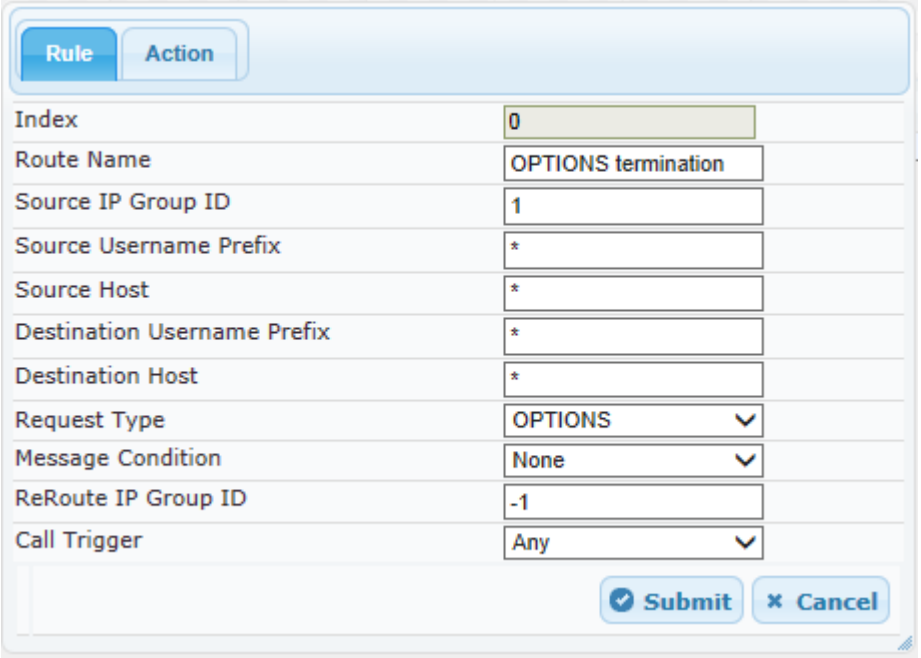
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to Bell Canada's SIP Trunk
- Calls from Bell Canada's SIP Trunk to Lync Server 2013

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

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Route Name	**OPTIONS termination** (arbitrary descriptive name)
Source IP Group ID	**1**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**Internal**

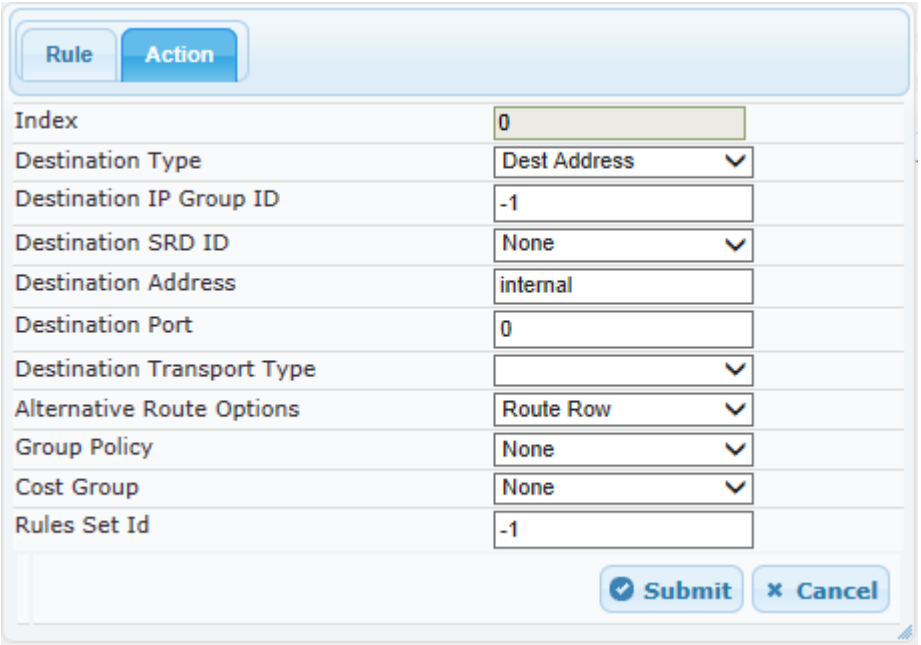
Figure 4-37: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



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

Parameter	Value
Destination Type	**Dest Address**
Destination Address	**internal**

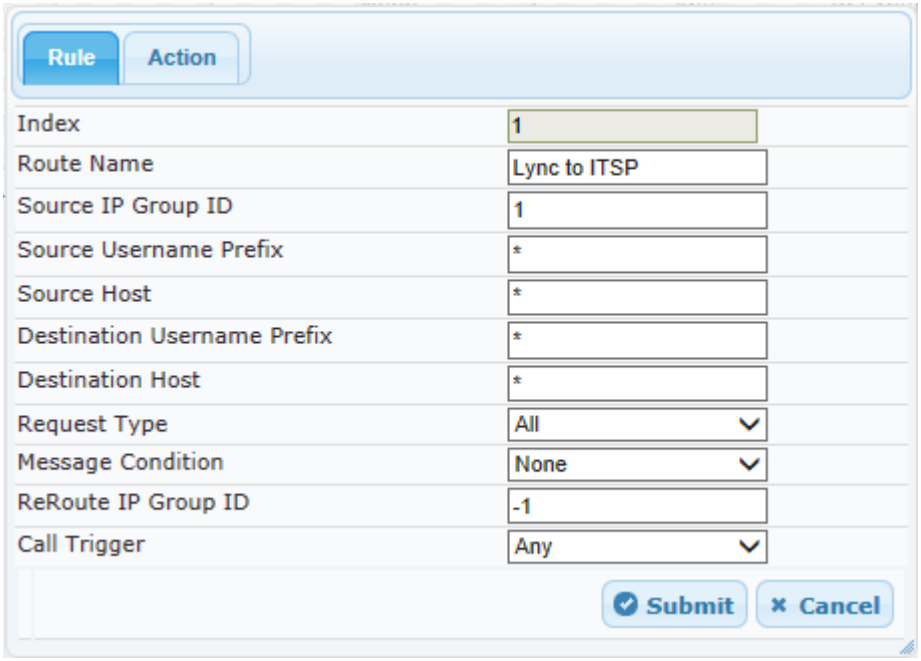
Figure 4-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



4. Configure a rule to route calls from Lync Server 2013 to Bell Canada's SIP Trunk:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Route Name	**Lync to ITSP** (arbitrary descriptive name)
Source IP Group ID	**1**

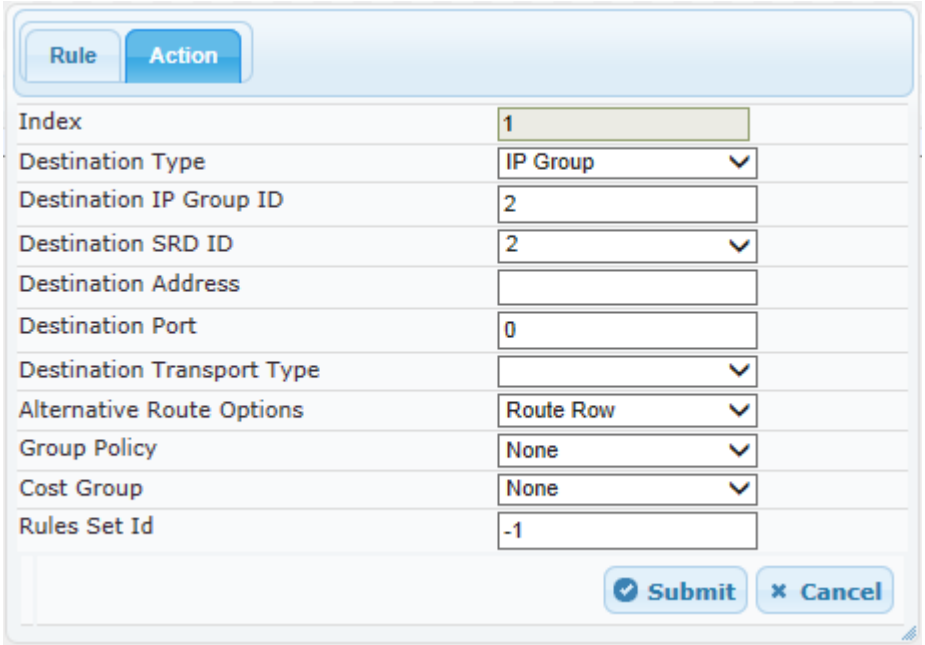
Figure 4-39: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab



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

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

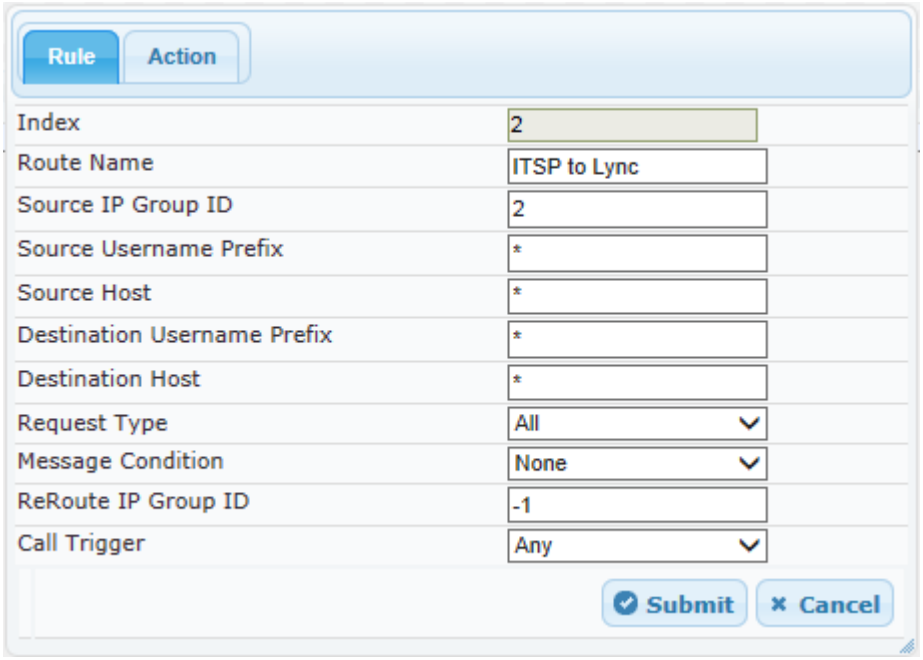
Figure 4-40: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab



6. Configure a rule to route calls from Bell Canada's SIP Trunk to Lync Server 2013:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Route Name	**ITSP to Lync** (arbitrary descriptive name)
Source IP Group ID	**2**

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



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

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 4-42: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab

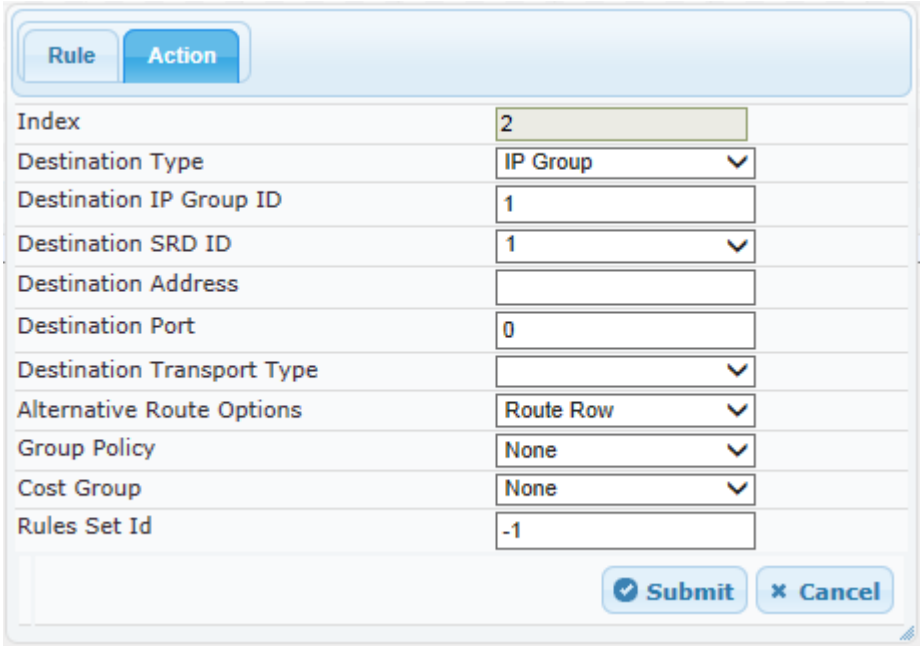
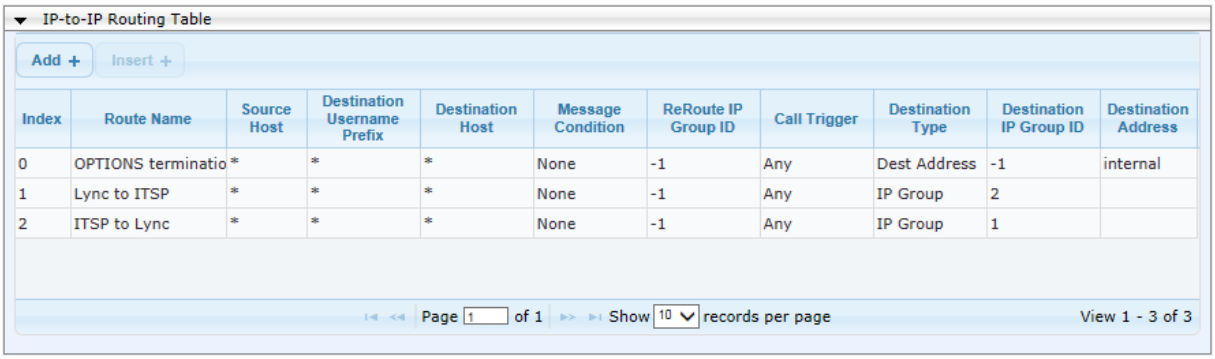


Figure 4-43 shows the configured routing rules:

Figure 4-43: 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 shows how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 44, IP Group 1 represents Lync Server 2013, and IP Group 2 represents Bell Canada's SIP Trunk.

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

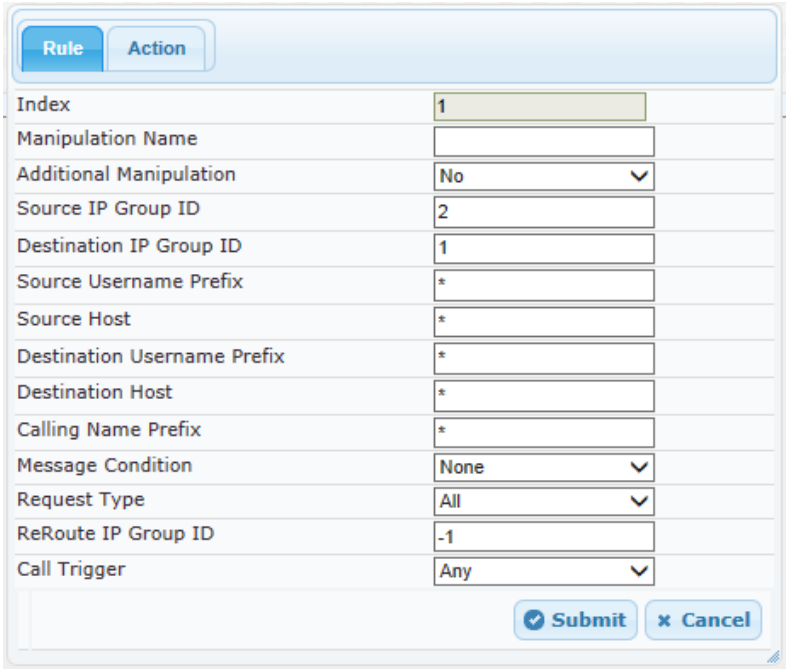
For this interoperability test topology, a manipulation is configured to add the "**+**" (plus sign) to the destination number for calls from IP Group 2 (Bell Canada's SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

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

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

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

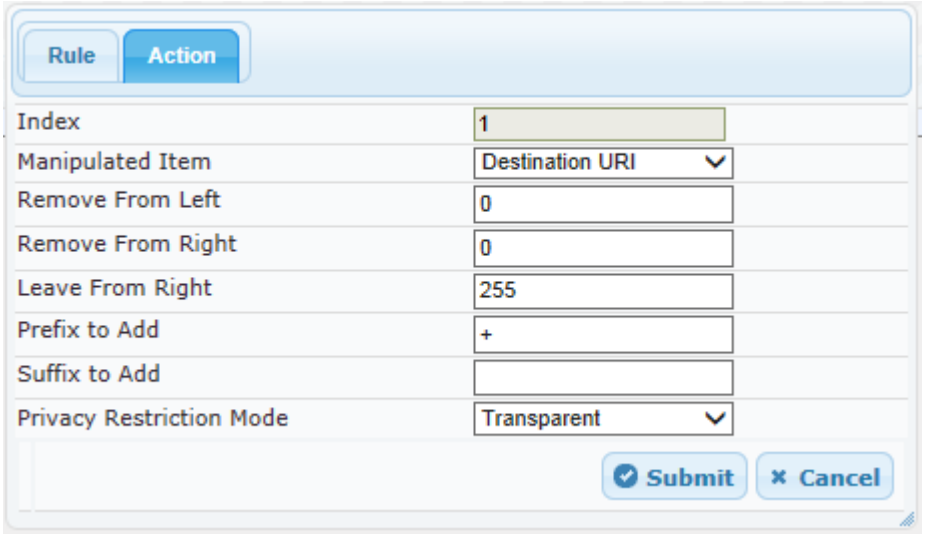
Figure 4-44: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Value
Manipulated Item	**Destination URI**
Prefix to Add	**+** (plus sign)

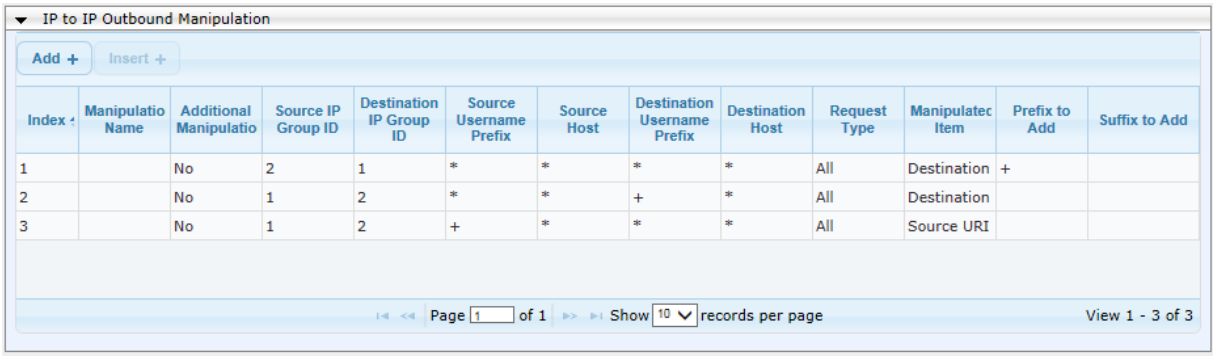
Figure 4-45: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

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

Figure 4-46: Example of Configured IP-to-IP Outbound Manipulation Rules



Rule Index	Rule Action
1	Calls from IP Group 2 to IP Group 1 with any destination number (*), add "+" to the prefix of the destination number.
2	Calls from IP Group 1 to IP Group 2 with the prefix destination number "+", remove "+" from this prefix.
3	Calls from IP Group 1 to IP Group 2 with source number prefix "+", remove the "+" from this prefix.

4.13 Step 13: Configure Message Manipulation Rules

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

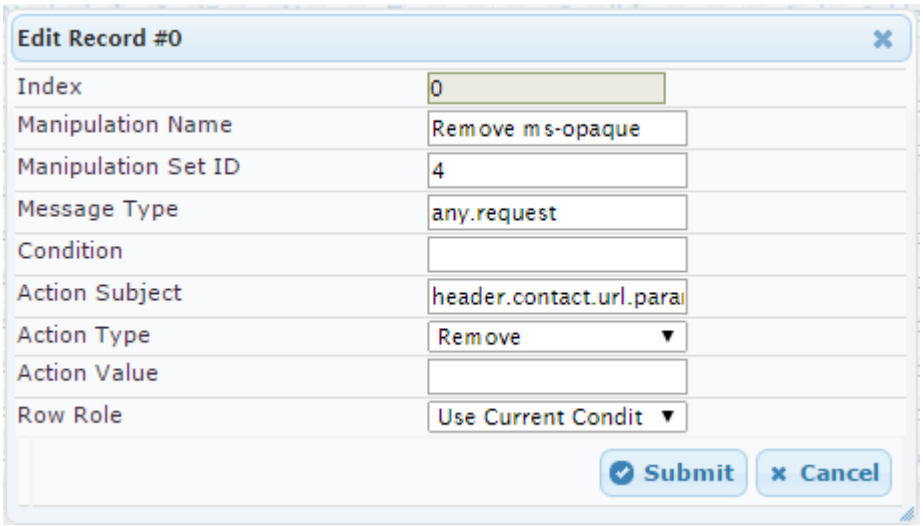
After configuring the SIP message manipulation rules, you must assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add a manipulation rule to Index 0 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes the 'ms-opaque' parameter from the Contact Header.

Parameter	Value
Index	**0**
Manipulation Name	**Remove ms-opaque**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.contact.url.param.ms-opaque**
Action Type	**Remove**

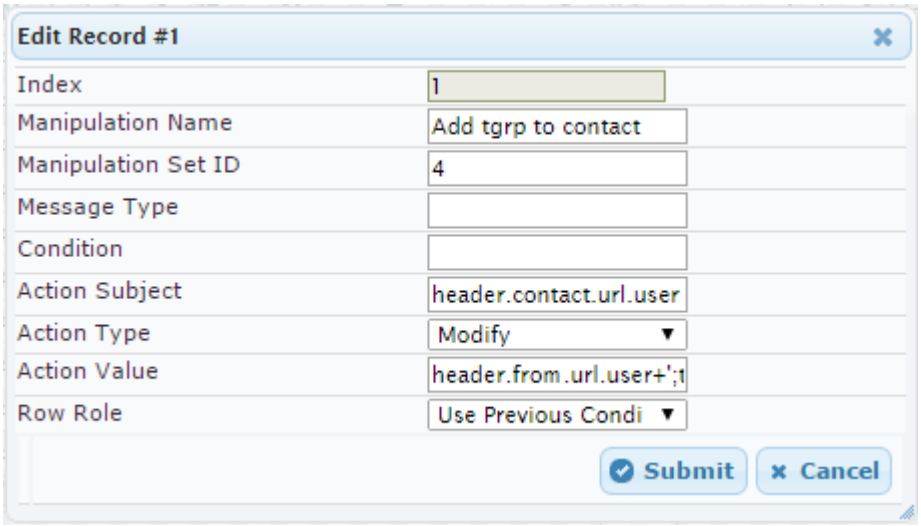
Figure 4-47: Configuring SIP Message Manipulation Rule 0 (for Bell Canada's SIP Trunk)



3. Add a manipulation rule to Index 1 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada's SIP Trunk (IP Group 2). This rule normalizes the SIP Contact Header according to Bell Canada requirements.

Parameter	Value
Index	**1**
Manipulation Name	**Add tgrp to contact**
Manipulation Set ID	**4**
Action Subject	**header.contact.url.user**
Action Type	**Modify**
Action Value	**header.from.url.user+';tgrp=vend5_6132606020_01a;trunk-context=siptrunking.bell.ca'**
Row Role	**Use Previous Condition**

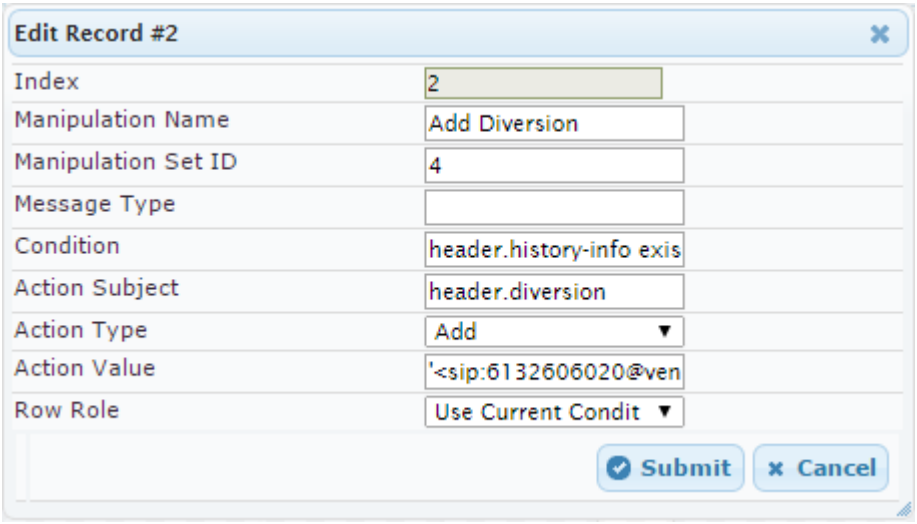
Figure 4-48: Configuring SIP Message Manipulation Rule 1 (for Bell Canada's SIP Trunk)



4. Add a manipulation rule to Index 2 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This adds the '<sip:6132606020@vendor5.lab.internetvoice.ca;user=phone>' Diversion Header string in case the History-Info Header exists, where 6132606020 is the trunk's main line.

Parameter	Value
Index	**2**
Manipulation Name	**Add Diversion**
Manipulation Set ID	**4**
Condition	**header.history-info exists**
Action Subject	**header.diversion**
Action Type	**Add**
Action Value	**'<sip:6132606020@vendor5.lab.internetvoice.ca;user=phone>'**

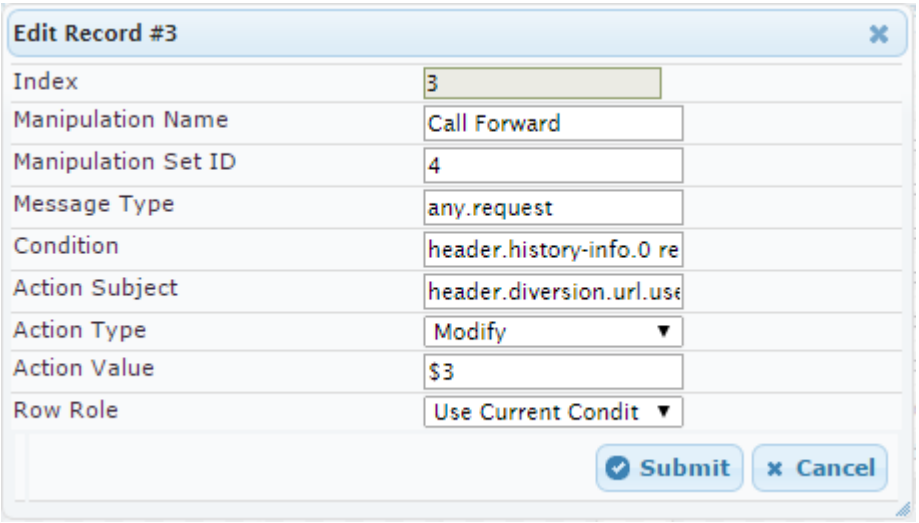
Figure 4-49: Configuring SIP Message Manipulation Rule 2 (for Bell Canada's SIP Trunk)



5. Add a manipulation rule to Index 3 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for a Call Forward initiated by the Lync Server 2013 (IP Group 1). This replaces the user part of the Diversion Header with the value from the History-Info Header.

Parameter	Value
Index	**3**
Manipulation Name	**Call Forward**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header.history-info.0 regex (<sip:)(.)(.*)(@)(.*)**
Action Subject	**header.diversion.url.user**
Action Type	**Modify**
Action Value	**$3**

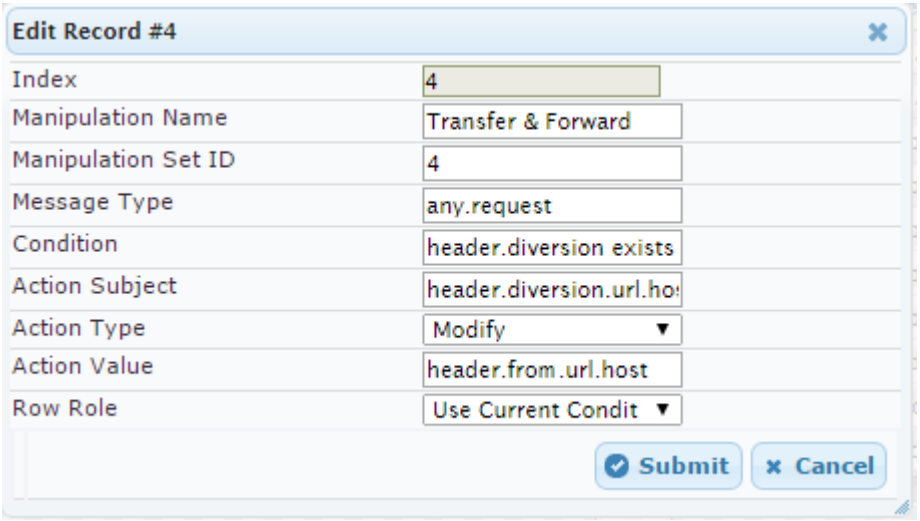
Figure 4-50: Configuring SIP Message Manipulation Rule 3 (for Bell Canada's SIP Trunk)



6. Add a manipulation rule to Index 4 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Call Transfer or Forward initiated by the Lync Server 2013 (IP Group 1). This replaces the host part of the Diversion Header with the value from the From Header, in case the Diversion Header exists.

Parameter	Value
Index	**4**
Manipulation Name	**Transfer & Forward**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header. diversion exists**
Action Subject	**header.diversion.url.host**
Action Type	**Modify**
Action Value	**header.from.url.host**

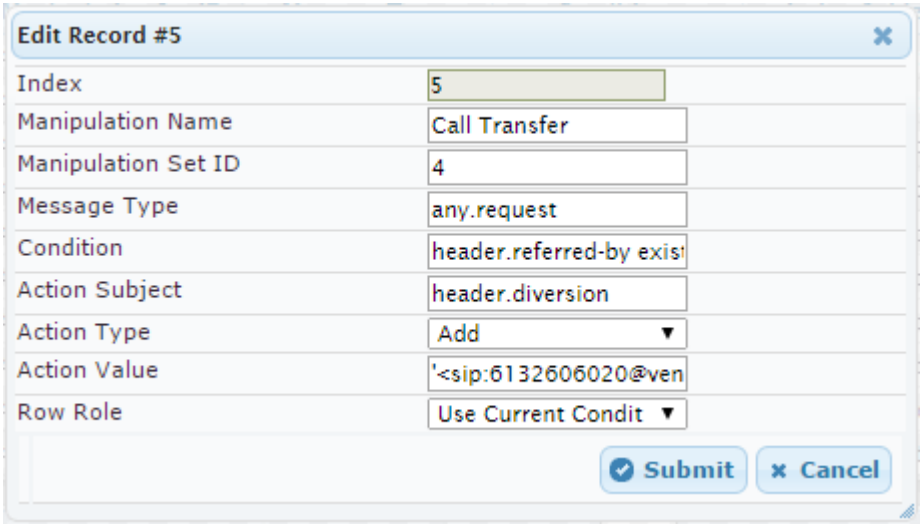
Figure 4-51: Configuring SIP Message Manipulation Rule 4 (for Bell Canada's SIP Trunk)



7. Add a manipulation rule to Index 5 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This adds the '<sip:6132606021@vendor5.lab.internetvoice.ca;user=phone>' Diversion Header string in case the Referred-By Header exists, where 6132606020 is the trunk's main line.

Parameter	Value
Index	**5**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Condition	**header.referred-by exists**
Action Subject	**header.diversion**
Action Type	**Add**
Action Value	**'<sip:6132606020@vendor5.lab.internetvoice.ca;user=phone>'**

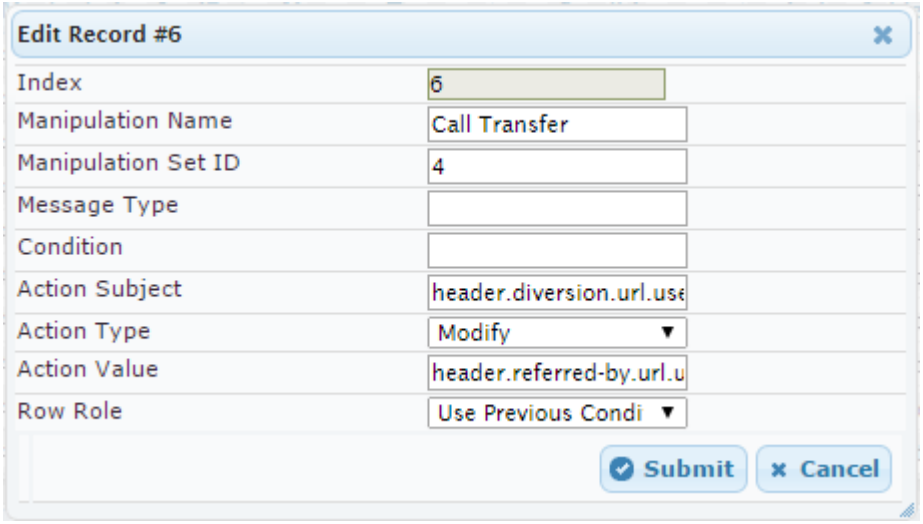
Figure 4-52: Configuring SIP Message Manipulation Rule 5 (for Bell Canada's SIP Trunk)



8. Add a manipulation rule to Index 6 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) based on the previous rule condition. This replaces the user part of the Diversion Header with the value from the Referred-By Header.

Parameter	Value
Index	**6**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Action Subject	**header.diversion.url.user**
Action Type	**Modify**
Action Value	**header.referred-by.url.user**
Row Role	**Use Previous Condition**

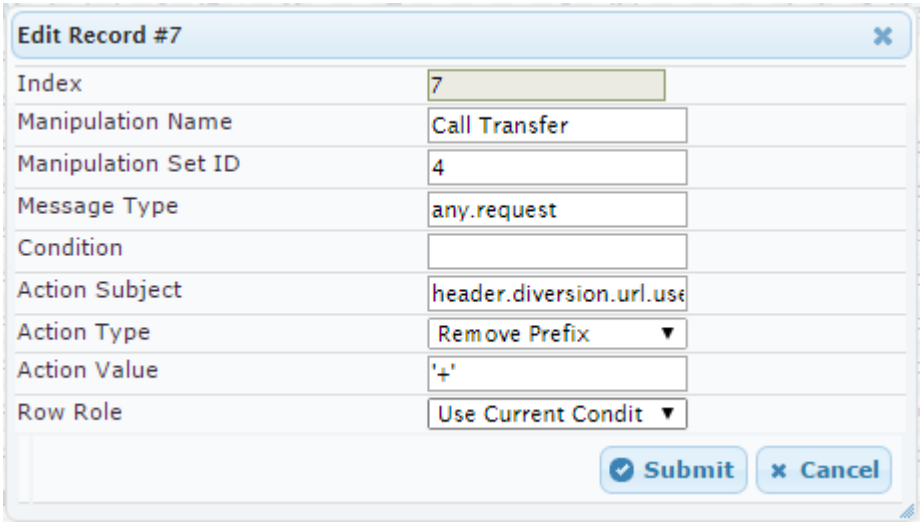
Figure 4-53: Configuring SIP Message Manipulation Rule 6 (for Bell Canada's SIP Trunk)



9. Add a manipulation rule to Index 7 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for a Call Transfer initiated by the Lync Server 2013 (IP Group 1). This removes the '+' prefix from the user part of the Diversion Header.

Parameter	Value
Index	**7**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.diversion.url.user**
Action Type	**Remove Prefix**
Action Value	**'+'**

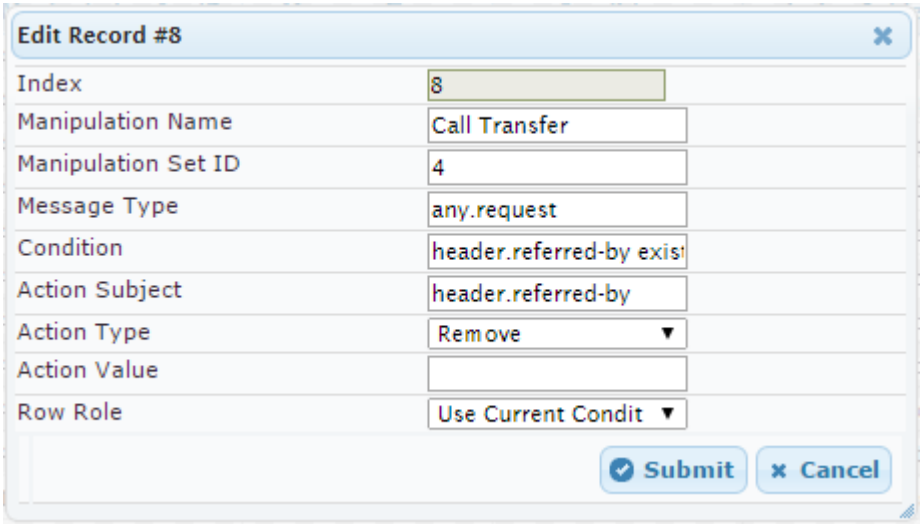
Figure 4-54: Configuring SIP Message Manipulation Rule 7 (for Bell Canada's SIP Trunk)



10. Add a manipulation rule to Index 8 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for a Call Transfer initiated by the Lync Server 2013 (IP Group 1). This removes the Referred-By Header.

Parameter	Value
Index	**8**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header.referred-by exists**
Action Subject	**header.referred-by**
Action Type	**Remove**

Figure 4-55: Configuring SIP Message Manipulation Rule 8 (for Bell Canada's SIP Trunk)



11. Add a manipulation rule to Index 9 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Rejected Calls initiated by the Lync Server 2013 (IP Group 1). This replaces the method type '603' with the value '486', because Bell Canada's SIP Trunk does not recognize the '603' method type.

Parameter	Value
Index	**9**
Manipulation Name	**Decline Cause**
Manipulation Set ID	**4**
Message Type	**invite.response.603**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'486'**

Figure 4-56: Configuring SIP Message Manipulation Rule 9 (for Bell Canada's SIP Trunk)

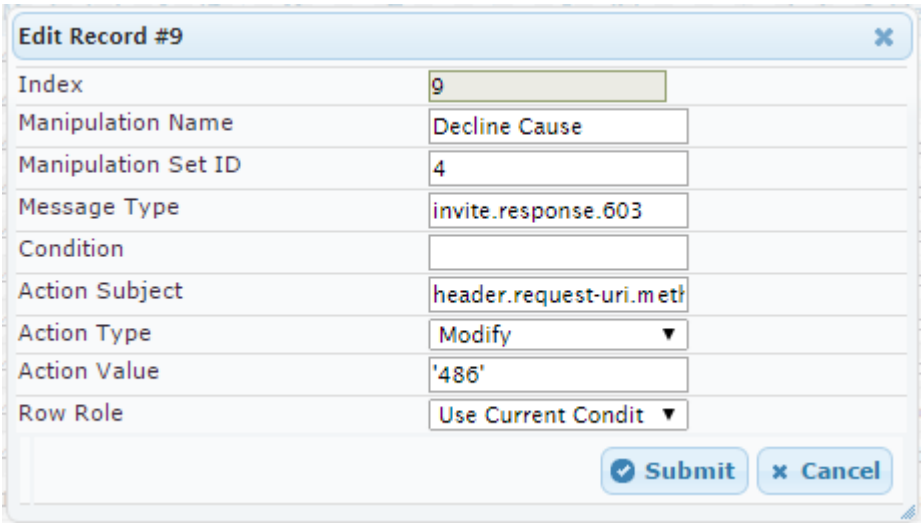
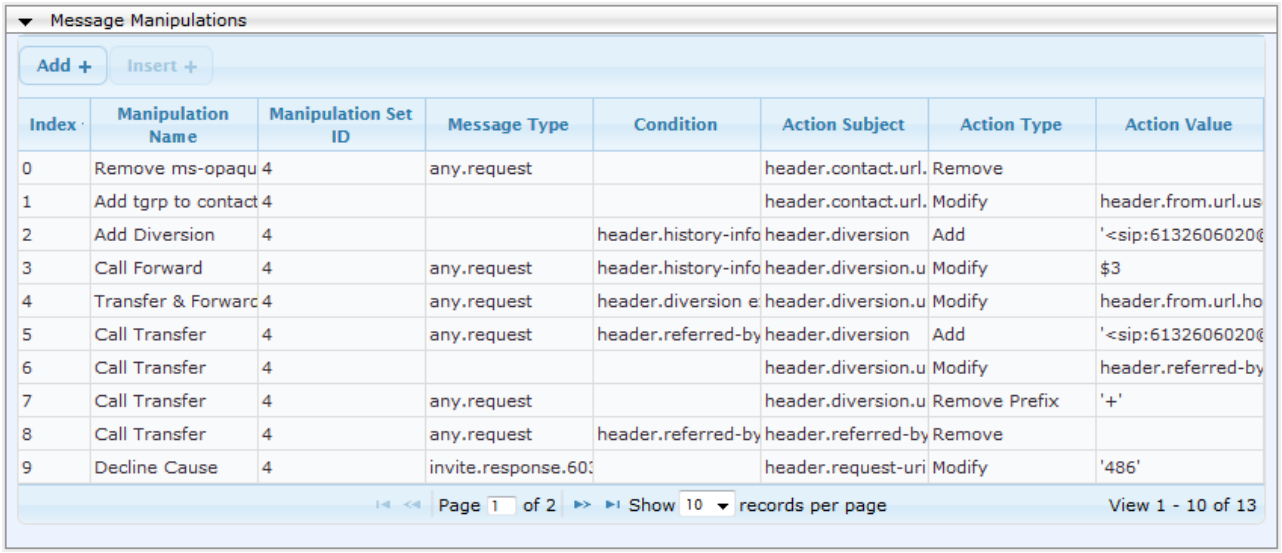


Figure 4-57: Configured SIP Message Manipulation Rules



Message Manipulations

Add + | Insert +

Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	Remove ms-opaqu	4	any.request		header.contact.url.	Remove	
1	Add tgrp to contact	4			header.contact.url.	Modify	header.from.url.us
2	Add Diversion	4		header.history-info	header.diversion	Add	'<sip:6132606020@
3	Call Forward	4	any.request	header.history-info	header.diversion.u	Modify	$3
4	Transfer & Forwarc	4	any.request	header.diversion e	header.diversion.u	Modify	header.from.url.ho
5	Call Transfer	4	any.request	header.referred-by	header.diversion	Add	'<sip:6132606020@
6	Call Transfer	4			header.diversion.u	Modify	header.referred-by
7	Call Transfer	4	any.request		header.diversion.u	Remove Prefix	'+'
8	Call Transfer	4	any.request	header.referred-by	header.referred-by	Remove	
9	Decline Cause	4	invite.response.60		header.request-uri	Modify	'486'

Page 1 of 2 Show 10 records per page View 1 - 10 of 13

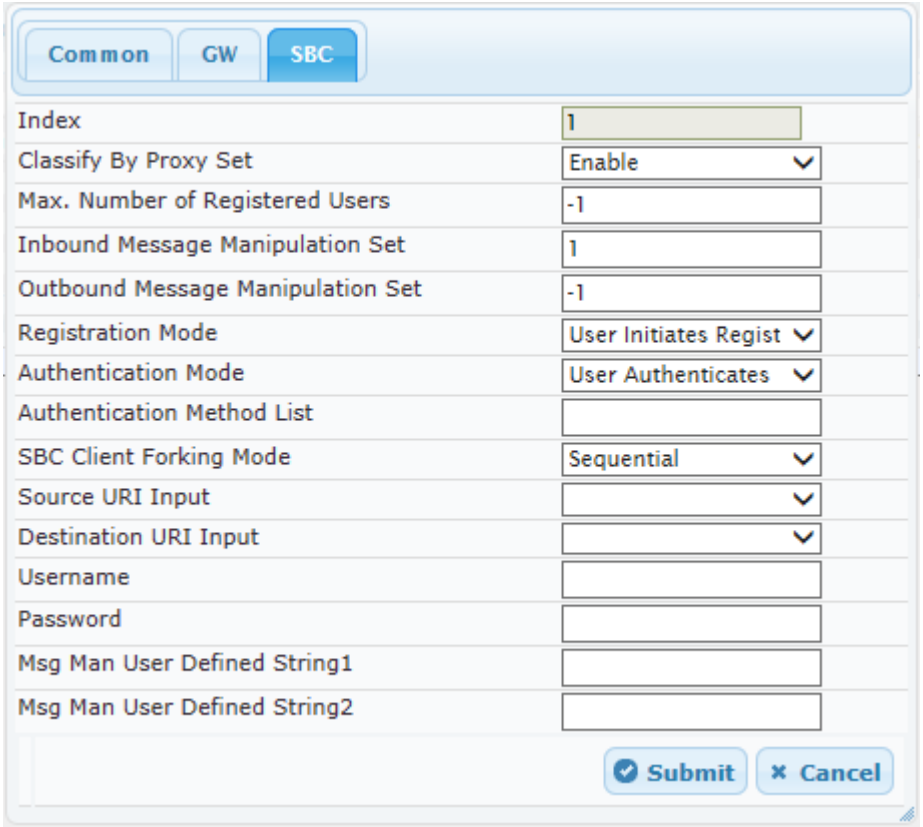
The table displayed below includes SIP message manipulation rules that are bound together by common Manipulation Set IDs 1 and 4, which are executed for messages sent to and from the Bell Canada SIP Trunk (IP Group 2) as well as the Lync Server 2013 (IP Group 1). These rules are specifically required to enable proper interworking between Bell Canada's SIP Trunk and Lync Server 2013. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes the 'ms-opaque' parameter from Contact Header.	-
1	This rule applies to messages sent to the Bell Canada's SIP Trunk (IP Group 2). This rule normalizes the SIP Contact Header according to Bell Canada requirements.	-
2	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This adds the '<sip: 6132606020@cust5-tor.vsac.bell.ca>' string to Diversion Header in case History-Info Header exists, where 6132606020is the trunk's main line.	-
3	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Call Forward initiated by the Lync Server 2013 (IP Group 1). This replaces the user part of the Diversion Header with the value from the History-Info Header.	For Call Forward initiated by the Lync Server 2013.
4	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Call Transfer or Forward initiated by the Lync Server 2013 (IP Group 1). This replaces the host part of the Diversion Header with the value from the From Header in case the Diversion Header exists.	For Call Transfer or Forward initiated by Lync Server 2013, Bell Canada's SIP Trunk needs to replace the host part of the Diversion Header with the value from the From Header in case the Diversion Header exists.

Rule Index	Rule Description	Reason for Introducing Rule
5	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This adds the '<sip:6132606021@vendor5.lab.internetvoice.ca;user=phone>' Diversion Header string in case the Referred-By Header exists, where 6132606020 is the trunk's main line.	For Call Transfer initiated by the Lync Server 2013.
6	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) based on the previous rule condition. This replaces the user part of the Diversion Header with the value from the Referred-By Header.	For Call Transfer initiated by the Lync Server 2013.
7	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes the '+' prefix from the user part of Diversion Header.	For Call Transfer initiated by the Lync Server 2013.
8	This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2) for Call Transfer initiated by the Lync Server 2013 (IP Group 1). This removes the Referred-By Header.	Bell Canada's SIP Trunk does not support "Referred-By" Header in SIP INVITE messages, so it is necessary to remove it.
9	This rule applies to response messages sent to the Bell Canada SIP Trunk (IP Group 2) for Rejected Calls initiated by the Lync Server 2013 (IP Group 1). This replaces the method type '603' with the value '486'.	Bell Canada's SIP Trunk does not recognize the '603' method type.

12. Assign Manipulation Set ID 1 to IP Group 1:
    a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
    b. Select the row of IP Group 1, and then click **Edit**.
    c. Click the **SBC** tab.
    d. Set the 'Inbound Message Manipulation Set' field to **1**.

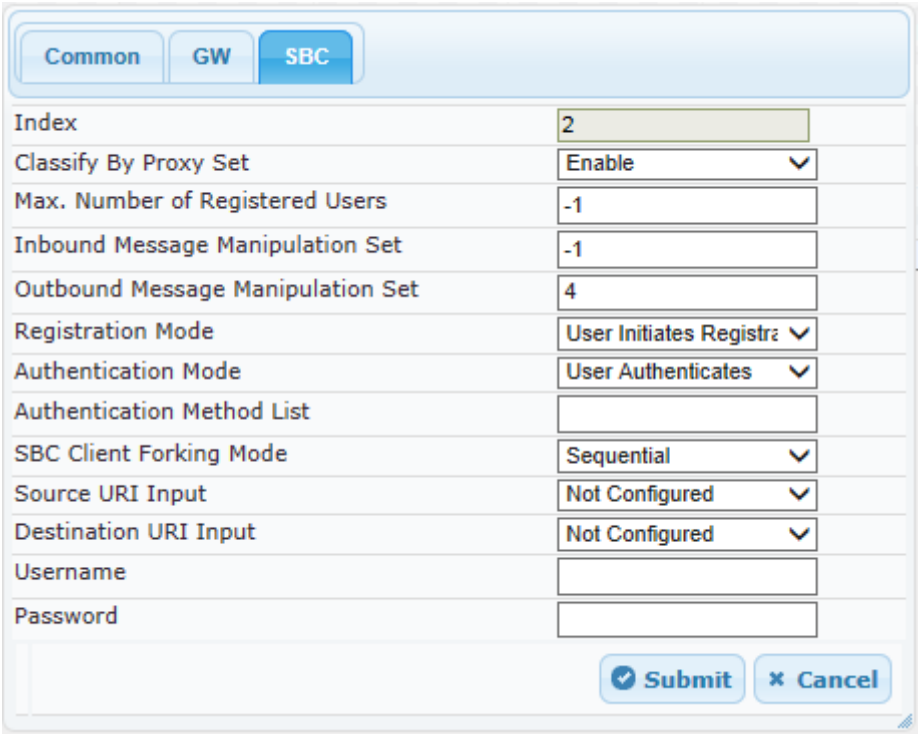
Figure 4-58: Assigning Manipulation Set to IP Group 1



    e. Click **Submit**.

13. Assign Manipulation Set ID 4 to IP Group 2:
    a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
    b. Select the row of IP Group 2, and then click **Edit**.
    c. Click the **SBC** tab.
    d. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-59: Assigning Manipulation Set 4 to IP Group 2



    e. Click **Submit**.

4.14 Step 14: Configure Registration Accounts

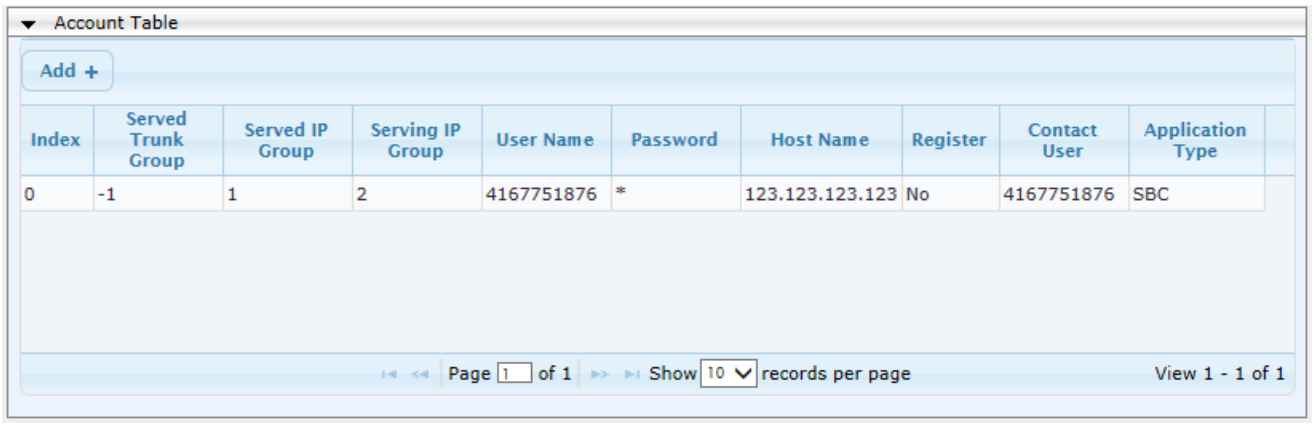
This step shows how to configure SIP registration accounts. This is required so that the E-SBC can register with the Bell Canada SIP Trunk on behalf of Lync Server 2013. The Bell Canada SIP Trunk does not require registration, only authentication to provide service.

In the interoperability test topology, the Served IP Group is Lync Server 2013 (IP Group 1) and the Serving IP Group is Bell Canada's 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 4-60: 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 2013)
Serving IP Group	**2** (Bell Canada's SIP Trunk)
Username	As provided by Bell Canada
Password	As provided by Bell Canada
Host Name	**123.123.123.123**
Register	**No**
Contact User	**4167751876** (trunk main line)
Application Type	**SBC**

4. Click **Apply**.

4.15 Step 15: Configure Miscellaneous Settings

This section describes configuration of miscellaneous E-SBC settings.

4.15.1 Step 15a: Configure Classification Table

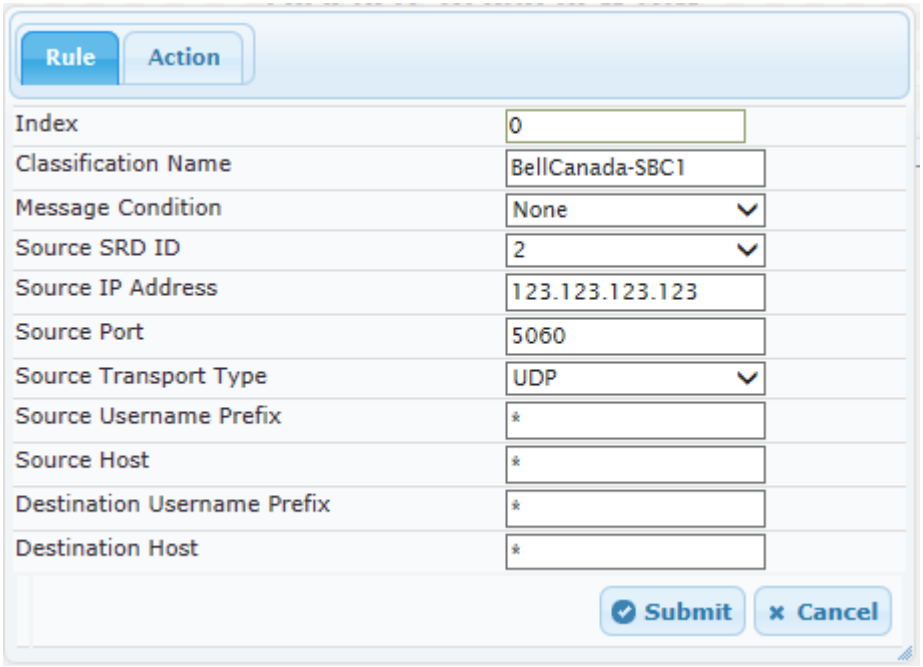
This step is only relevant to configuration with Bell Canada Load Balancer. It shows how to configure the E-SBC Classification Table. For the interoperability test topology with Bell Canada Load Balancer, when Load Balancer IP / FQDN is configured in Proxy Set, it's necessary to allow messages to be received from Bell Canada SBCs. The Classification Table does this.

➢ **To configure Classification Table:**

1. Open the Classification Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Classification Name	**BellCanada-SBC1** (arbitrary descriptive name)
Source SRD ID	**2**
Source IP Address	**123.123.123.123** (IP address received from Bell Canada)
Source Port	**5060**
Source Transport Type	**UDP**

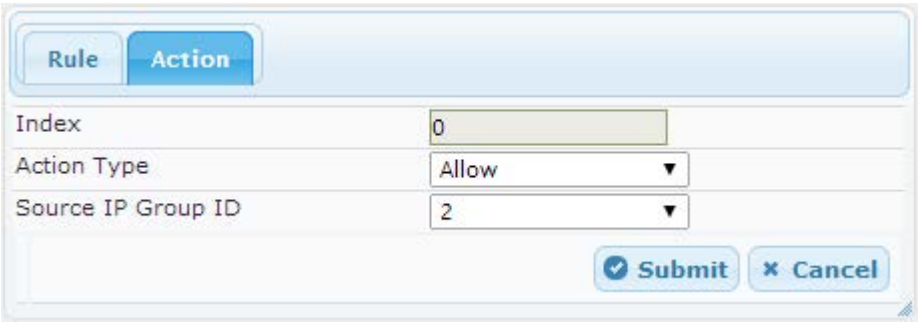
Figure 4-61: Classification Table Page – Rule Tab



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

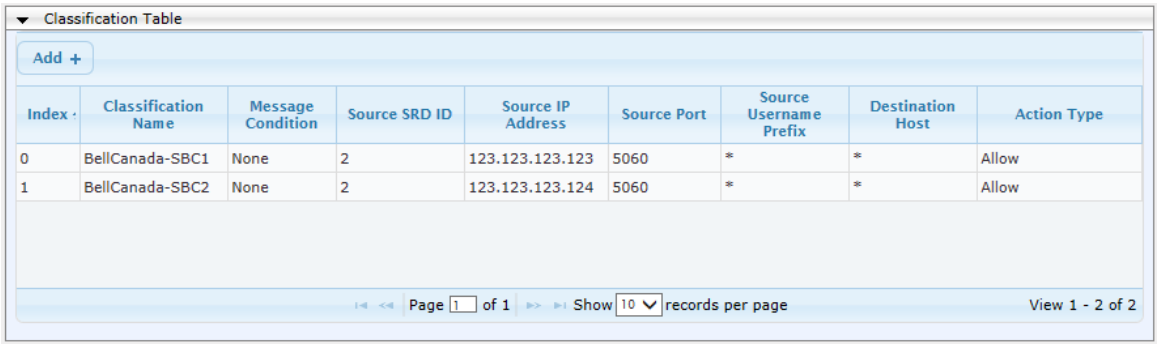
Parameter	Value
Action Type	**Allow**
Source IP Group ID	**2**

Figure 4-62: Classification Table Page – Action Tab



5. Click **Submit**.

Figure 4-63: Example of Classification Table



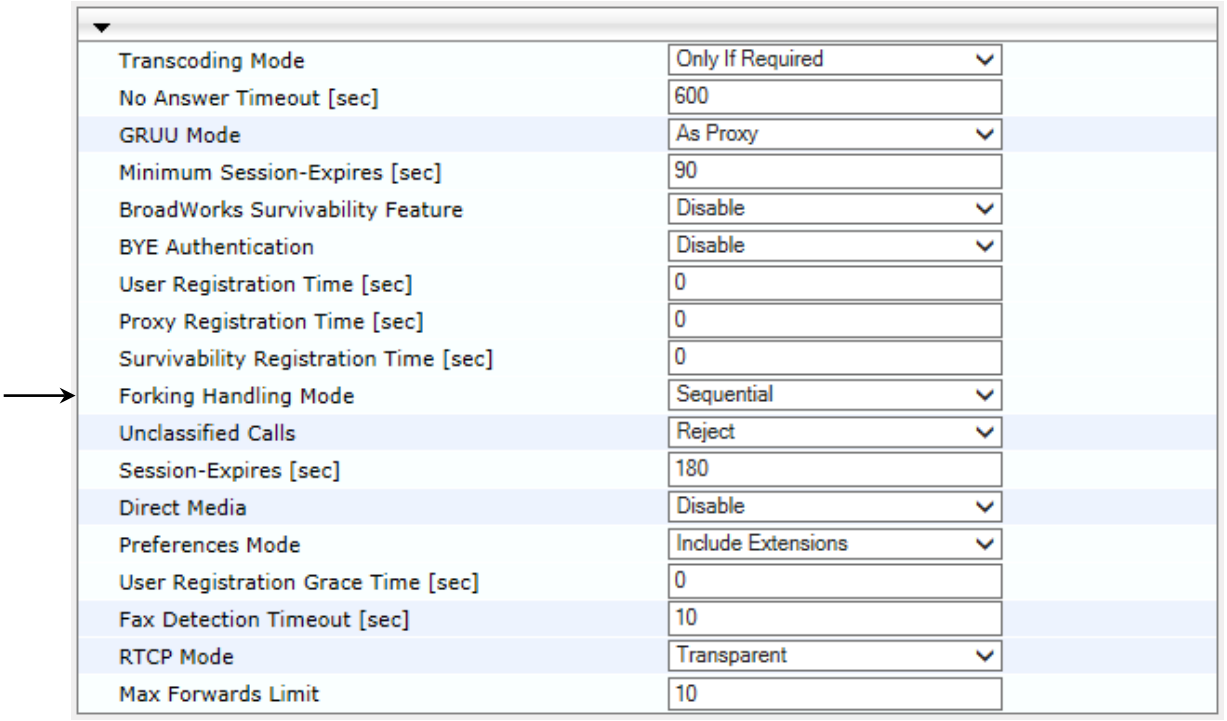
4.15.2 Step 15b: Configure Call Forking Mode

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

➢ **To configure call forking:**

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

Figure 4-64: Configuring Forking Mode



3. Click **Submit**.

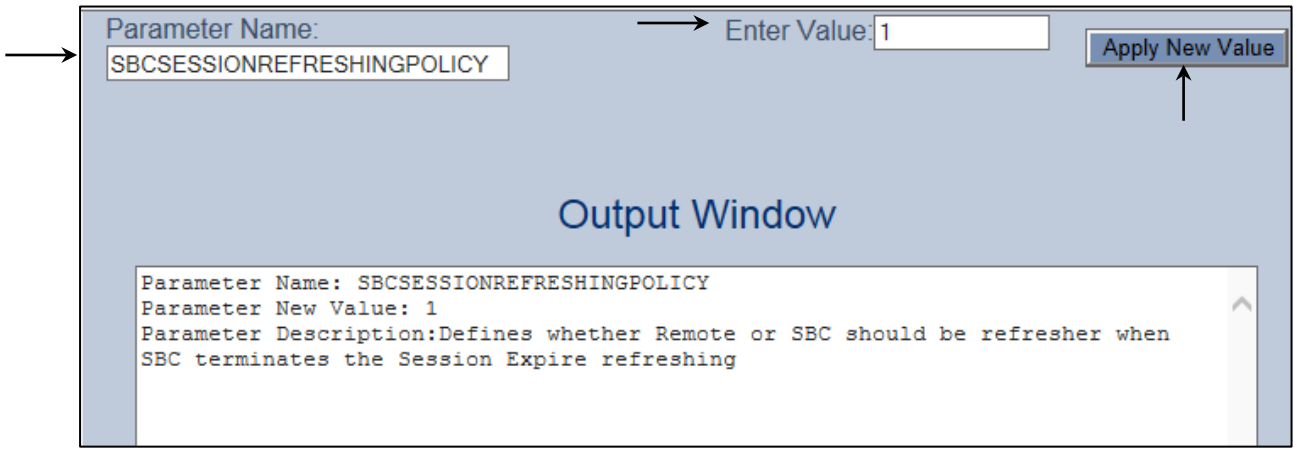
4.15.3 Step 15c: Configure SBC Session Refreshing Policy

This step shows how to configure the 'SBC Session Refreshing Policy' parameter. In some cases, Microsoft Lync does not perform a refresh of Session Timer even when it confirms that it will be refresher. To resolve this issue, the SBC is configured as Session Expire refresher.

➢ **To configure SBC Session Refreshing Policy:**

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.15/AdminPage).
2. In the left pane of the page that opens, click ***ini* Parameters**.

Figure 4-65: Configuring SBC Session Refreshing Policy in AdminPage



3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
SBCSESSIONREFRESHINGPOLICY	**1** (enables SBC as refresher of Session Timer)

4. Click the **Apply New Value** button for each field.

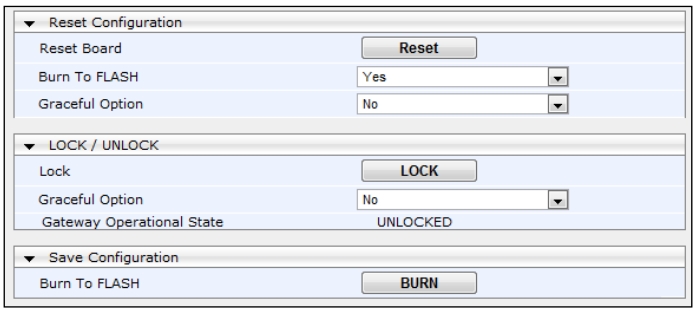
4.16 Step 16: Reset the E-SBC

After completing configuration of the E-SBC, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

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

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

Figure 4-66: Resetting the E-SBC



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

This page is intentionally left blank.

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, open the Web interface and access the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 74
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 6.80A.256
;DSP Software Version: 5014AE3_R => 680.22
;Board IP Address: 10.15.17.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;Key features:;Board Type: 74 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;Channel Type: DspCh=30
IPMediaDspCh=30 ;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 ;DSP Voice features: IpmDetector RTCP-XR
AMRPolicyManagement ;E1Trunks=1 ;FXSPorts=8 ;FXOPorts=0 ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;DATA features:
;QOE features: VoiceQualityMonitoring MediaEnhancement ;Control
Protocols: MSFT CLI TRANSCODING=30 FEU=100 TestCall=100 MGCP MEGACO H323
SIP TPNCP SASurvivability SBC=50 ;Default features:;Coders: G711 G726;

;------  HW components------
;
; Slot # : Module type : # of ports
;---------------------------------------------
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : FXS         : 4
;---------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '10.15.25.1'
LDAPSEARCHDNSINPARALLEL = 0
```

```
[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

FarEndDisconnectType = 7

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

RFC2833TxPayloadType = 101
RFC2833RxPayloadType = 101
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UseRProductName = 'Mediant 800 E-SBC'
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'

[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
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1

[SCTP Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_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 ]


[ 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", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

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

[ \DeviceTable ]
```

```
[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.55, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.160, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]


[ DspTemplates ]

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

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 1 = "MRLan", "Voice", "", 6000, 10, 6090, 1, "", "";
CpMediaRealm 2 = "MRWan", "WANSP", "", 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 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 1 = "123.123.123.123", 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_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, 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_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;
IpProfile 1 = "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, 0, 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,
1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 3, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300;
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, 1, "", 2, -1, 2,
2, 0, 0, 1, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 2, 2, 2, 1, 3, 0, 1,
0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 300;

[ \IpProfile ]


[ ProxySet ]
```

```
FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, "-1", -1, -1, "";
ProxySet 1 = "Lync", 1, 60, 1, 1, 1, 0, "-1", 1, -1, "";
ProxySet 2 = "BellCanada", 1, 60, 0, 0, 2, 0, "-1", -1, -1, "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "Lync", 1, "cust5-tor.vsac.bell.ca", "", 0, -1, -1, 0, -1,
1, "MRLan", 1, 1, -1, 1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0,
"", "", "", "", 0, "", "";
IPGroup 2 = 0, "BellCanada", 2, "siptrunking.bell.ca", "", 0, -1, -1, 0,
-1, 2, "MRWan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==",
0, "", "", "", 0, "", "";
[ \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, "4167751876", "$1$vZzcjKytoaKqpKKm/eg=",
"123.123.123.123", 0, "4167751876", 2;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
```

```
IP2IPRouting 0 = "OPTIONS termination", 1, "*", "*", "*", "*", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "Lync to ITSP", 1, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 2, "", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to Lync", 2, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 1, "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;

[ \TLSContexts ]


[ SIPInterface ]

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

[ \SIPInterface ]


[ IPOutboundManipulation ]

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

```
IPOutboundManipulation 1 = "", 0, 1, 2, "*", "*", "+9", "*", "*", "", 0,
-1, 0, 1, 1, 0, 255, "011", "", 0;
IPOutboundManipulation 2 = "", 0, 1, 2, "*", "*", "7", "*", "*", "", 0, -
1, 0, 1, 0, 0, 255, "1", "", 0;
IPOutboundManipulation 3 = "", 0, 1, 2, "*", "*", "9", "*", "*", "", 0, -
1, 0, 1, 0, 0, 255, "011", "", 0;
IPOutboundManipulation 4 = "", 0, 1, 2, "+", "*", "*", "*", "*", "", 0, -
1, 0, 0, 1, 0, 255, "", "", 0;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

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


[ AllowedCodersGroup1 ]

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

[ \AllowedCodersGroup1 ]


[ AllowedCodersGroup2 ]

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

[ \AllowedCodersGroup2 ]
```

```
[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Remove ms-opaque", 4, "any.request", "",
"header.contact.url.param.ms-opaque", 1, "", 0;
MessageManipulations 1 = "Add tgrp to contact", 4, "", "",
"header.contact.url.user", 2,
"header.from.url.user+';tgrp=vend5_6132606020_01a;trunk-
context=siptrunking.bell.ca'", 1;
MessageManipulations 2 = "Add Diversion", 4, "", "header.history-info
exists", "header.diversion", 0,
"'<sip:6132606020@vendor5.lab.internetvoice.ca;user=phone>'", 0;
MessageManipulations 3 = "Call Forward", 4, "any.request",
"header.history-info.0 regex (<sip:)(.)(.*)(@)(.*)",
"header.diversion.url.user", 2, "$3", 0;
MessageManipulations 4 = "Transfer & Forward", 4, "any.request",
"header.diversion exists", "header.diversion.url.host", 2,
"header.from.url.host", 0;
MessageManipulations 5 = "Call Transfer", 4, "any.request",
"header.referred-by exists", "header.diversion", 0,
"'<sip:6132606020@vendor5.lab.internetvoice.ca>'", 0;
MessageManipulations 6 = "Call Transfer", 4, "any.request", "",
"header.diversion.url.user", 2, "header.referred-by.url.user", 1;
MessageManipulations 7 = "Call Transfer", 4, "any.request", "",
"header.diversion.url.user", 6, "'+'", 0;
MessageManipulations 8 = "Call Transfer", 4, "any.request",
"header.referred-by exists", "header.referred-by", 1, "", 0;
MessageManipulations 9 = "Decline Cause", 4, "invite.response.603", "",
"header.request-uri.methodtype", 2, "'486'", 0;
MessageManipulations 10 = "Dynamic ONND", 4, "any.request", "",
"header.to.url.userphone", 1, "", 0;
MessageManipulations 11 = "Dynamic ONND", 4, "any.request", "",
"header.from.url.userphone", 1, "", 0;
MessageManipulations 12 = "Dynamic ONND", 4, "any.request", "",
"header.p-asserted-identity.url.userphone", 1, "", 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 ]
```

B Configuring Dynamic ONND

The procedure below describes additional steps needed to configure Dynamic Outgoing Name & Number Display (ONND) presentation mode.

B.1 Configure SIP Message Manipulation Rules

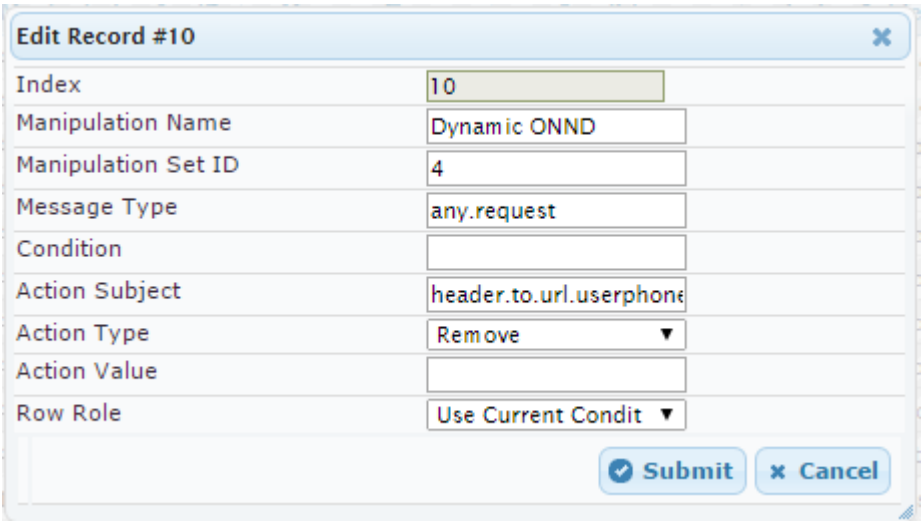
The following SIP message manipulation rules should be configured in order to work in Dynamic ONND mode.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add a manipulation rule to Index 10 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes the 'userphone' parameter from the SIP To Header.

Parameter	Value
Index	**10**
Manipulation Name	**Dynamic ONND**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.to.url.userphone**
Action Type	**Remove**

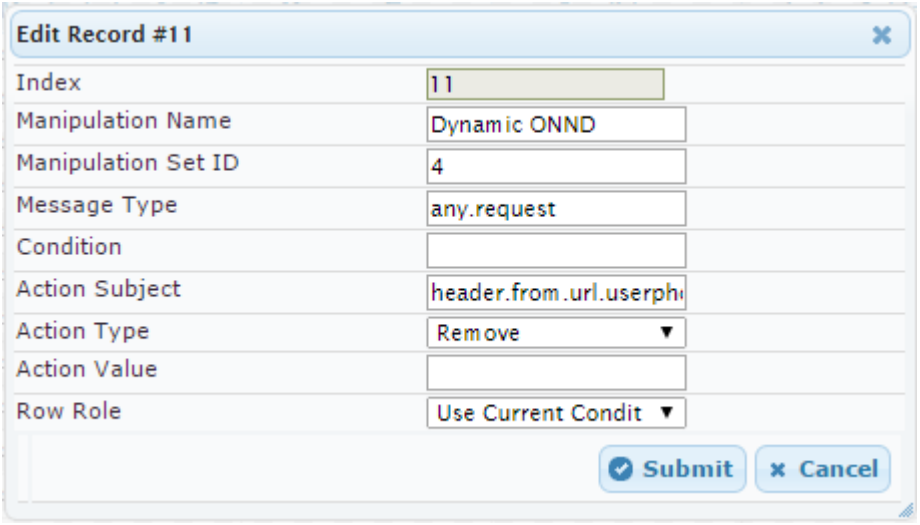
Figure B-1: Configuring SIP Message Manipulation Rule 10 (for Bell Canada's SIP Trunk)



3. Add a manipulation rule to Index 11 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes the 'userphone' parameter from the SIP From Header.

Parameter	Value
Index	**11**
Manipulation Name	**Dynamic ONND**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.from.url.userphone**
Action Type	**Remove**

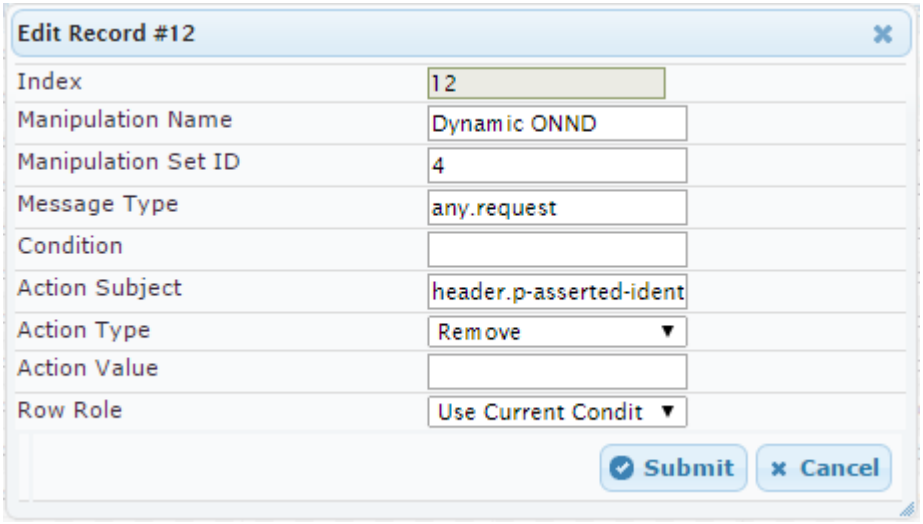
Figure B-2: Configuring SIP Message Manipulation Rule 11 (for Bell Canada's SIP Trunk)



4. Add a manipulation rule to Index 12 for Bell Canada's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the Bell Canada SIP Trunk (IP Group 2). This removes the 'userphone' parameter from the SIP P-Asserted-Identity Header.

Parameter	Value
Index	**12**
Manipulation Name	**Dynamic ONND**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.p-asserted-identity.url.userphone**
Action Type	**Remove**

Figure B-3: Configuring SIP Message Manipulation Rule 11 (for Bell Canada's SIP Trunk)



AudioCodes

Configuration Note

http://www.audiocodes.