AudioCodes™ Mediant™ Series

Enterprise Session Border Controllers

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2010 and QSC AG SIP Trunk using AudioCodes Mediant E-SBC

QSC AG
Ihre Premium-Alternative

Microsoft Partner
Gold Unified Communications

Microsoft® Lync™

Version 6.6

Document #: LTRT-33402

January 2013

AudioCodes

Table of Contents

List of Figures

Reader's Notes

Notice

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

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

Date Published: January-30-2013

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Note: Throughout this manual, unless otherwise specified, the term *E-SBC* refers to any of the following AudioCodes products:

- Mediant 800 Gateway & E-SBC
- Mediant 1000B Gateway & E-SBC
- Mediant 3000 Gateway & E-SBC
- Mediant 4000 E-SBC

Reader's Notes

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between QSC AG SIP Trunking and Microsoft's Lync Communication platform (Lync Server 2010).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and QSC AG Partners who are responsible for installing and configuring QSC AG SIP Trunking and Microsoft's Lync Communication platform 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 service provider's VoIP networks.

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

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

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

Reader's Notes

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.60A.022.003
Protocol	▪ SIP/UDP (to the QSC AG SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 QSC AG SIP Trunking Version

Table 2-2: QSC AG Version

Vendor/Service Provider	QSC AG
SSW Model/Service	IPfonie extended
Software Version	
Protocol	SIP-DDI
Additional Notes	None

2.3 Microsoft Lync Server 2010 Version

Table 2-3: Microsoft Lync Server 2010 Version

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

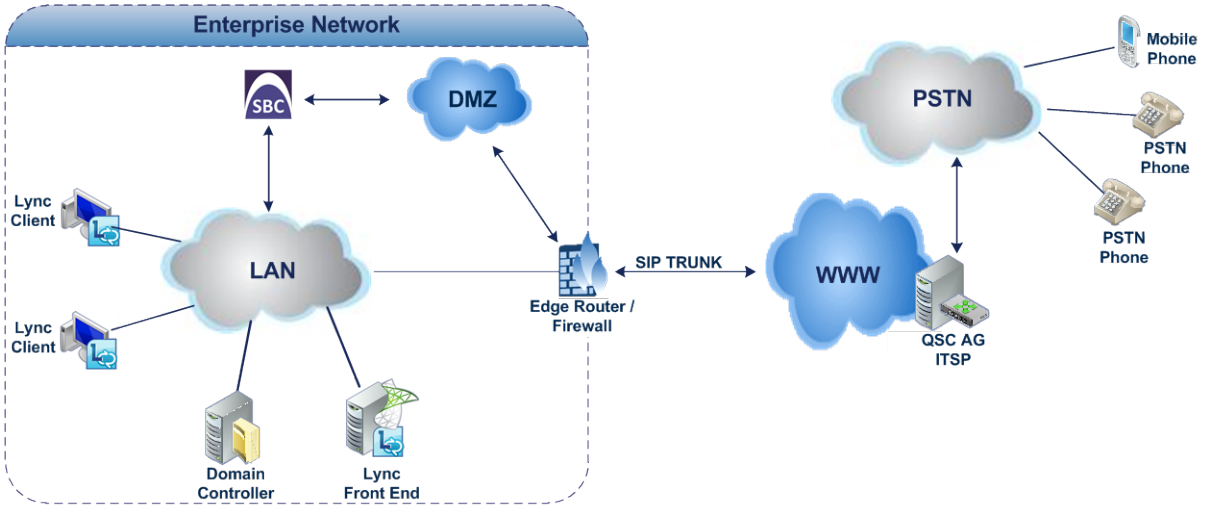
2.4 Deploying the E-SBC - Typical Topology

The procedures in this document describe how to deploy the E-SBC using the following example scenario:

- The Enterprise is deployed with Microsoft Lync Server 2010 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 QSC AG SIP Trunking service (Internet telephony service provider / ITSP).
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - Session: Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - Border: IP-to-IP network border between Lync Server 2010 network in the Enterprise LAN and QSC AG SIP Trunk located in the public network.

The figure below illustrates E-SBC interworking between Lync Server 2010 and QSC AG SIP Trunking site.

Figure 2-1: E-SBC Interworking Microsoft Lync and QSC AG SIP Trunk Topology Example



2.5 Environment Setup

The example scenario includes the following environment setup:

Table 2-4: Environment Setup

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

2.6 Known Limitations

There were no limitations observed in the Interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2010 and QSC AG SIP Trunk.

Reader's Notes

3 Configuring Lync Server 2010

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

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

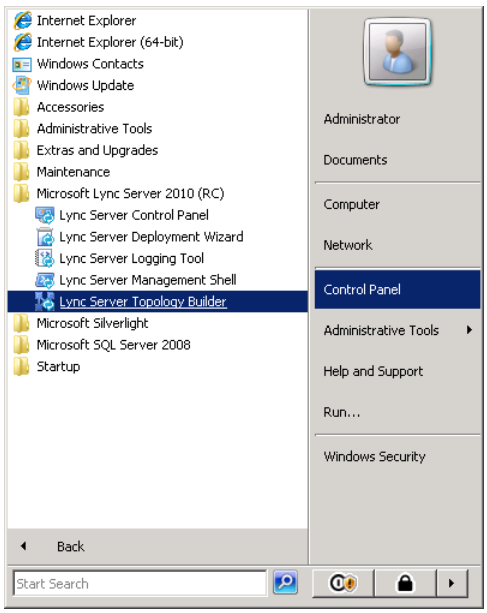
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

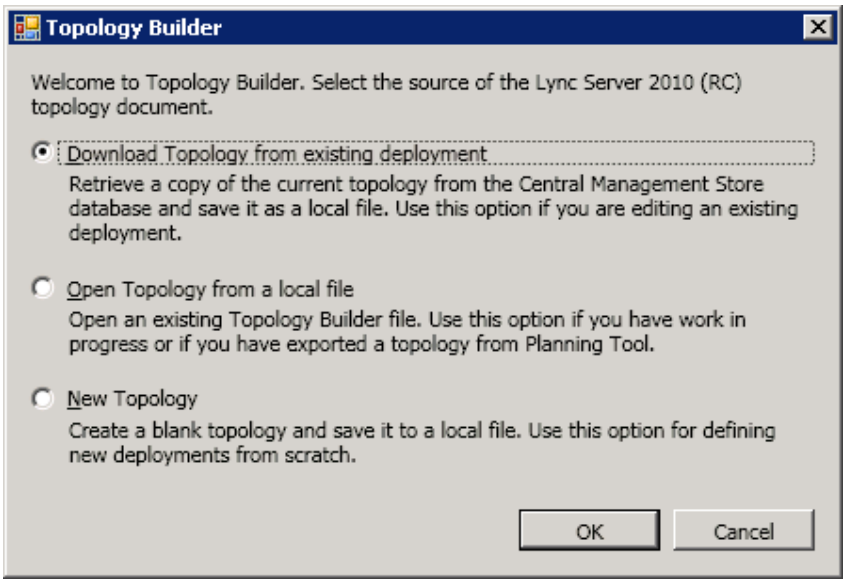
1. On the server where the Topology Builder is installed, start the Lync Server 2010 Topology Builder by doing the following: Click the Windows **Start** menu, click **All Programs**, and then click **Lync Server Topology Builder**.

Figure 3-1: Starting the Lync Server Topology Builder



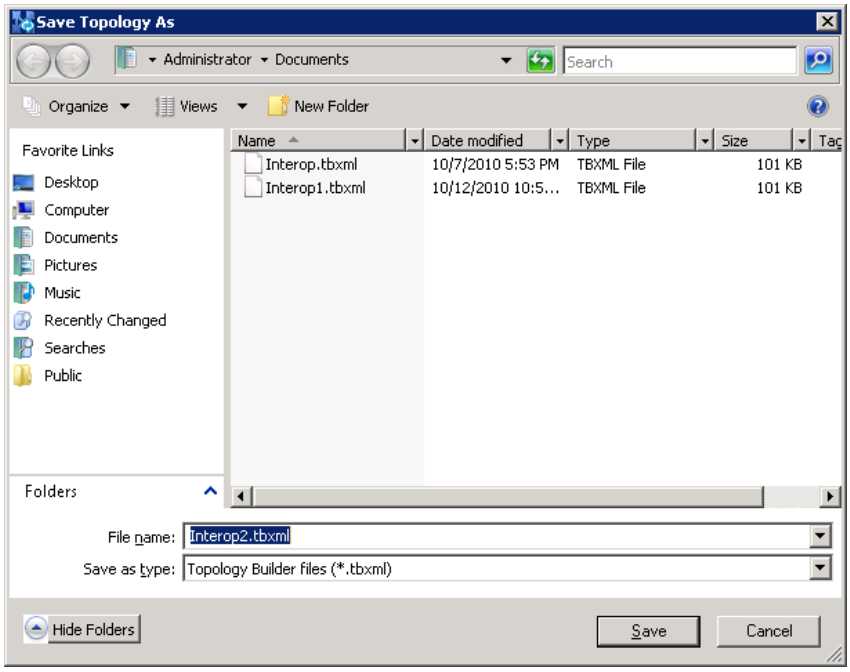
The following screen is displayed:

Figure 3-2: Topology Builder Options



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

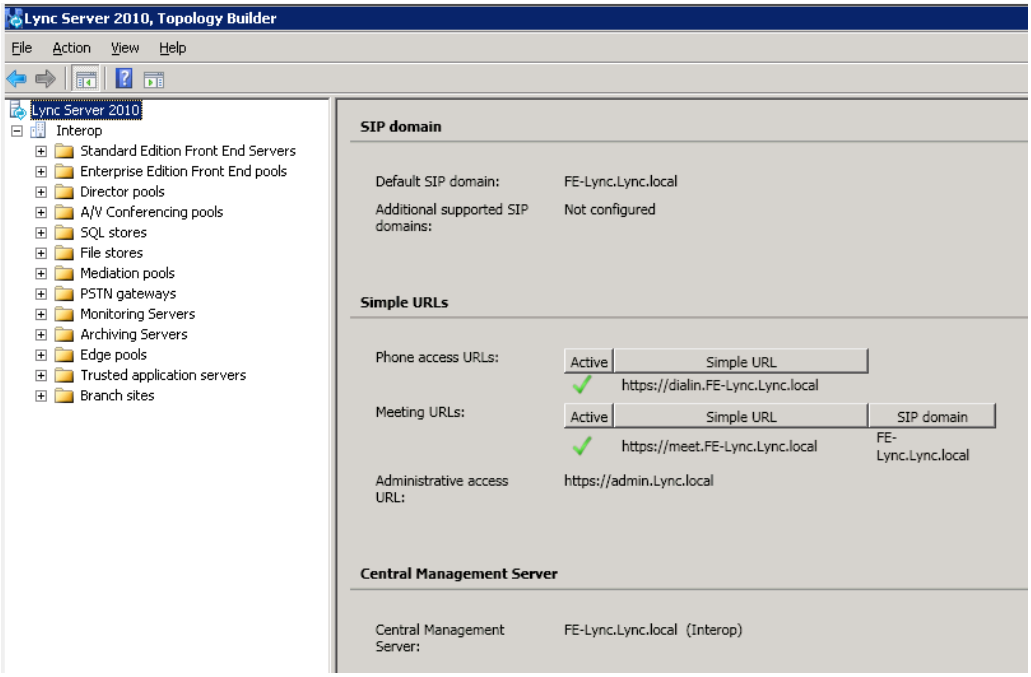
Figure 3-3: Save Topology



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

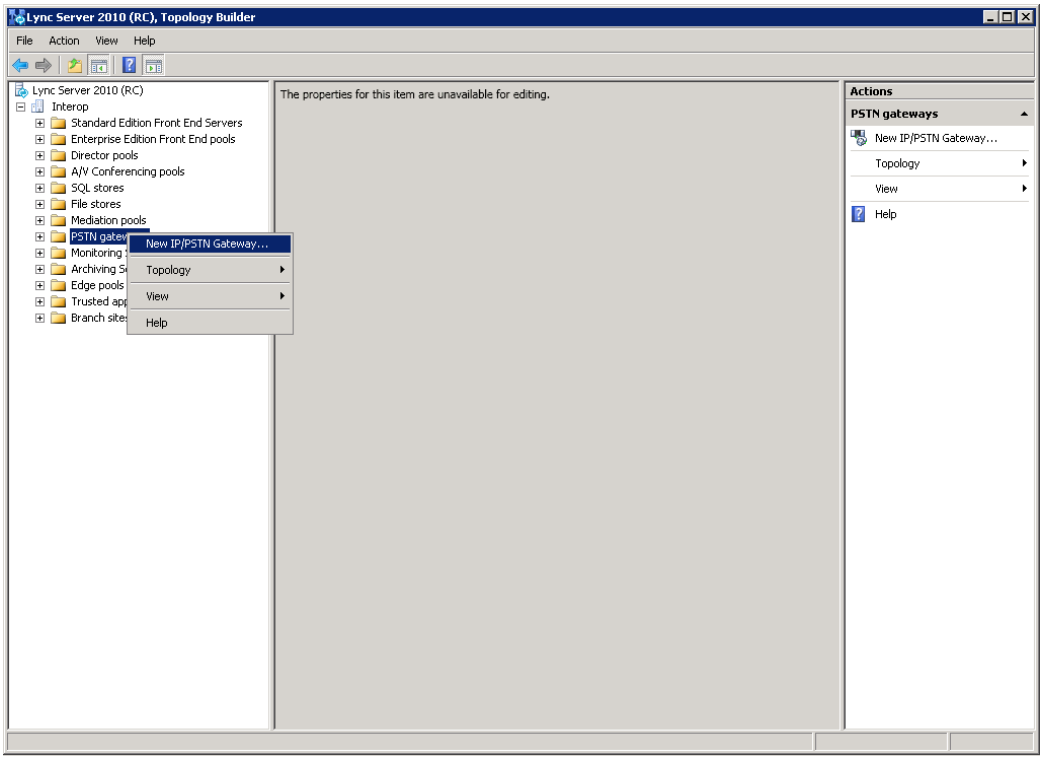
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



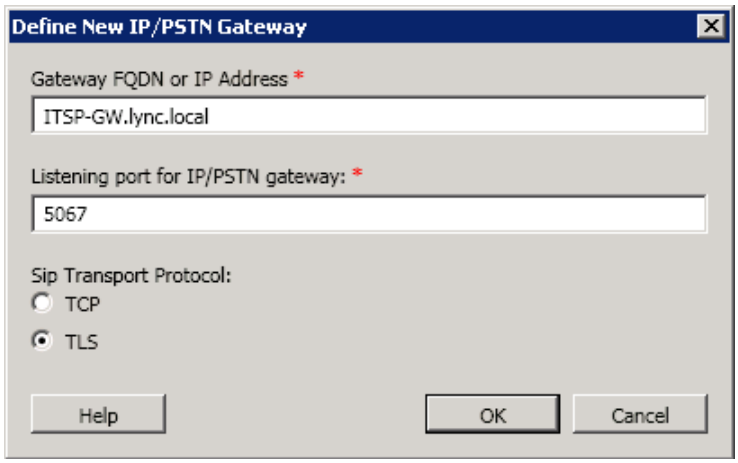
4. Expand the site tree located in the left pane.
5. Right-click the **PSTN gateways** folder, and then choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



The following dialog box appears:

Figure 3-6: Define New IP/PSTN Gateway

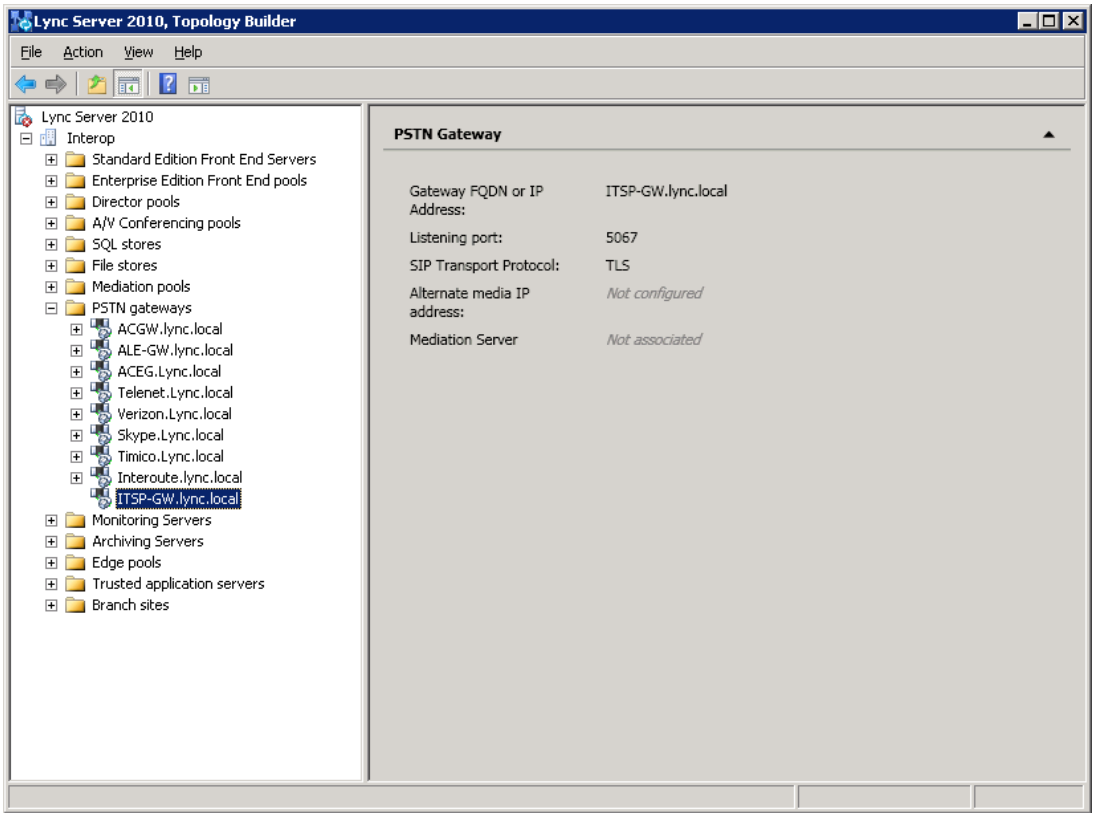


6. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., "ITSP-GW.lync.local"), and then click **OK**.

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

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

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



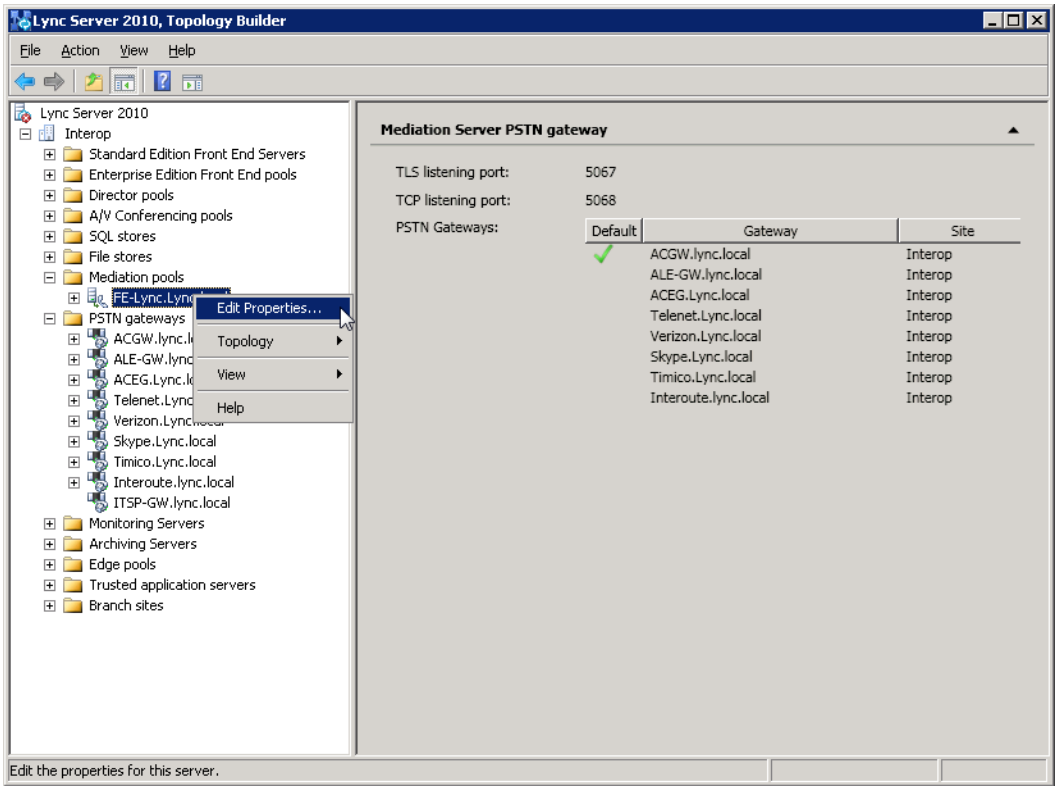
3.2 Associating IP / PSTN Gateway with Mediation Server

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

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

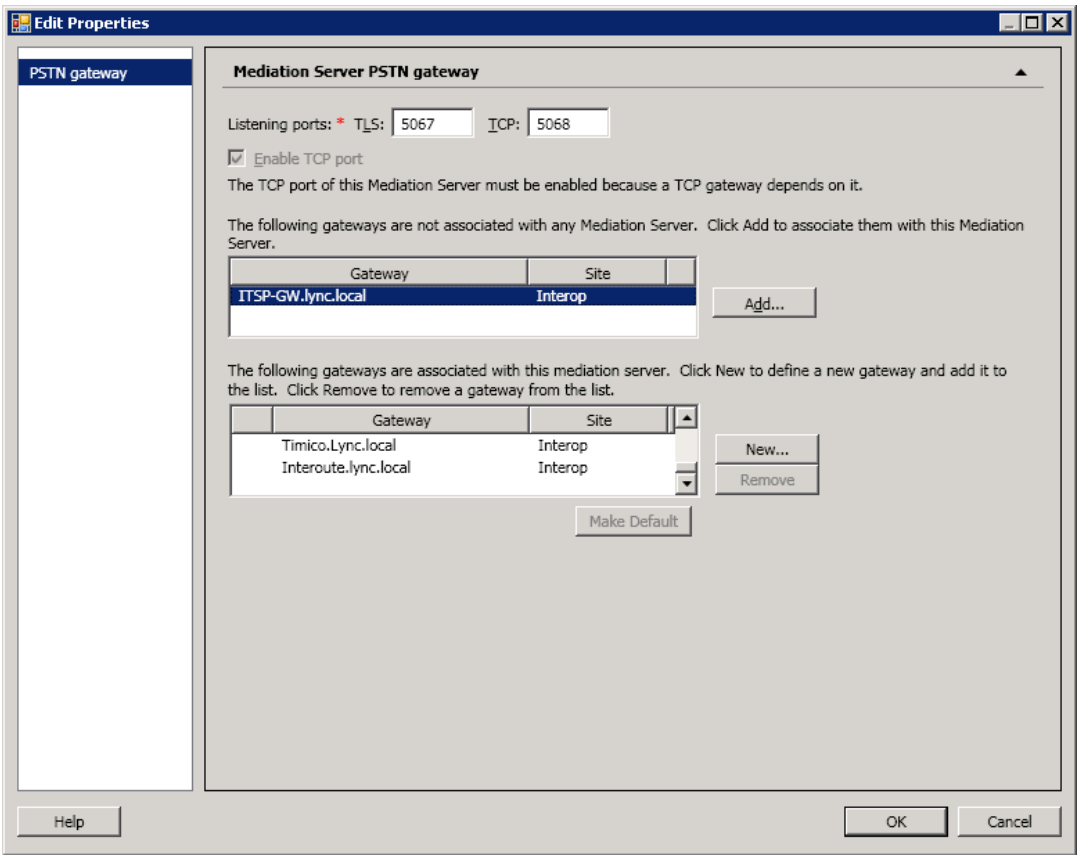
1. In the tree, right-click the Mediation Server that uses the E-SBC (e.g., **FE-Lync.Lync.local**), and then choose **Edit Properties**, as shown below:

Figure 3-8: Choosing Mediation Server



The following screen is displayed:

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

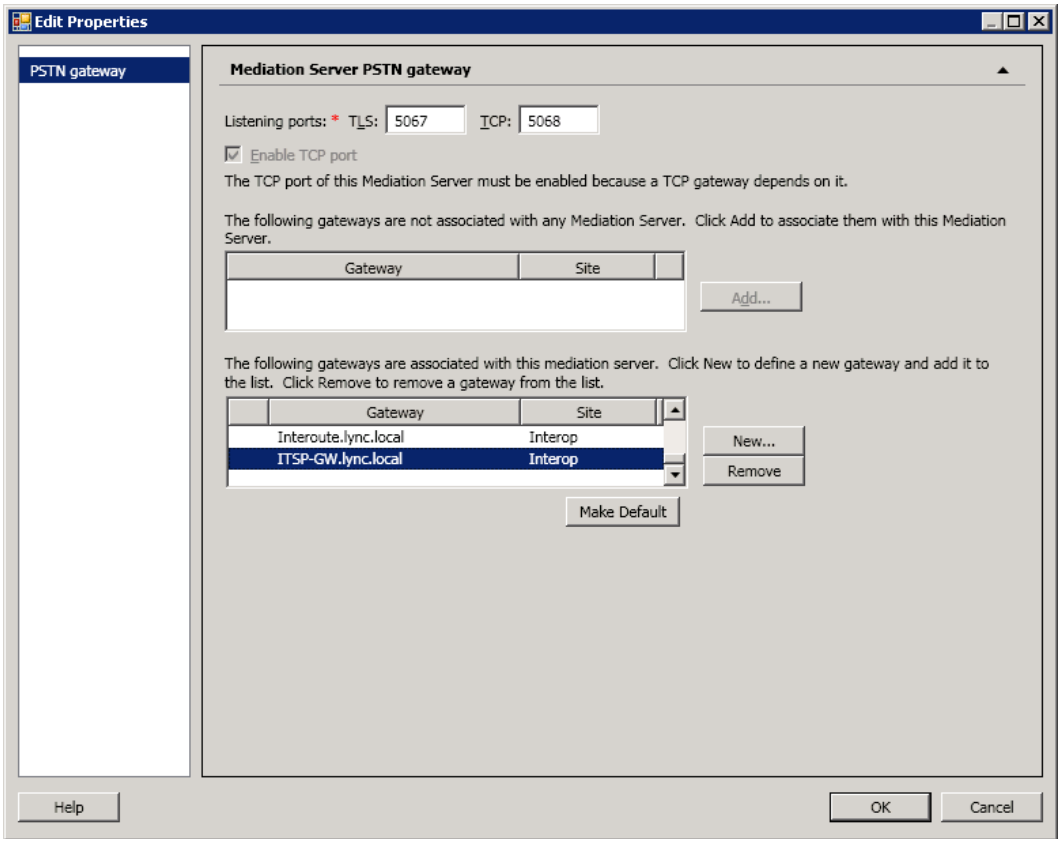


2. In the left pane, choose **PSTN gateway** to open the Mediation Server PSTN gateway pane, and then do the following:
   a. In the list of gateways that are not associated with the Mediation Server, select the E-SBC (e.g., **ITSP-GW.lync.local**).
   b. Click **Add** to associate it with the Mediation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

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

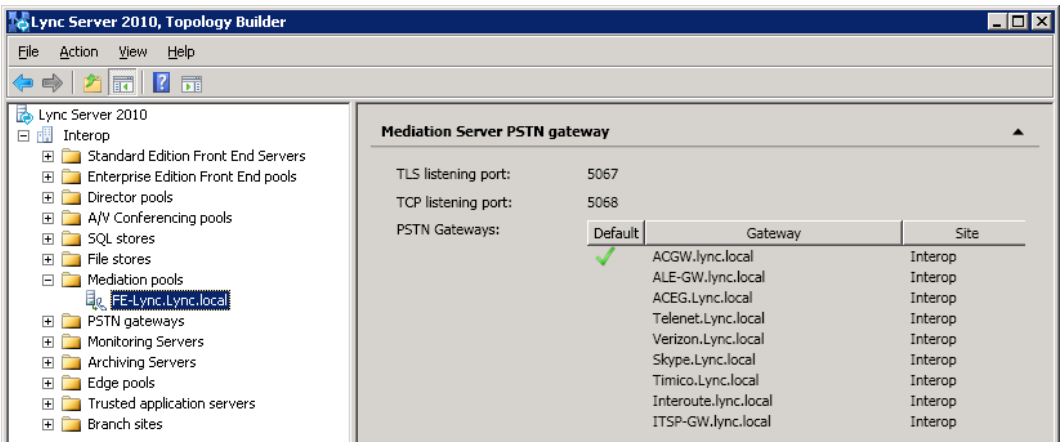
The E-SBC appears in the sub-pane that lists gateways associated with the Mediation Server, as shown below:

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



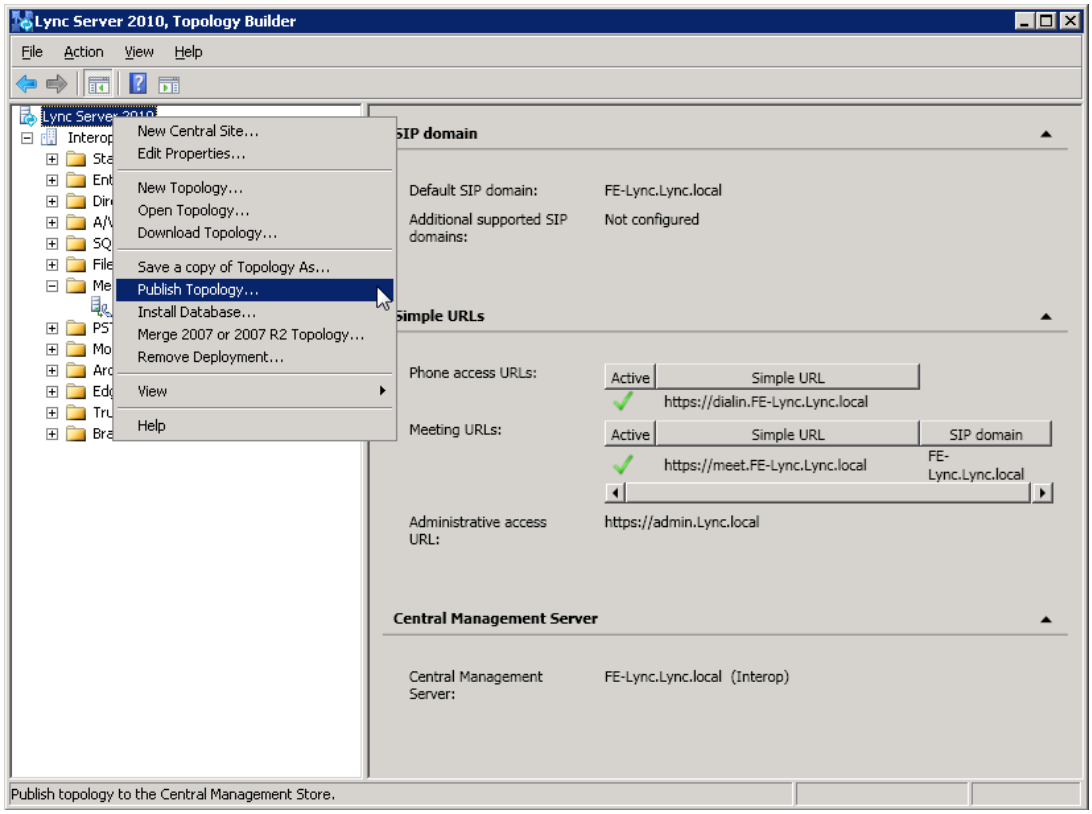
3. Click **OK**.

Figure 3-11: Media Server PSTN Gateway Association Properties



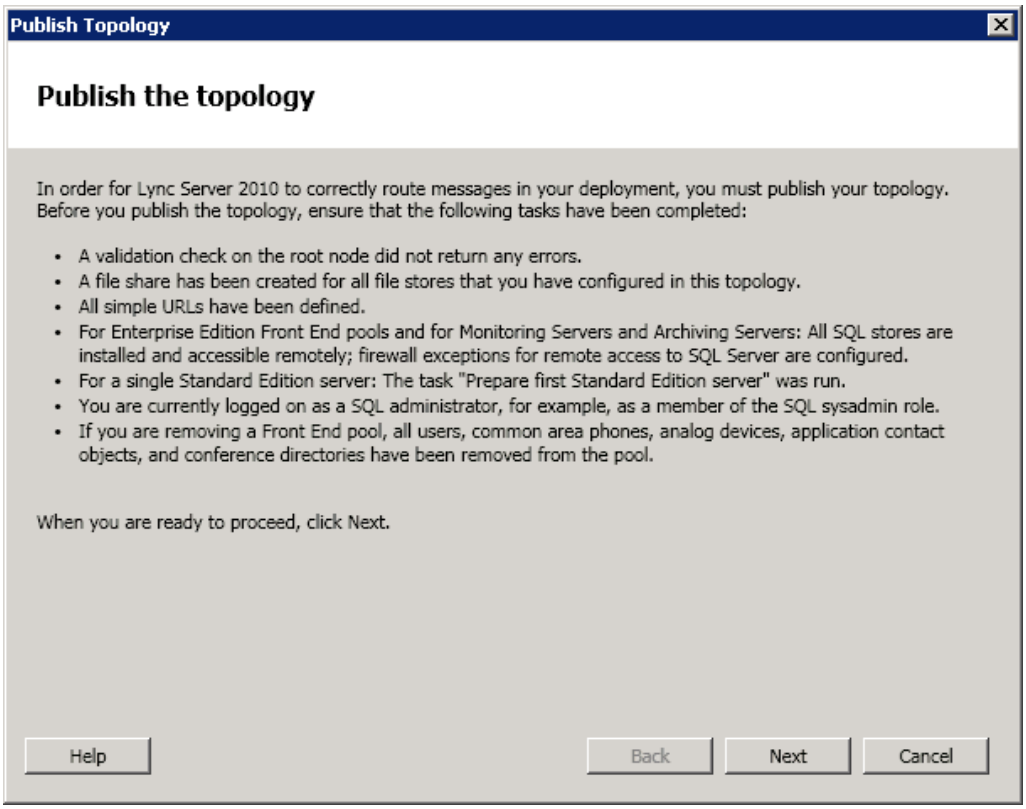
4. In the main tree, select the root item **Lync Server 2010**, and then from the **Action** menu on the menu bar, choose **Publish Topology**, as shown below:

Figure 3-12: Choosing Publish Topology



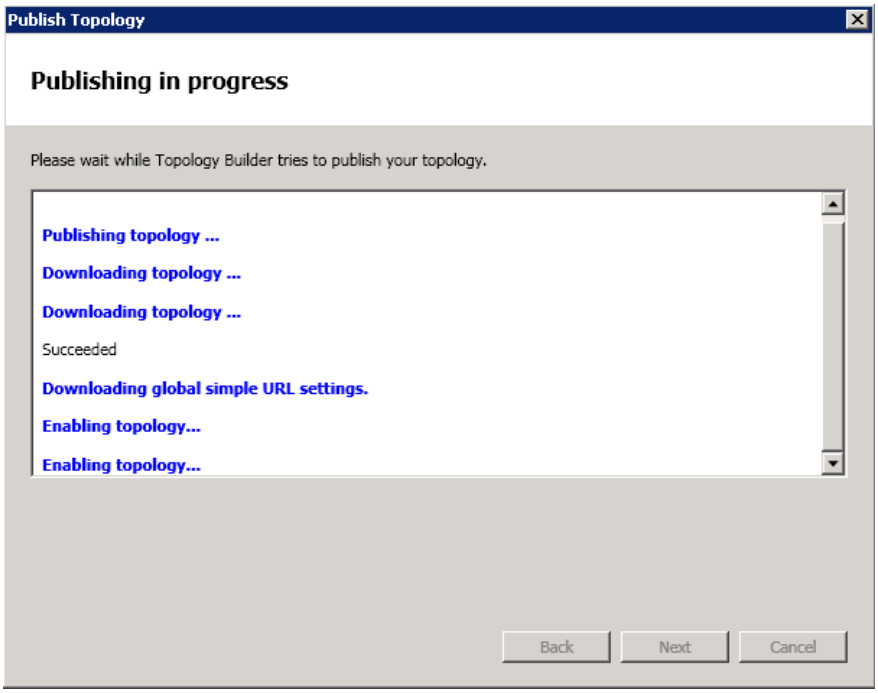
The Publish Topology screen is displayed:

Figure 3-13: Publish Topology Screen



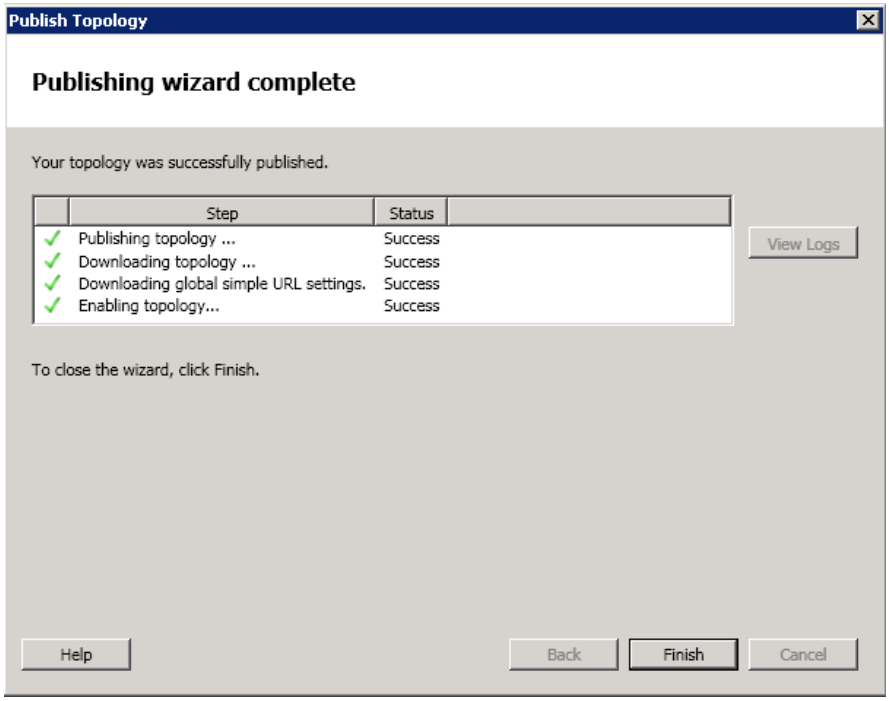
5. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-14: Publish Topology Progress Screen



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

Figure 3-15: Publish Topology Successfully Completed



7. Click **Finish**.

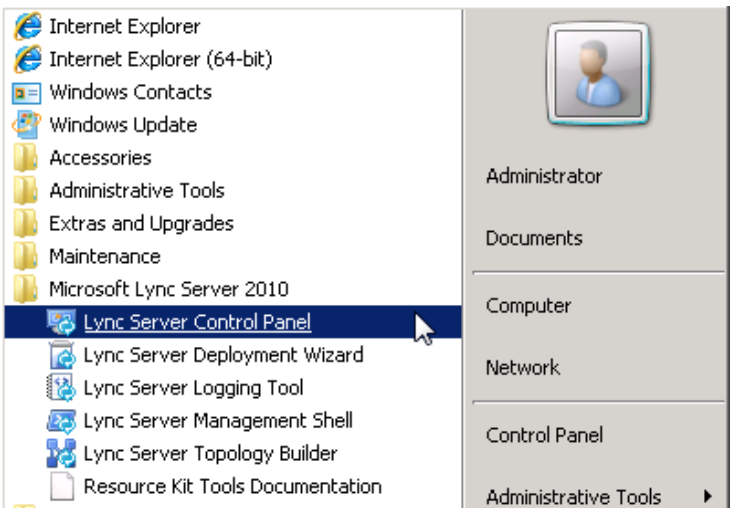
3.3 Configuring the "Route" on Lync Server 2010

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

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

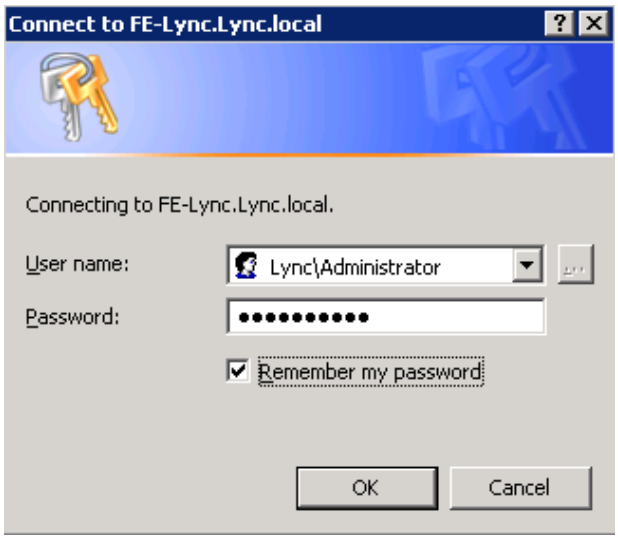
1. Start the Microsoft Lync Server 2010 Control Panel: click **Start**, click **All Programs**, click **Microsoft Lync Server 2010**, and then click **Lync Server Control Panel**, as shown below:

Figure 3-16: Opening the Lync Server Control Panel



You are prompted to enter your login credentials:

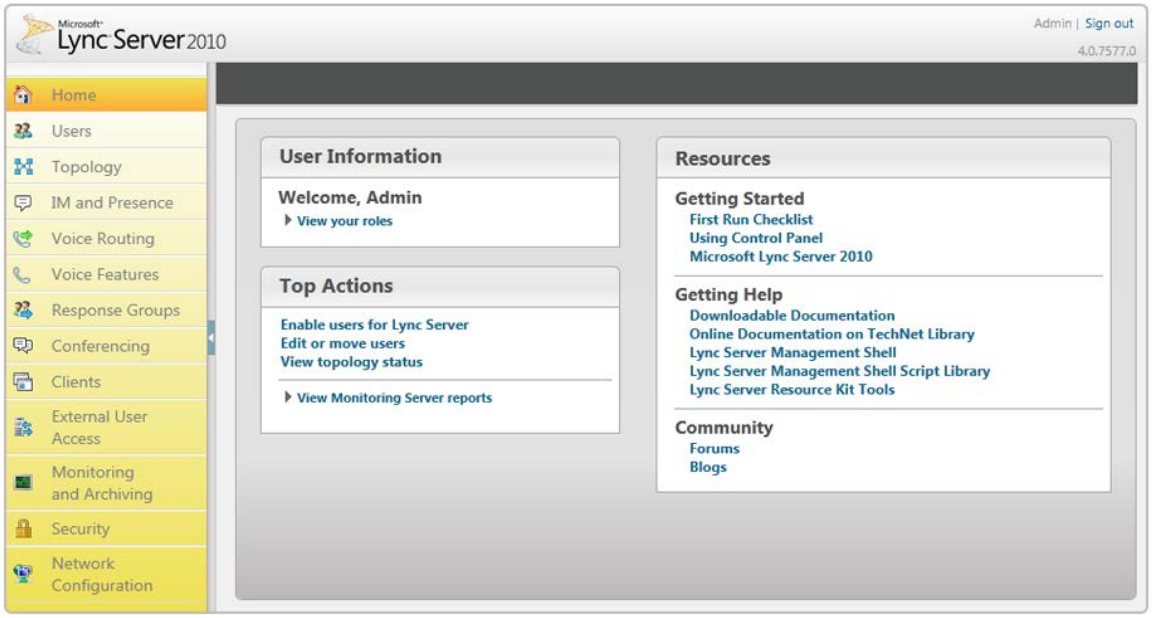
Figure 3-17: Lync Server Credentials



2. Enter your domain username and password, and then click **OK**.

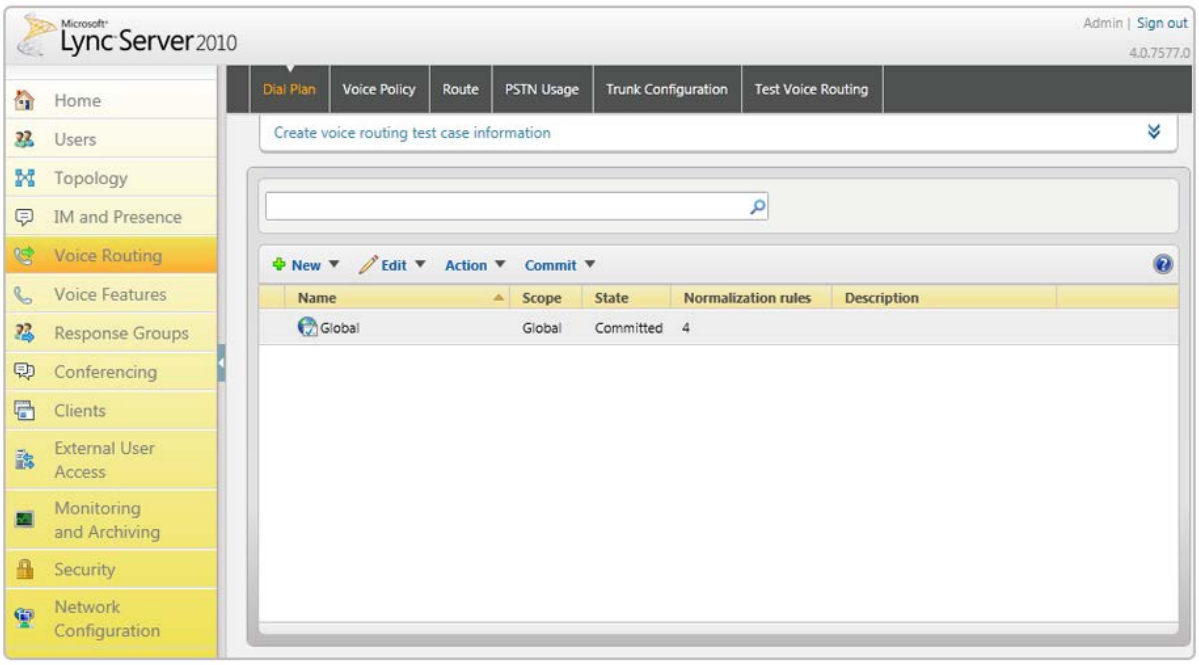
The Microsoft Lync Server 2010 Control Panel is displayed:

Figure 3-18: Microsoft Lync Server 2010 Control Panel



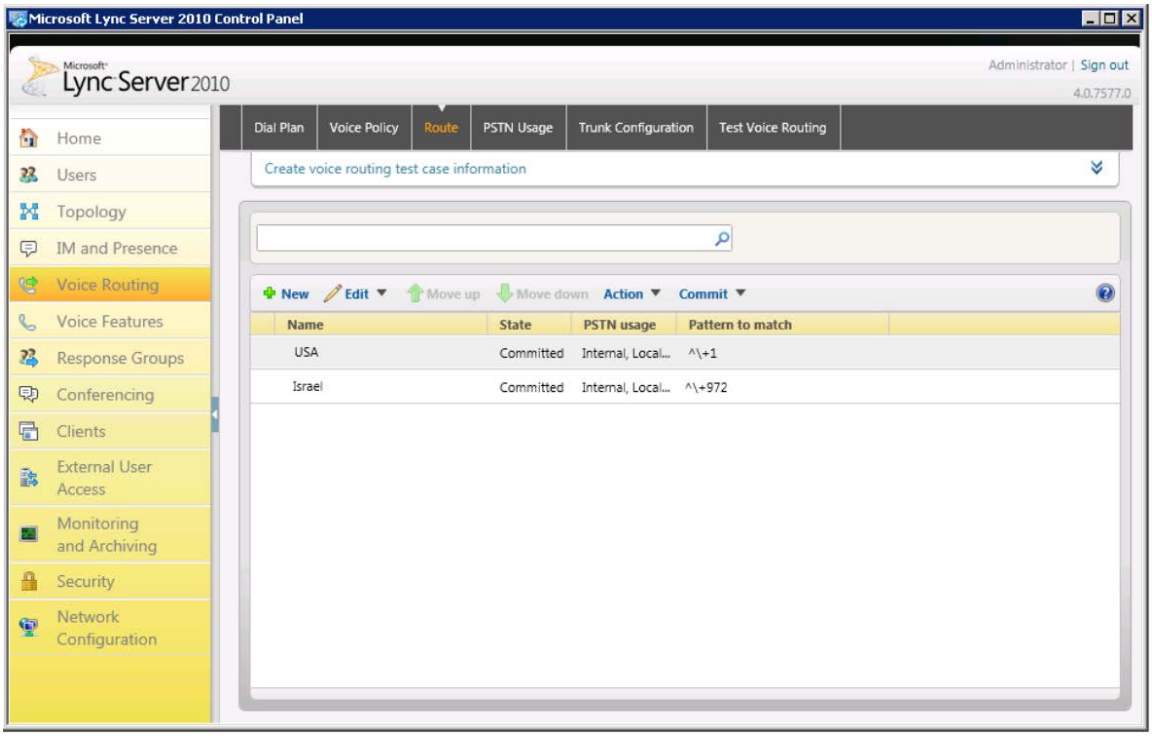
3. In the left navigation pane, select **Voice Routing**.

Figure 3-19: Voice Routing Page



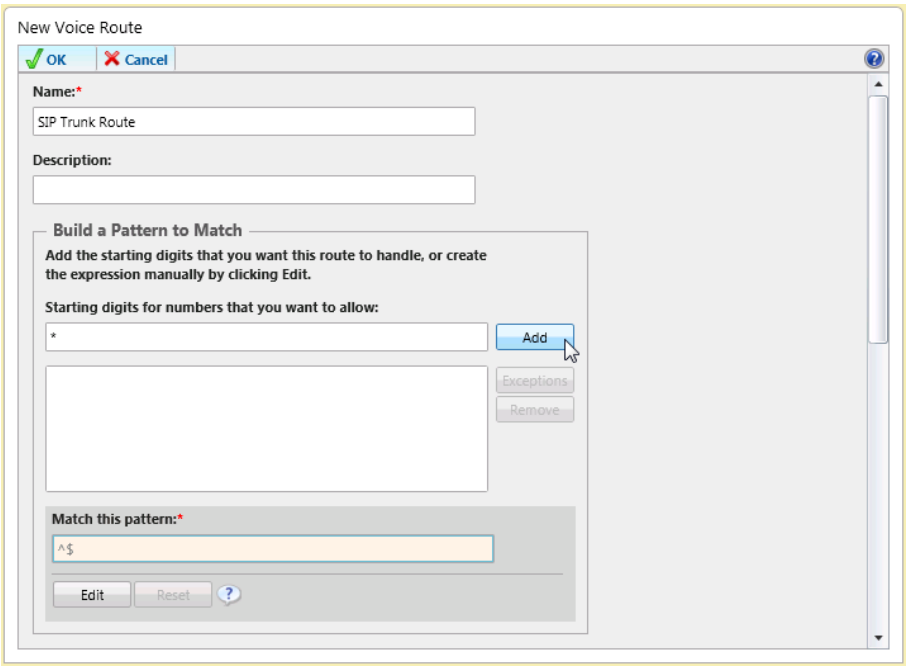
4. In the Voice Routing page, click the **Route** tab.

Figure 3-20: Route Option



5. Click **New**; the New Voice Route dialog box appears:

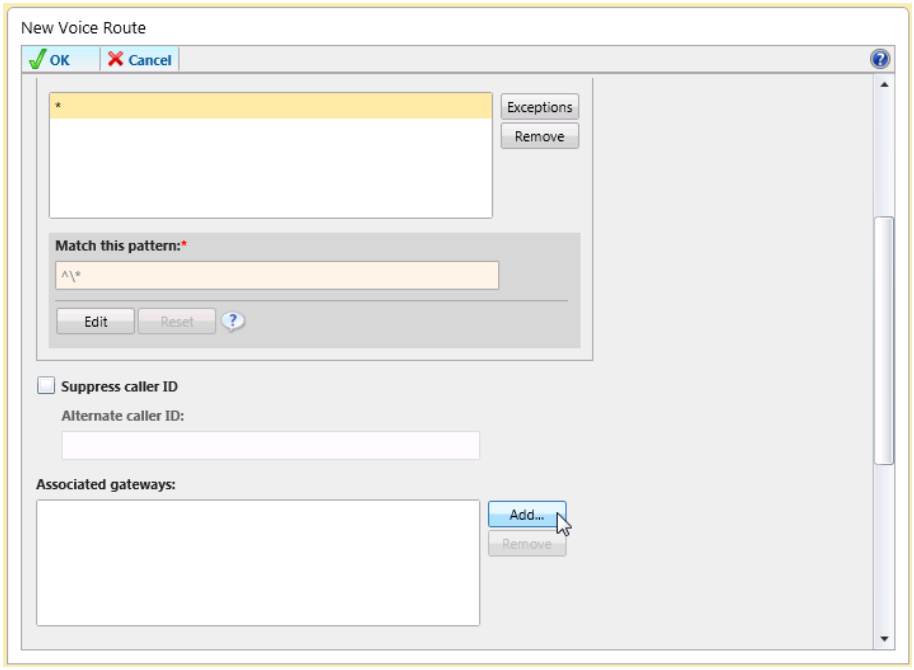
Figure 3-21: Adding New Voice Route



6. In the Name field, enter a name for this route (e.g., "SIP Trunk Route").
7. In the Build a Pattern to Match field, enter the starting digits you want this route to handle (e.g., "*", which means to match all numbers).

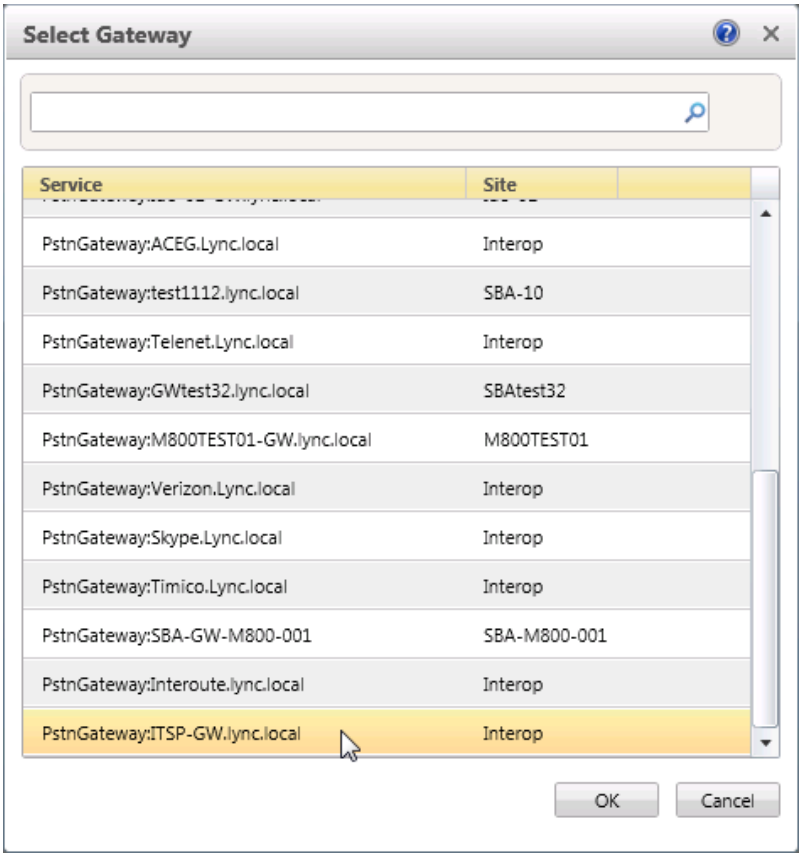
8. Click **Add**.

Figure 3-22: Adding New E-SBC Gateway



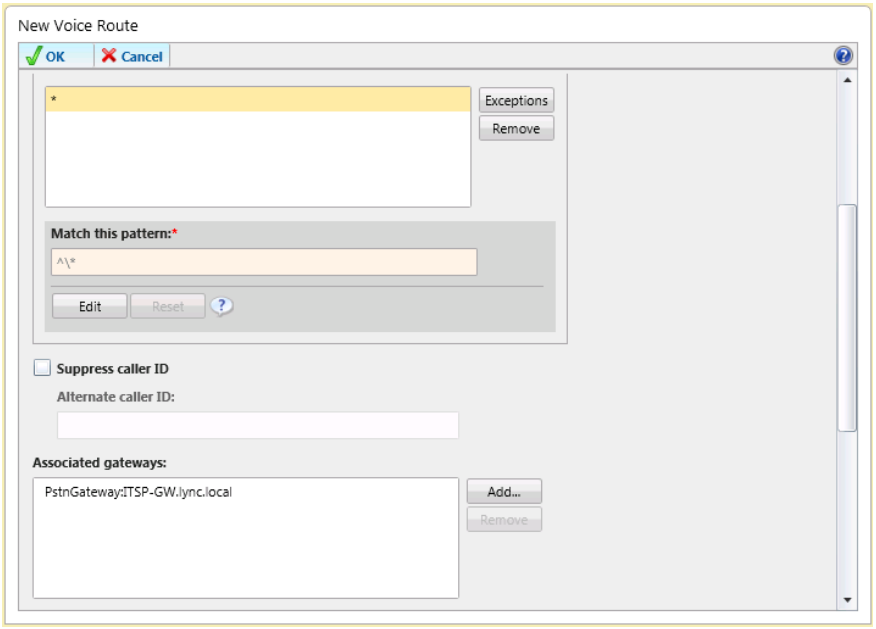
9. Associate the route with the E-SBC IP/PSTN gateway that you created:
   a. In the Associated gateways pane, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-23: List of Deployed Gateways



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

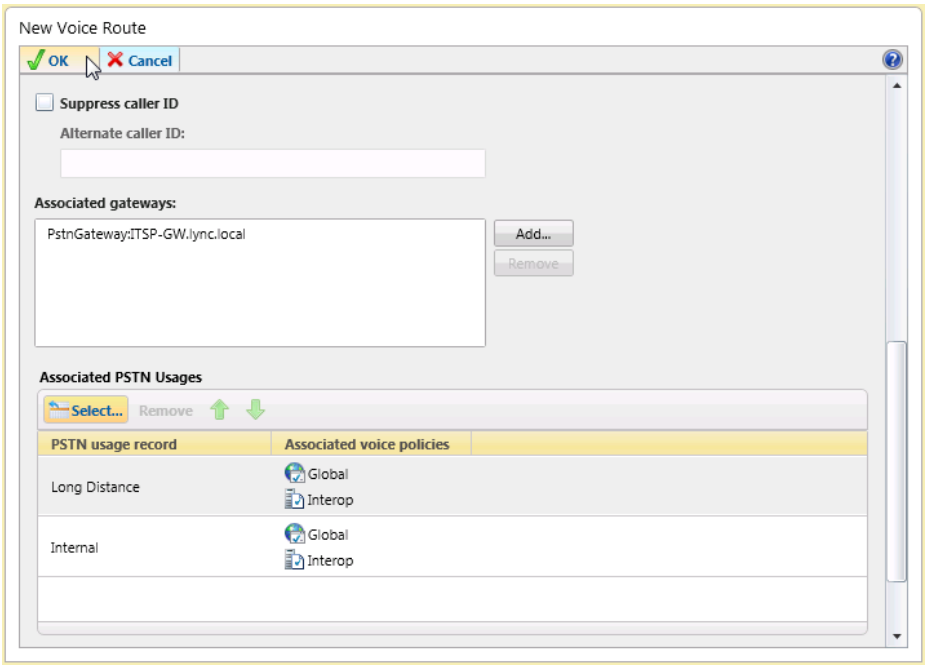
Figure 3-24: Selected E-SBC Gateway



10. Associate a PSTN Usage to this route:

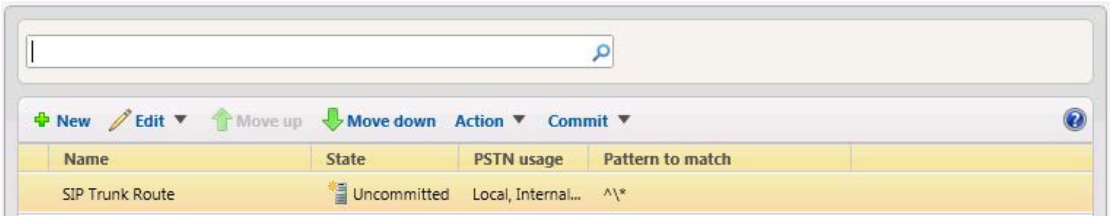
a. In the Associated PSTN Usages group, click **Select** and then add the associated PSTN Usage.

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



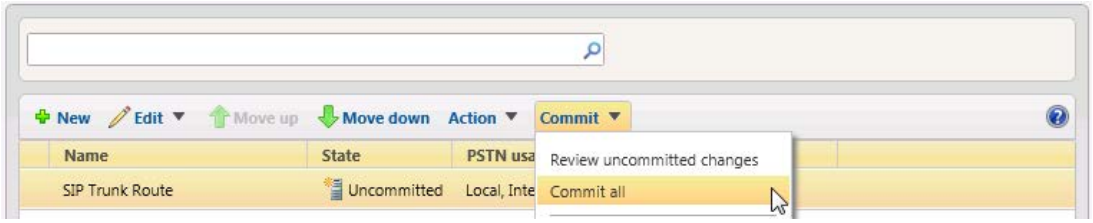
11. Click **OK** (located on the top of the New Voice Route dialog box); the New Voice Route (Uncommitted) is displayed:

Figure 3-26: Confirmation of New Voice Route



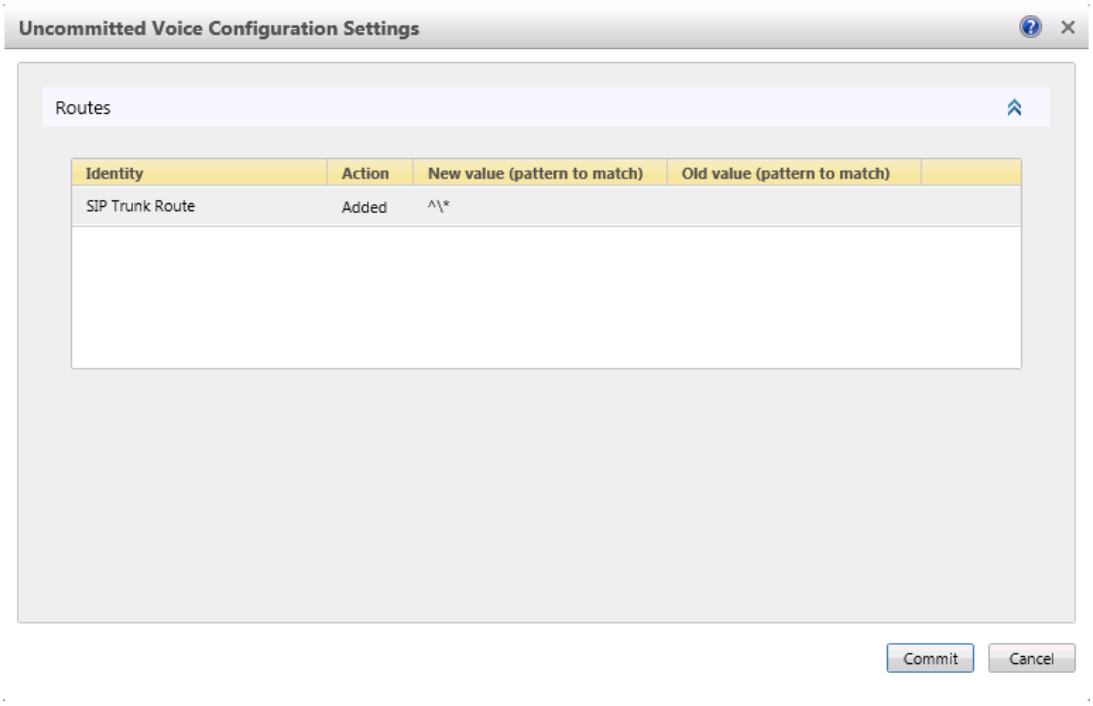
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-27: Committing Voice Routes



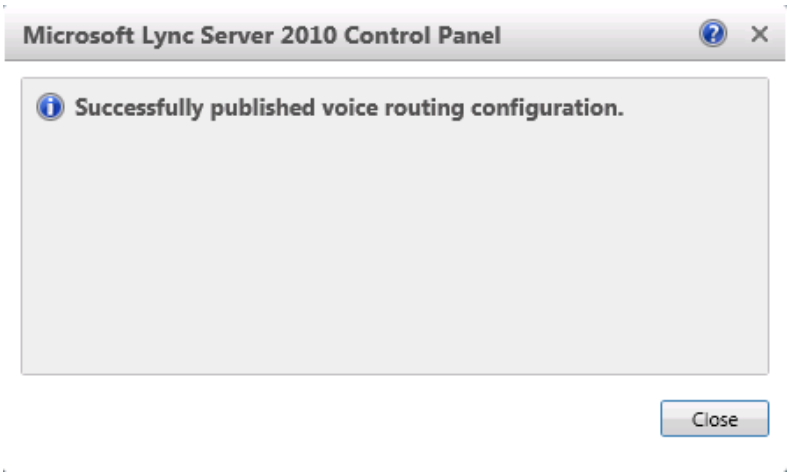
The Uncommitted Voice Configuration Settings dialog box appears:

Figure 3-28: Uncommitted Voice Configuration Settings



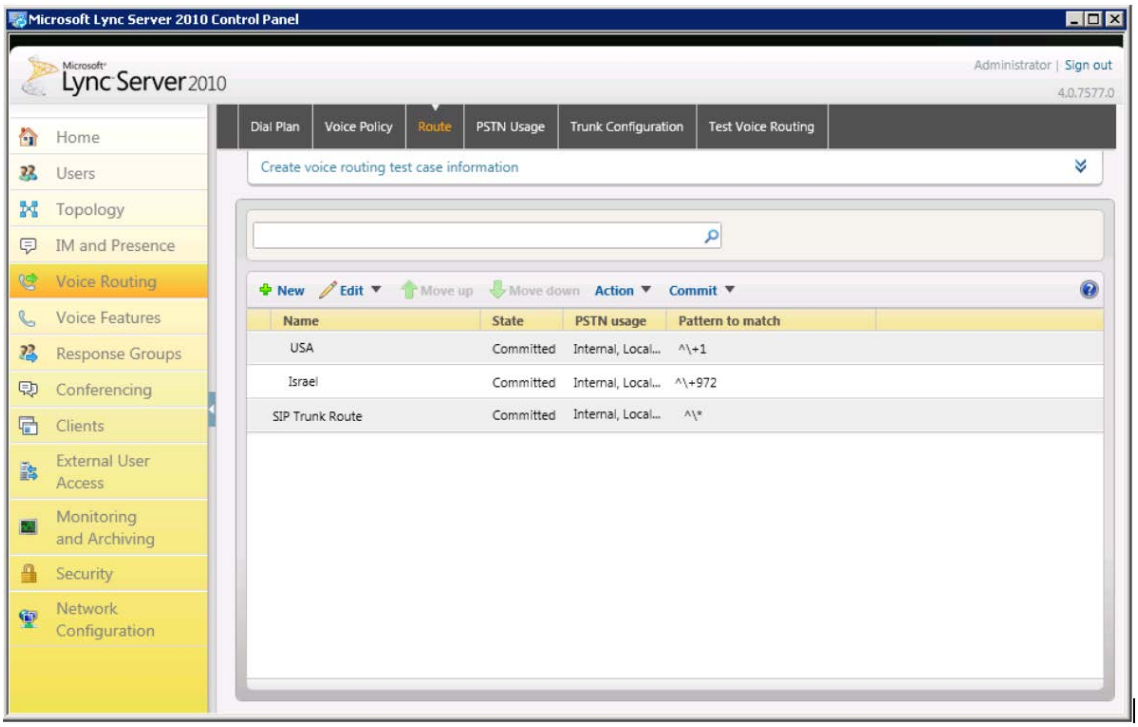
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-29: Confirmation of Successful Voice Routing Configuration



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

Figure 3-30: Voice Routing Screen Displaying Committed Routes



Reader's Notes

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2010 and QSC AG SIP Trunk:

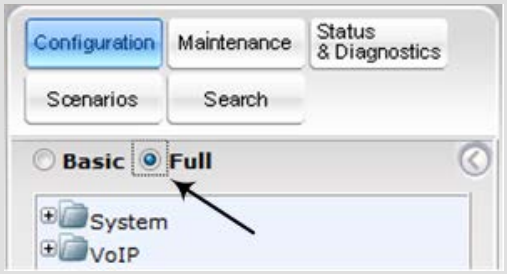
- E-SBC WAN interface: QSC AG SIP Trunking environment
- E-SBC LAN interface: Lync Server 2010 environment

This configuration is done using the E-SBC's Web-based management tool (embedded Web server).

Notes:

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

  For more information about the Software Upgrade Feature 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 Technical Note* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Full-menu display mode. To do this, select the **Full** option, as displayed below:



When the E-SBC is reset, the Web GUI reverts to Basic-menu display.

4.1 Step 1: Network Interface Configuration

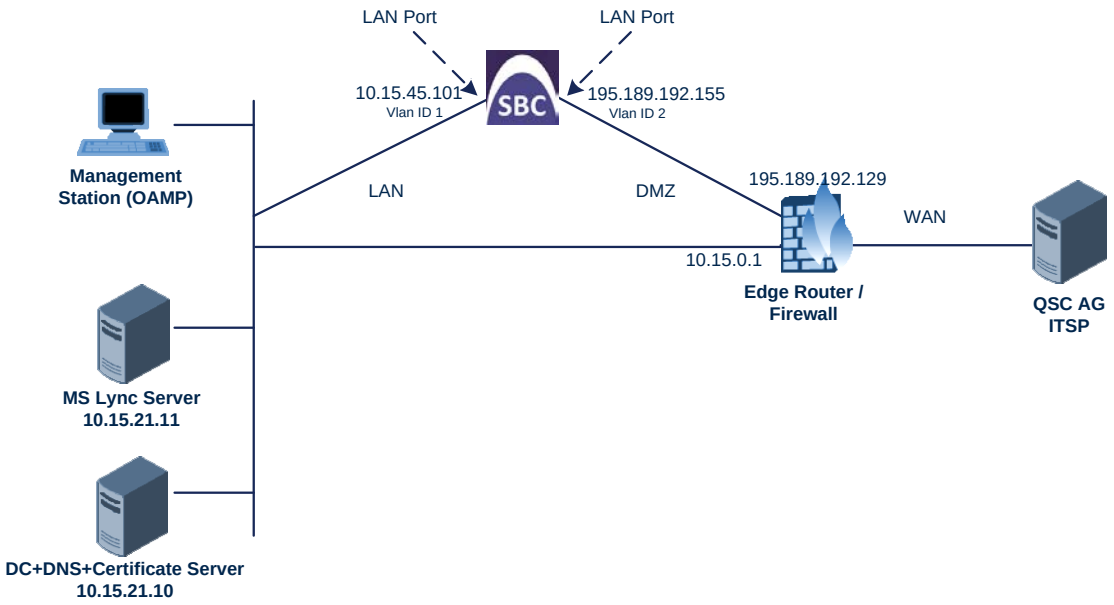
This step describes how to configure the E-SBC's network interfaces. There are several ways to deploy the E-SBC. However, the example scenario in this document uses the following deployment method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the QSC AG SIP Trunk located on the WAN.
- The E-SBC connects to the WAN through a DMZ network.

The type of physical LAN connection depends on the method used to connect to the Enterprise's network. In this example, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and network cables).

In addition, the E-SBC uses two logical network interfaces; one to the LAN (VLAN ID 1) and one to the WAN (VLAN ID 2).

Figure 4-1: Network Interfaces



4.1.1 Configure Network Interfaces

The procedure below describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP ("Voice")
- WAN VoIP ("WANSP")

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

1. Open the Multiple Interface Table page (**Configuration** > **VoIP** > **Network** > **IP Settings**).

Figure 4-2: Multiple Interface Table

2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button corresponding to the Application Type, "OAMP + Media + Control", and then click **Edit**.
   b. Set the interface as follows:

Parameter	Setting
IP Address	E-SBC IP address (e.g., "10.15.45.101")
Prefix Length	Subnet mask in bits (e.g., "16" for 255.255.0.0)
Gateway	Default Gateway (e.g., "10.15.0.1")
VLAN ID	VLAN ID (e.g., "1")
Interface Name	Arbitrary descriptive name (e.g., "Voice")
Primary DNS Server IP Address	DNS IP address (e.g., "10.15.21.10")
Underlying Interface	Ethernet port group (e.g., **GROUP_1**)

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

Parameter	Setting
Application Type	Application (e.g., **Media + Control**)
IP Address	WAN IP address (e.g., "195.189.192.155")
Prefix Length	"16" for 255.255.0.0
Gateway	Default Gateway - router's IP address (e.g., "195.189.192.129")
VLAN ID	WAN VLAN ID (e.g., "2")
Interface Name	Arbitrary descriptive name of WAN interface (e.g., "WANSP")
Primary DNS Server IP Address	DNS IP address (eg.,"80.179.52.100")
Secondary DNS Server IP Address	DNS IP address (e.g.,"80.179.55.100")

Parameter	Setting
Underlying Interface	Ethernet port group (e.g., **GROUP_2**)

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

4.1.2 Configure the Native VLAN ID

The procedure below describes how to configure the Native VLAN ID for the two network interfaces (LAN and WAN). You must configure a separate physical port interface with a unique Native VLAN ID for both the Voice and the WANSP interfaces.

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

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

Figure 4-3: Ports Native VLAN

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

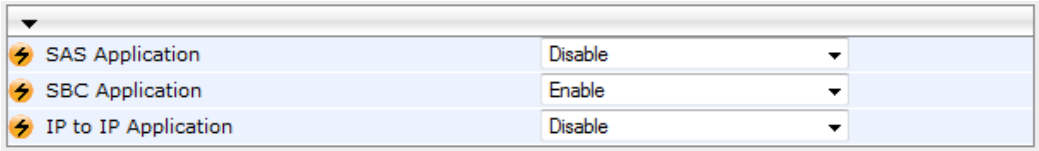
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-4: Applications Enabling



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

4.3 Step 3: Signaling Routing Domains

This step describes how to configure Signaling Routing Domains (SRD). An SRD is a set of definitions comprising IP interfaces, E-SBC resources, SIP behaviors, and Media Realms.

4.3.1 Configuring Media Realms

A Media Realm represents a set of ports associated with an IP interface, which are used by the E-SBC to transmit or receive media (RTP or SRTP). Media Realms are associated with SRDs or IP Groups.

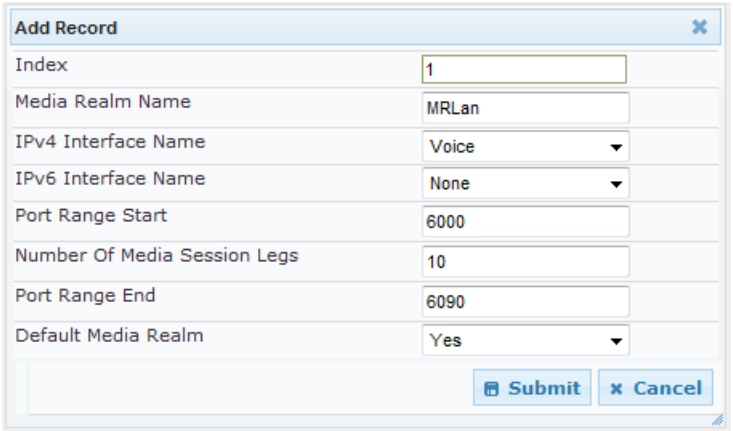
The simplest configuration is to create one Media Realm for internal (LAN) traffic and another for external (WAN) traffic, which is described in the procedure below for our example scenario.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** > **VoIP** > **Media** > **Media Realm Configuration**).
2. Add a Media Realm for the LAN traffic:
   a. Click **Add**.
   b. Configure the Media Realm as follows:

Parameter	Setting
Index	"1"
Media Realm Name	Enter an arbitrary name (e.g., "MRLan")
IPv4 Interface Name	Select the interface name (e.g., **Voice**)
Port Range Start	Enter a number that represents the lowest UDP port number that will be used for media on the LAN (e.g., "6000")
Number of Media Session Legs	Enter the number of media sessions that are assigned with the port range (e.g., "10")

Figure 4-5: LAN Media Realm Configuration

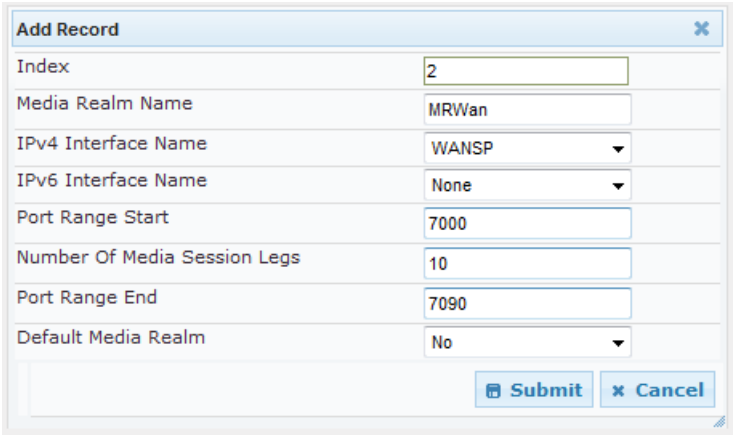


   c. Click **Submit**.

3. Add a Media Realm for the external traffic (WAN):
   a. Click **Add**.
   b. Configure the Media Realm as follows:

Parameter	Setting
Index	Enter "2"
Media Realm Name	Enter an arbitrary name (e.g., "MRWan")
IPv4 Interface Name	Select the interface name (e.g., **WANSP**)
Port Range Start	Enter a number that represents the lowest UDP port number that will be used for media on the WAN (e.g., "7000")
Number of Media Session Legs	Enter the number of media sessions that are assigned with the port range (e.g., "10")

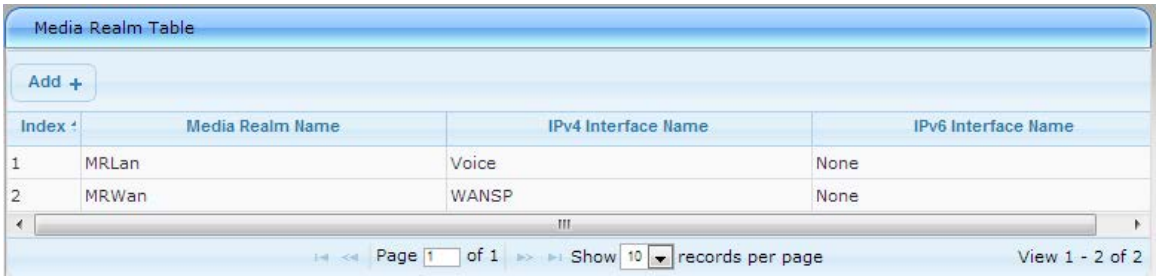
Figure 4-6: WAN Media Realm Configuration



   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-7: Required Media Realm Table



4.3.2 Configuring SRDs

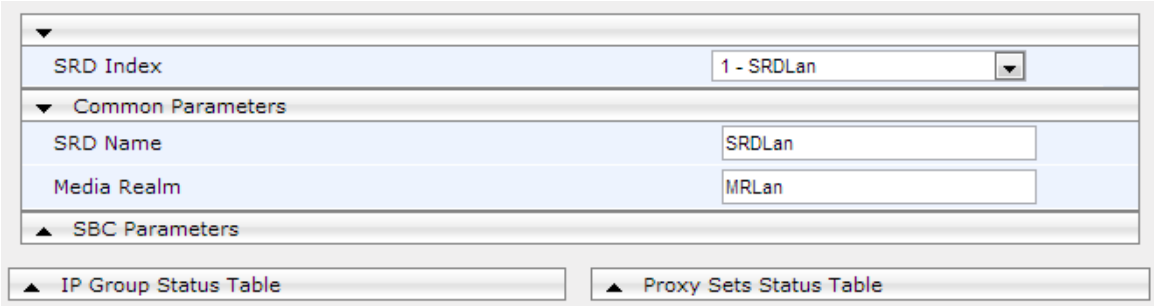
The procedure below describes how to configure the SRDs. You configure two SRDs; one for the LAN and another for the WAN.

➢ **To configure SRDs:**

1. Open the SRD Table page (**Configuration** > **VoIP** > **Control Network** > **SRD Table**).
2. Add an SRD for the E-SBC's internal interface (towards the Lync Server 2010):
   a. Configure the following parameters:

Parameter	Setting
SRD Index	**1**
SRD Name	Descriptive name for the SRD (e.g., "SRDLan")
Media Realm	Associates the SRD with a Media Realm (e.g., "MRLan")

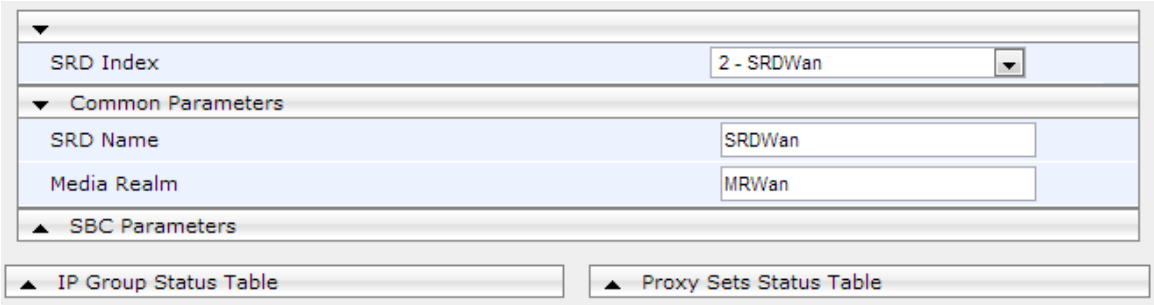
Figure 4-8: LAN SRD Configuration



   b. Click **Submit**.
3. Add an SRD for the E-SBC's external interface (toward the QSC AG SIP Trunk):
   a. Configure the following parameters:

Parameter	Setting
SRD Index	**2**
SRD Name	Descriptive name for the SRD (e.g., "SRDWan")
Media Realm	Associates the SRD with a Media Realm (e.g., "MRWan")

Figure 4-9: WAN SRD Configuration



   b. Click **Submit**.

4.3.3 Configuring SIP Signaling Interfaces

A SIP Interface consists of a combination of ports (UDP, TCP, and TLS) associated with a specific IP network interface. The SIP Interface is associated with an SRD.

The procedure below describes how to add SIP interfaces. In our example scenario, you need to add an internal and external SIP interface for the E-SBC.

➢ **To add SIP interfaces:**

1. Open the SIP Interface Table page (**Configuration** > **VoIP** > **Control Network** > **SIP Interface Table**).
2. Add a SIP interface for the LAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Setting
Index	"1"
Network Interface	"Voice"
Application Type	**SBC**
TLS Port	"5067"
TCP and UDP	"0"
SRD	"1"

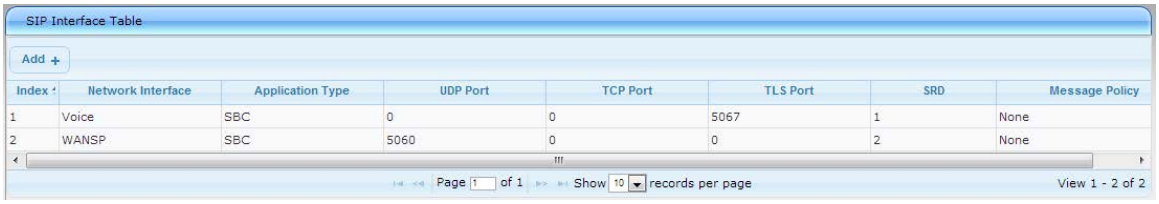
   c. Click **Submit**.
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Setting
Index	"2"
Network Interface	"WANSP"
Application Type	**SBC**
UDP Port	"5060"
TCP and TLS	"0"
SRD	"2"

   c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-10: Required SIP Interface Table



4.4 Step 4: Configure Proxy Sets

This step describes how to configure the Proxy Sets. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). In the example scenario, you need to configure two Proxy Sets for the following entities:

- Microsoft Lync Server 2010
- QSC AG SIP Trunk

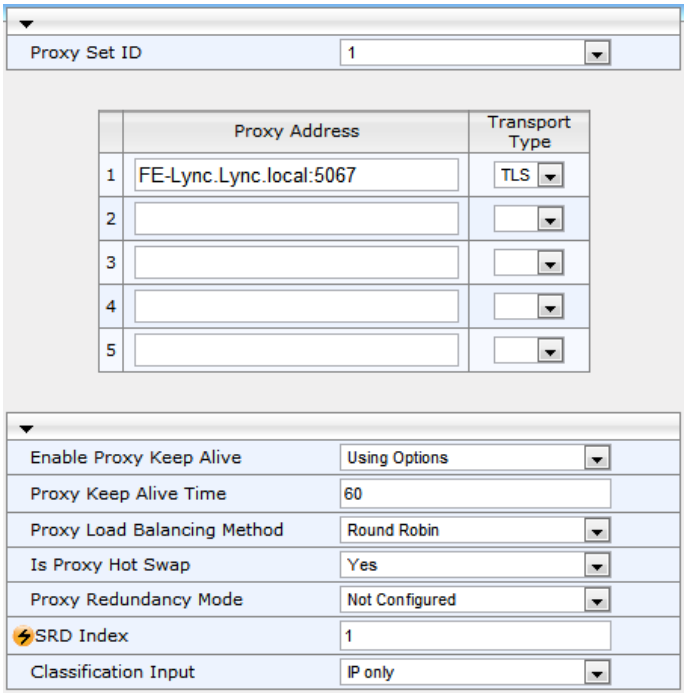
These Proxy Sets will later be associated with IP Groups.

➢ **To add Proxy Sets:**

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

Parameter	Setting
Proxy Set ID	**1**
Proxy Address	Enter the Lync Server 2010 SIP Trunking IP address or FQDN and destination port (e.g., "FE-Lync.Lync.local:5067")
Transport Type	**TLS**
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
SRD Index	"1"

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

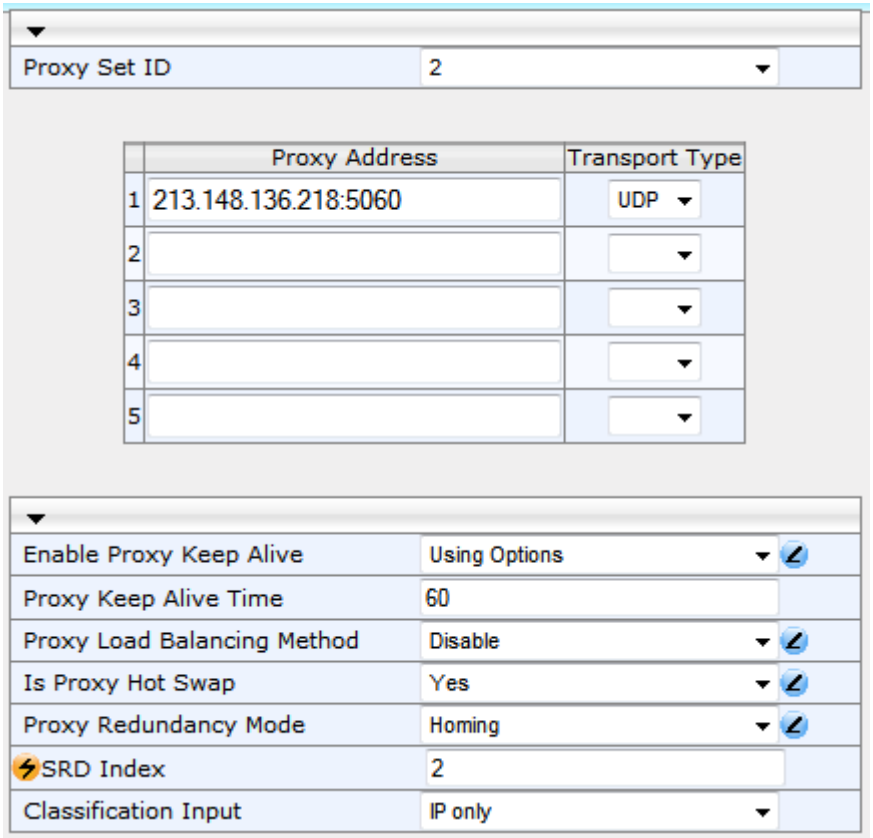


   b. Click **Submit**.

3. Add a Proxy Set for the QSC AG SIP Trunk:

Parameter	Setting
Proxy Set ID	**2**
Proxy Address	QSC AG IP address or FQDN and destination port (e.g., "213.148.136.218:5060")
Transport Type	**UDP**
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	"2" (enables classification by Proxy Set for this SRD in the IP Group belonging to the QSC AG SIP Trunk)

Figure 4-12: Proxy Set for QSC AG SIP Trunk



c. Click **Submit**.

4.5 Step 5: Configure IP Groups

This step describes how to create IP Groups. An IP Group represents a SIP entity behavior in the E-SBC's network. In our example scenario, you need to create IP Groups for the following entities:

- Lync Server 2010 (Mediation Server) on the LAN
- QSC AG SIP Trunk for number range A: **024639749900** to **024639749909**
- QSC AG SIP Trunk for number range B: **024639749910** to **024639749919**

Note: Each IP Group that you define for the QSC AG SIP trunk represents a range of 10 QSC AG client extensions as defined in the Accounts table (see Section 4.10 on page 55).

These IP Groups are later used by the SBC application for routing calls.

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group for the Lync Server 2010 Mediation Server:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"1"
Type	**Server**
Description	Enter descriptive name (e.g., "Lync Server")
Proxy Set ID	"1"
SIP Group Name	"Lync Server"
SRD	"1"
Media Realm Name	"MRLan"
IP Profile ID	"1"

3. Click **Submit**.

4. Add an IP Group for the QSC AG SIP Trunk for number range A (024639749900 to 024639749909):
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"2"
Type	**Server**
Description	Enter descriptive name (e.g., "QSC - 02463974990")
Proxy Set ID	"2"
SIP Group Name	"sip.qsc.de"
SRD	"2"
Media Realm Name	"MRWan"
IP Profile ID	"2"

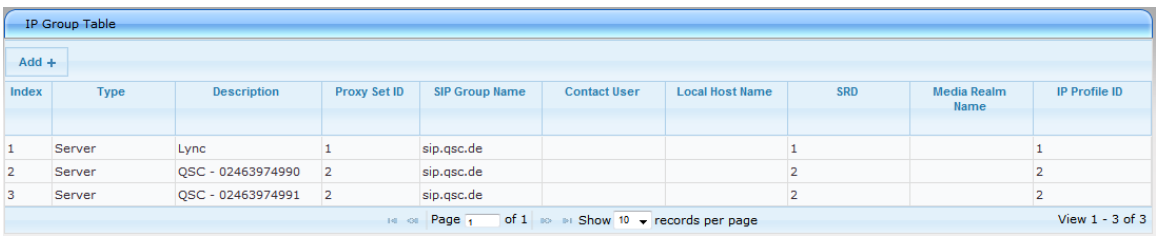
   c. Click **Submit**.
5. Add another IP Group for the QSC AG SIP Trunk for number range B (024639749910 to 024639749919):
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"3"
Type	**Server**
Description	Enter descriptive name (e.g., "QSC - 02463974991")
Proxy Set ID	"2"
SIP Group Name	"sip.qsc.de"
SRD	"2"
Media Realm Name	"MRWan"
IP Profile ID	"2"

   c. Click **Submit**.

The configured IP Group table is shown below:

Figure 4-13: Configured IP Group Table



4.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. In our example scenario, the IP Profiles are used to configure the SRTP / TLS modes and other parameters that differ between the two entities - Lync Server 2010 and QSC AG SIP Trunk. Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.5 on page 43).

In our example, you need to add an IP Profile for each entity:

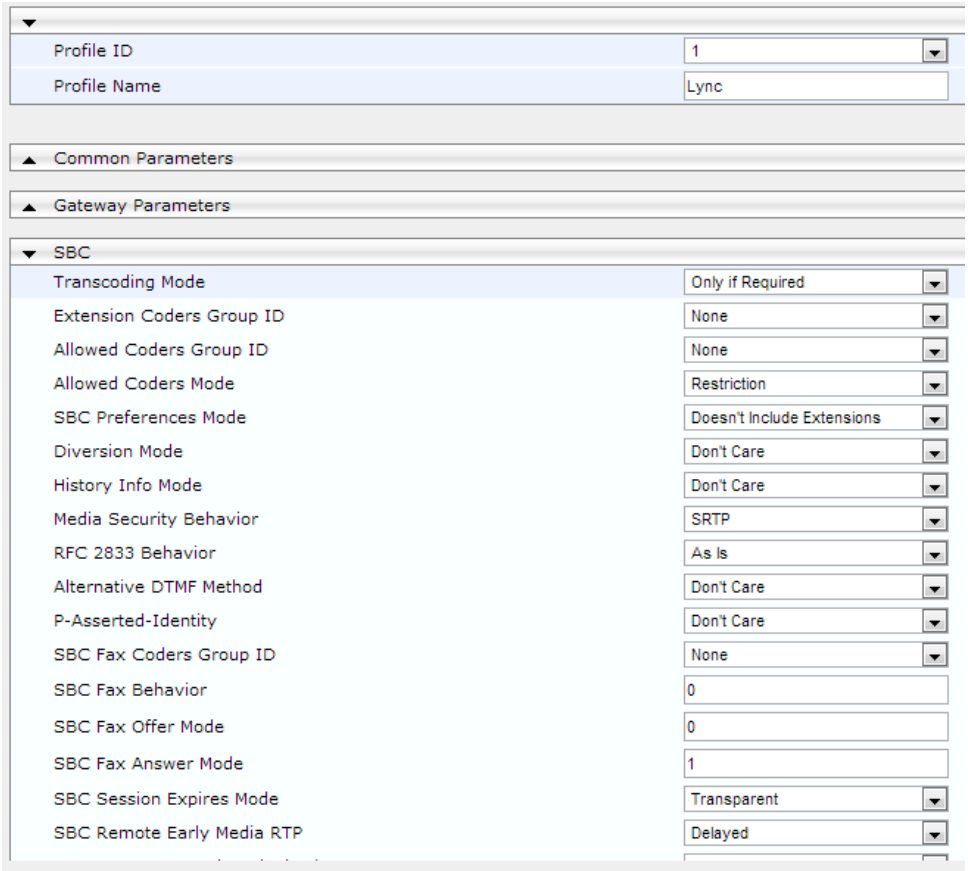
- Microsoft Lync Server 2010 - to operate in secure mode using SRTP and TLS
- QSC AG SIP trunk - to operate in non-secure mode using RTP and UDP

➢ **To add IP Profiles:**

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

Parameter	Setting
Profile ID	**1**
Media Security Behavior	**SRTP**
SBC Remote Early Media RTP	**Delayed** (required, as when Lync Server 2010 sends a SIP 18x response, it does not send RTP immediately to the remote side).

Figure 4-14: IP Profile for Lync Server 2010

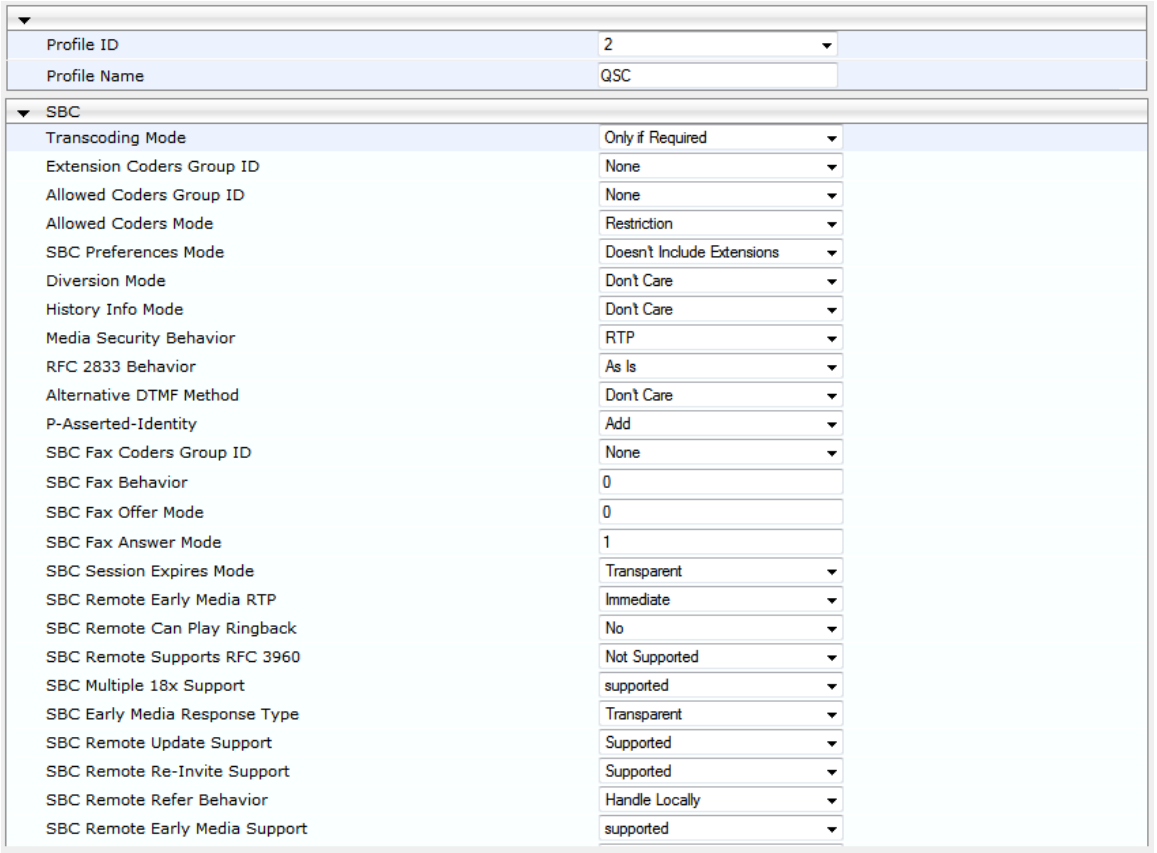


   b. Click **Submit**.

3. Add an IP Profile for the QSC AG SIP Trunk:
   a. Configure the parameters as follows:

Parameter	Setting
Profile ID	**2**
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** (required for anonymous calls)
SBC Remote Can Play Ringback	**No** (required, as Lync Server 2010 does not provide a Ringback tone for incoming calls)
SBC Remote Refer Behavior	**Handle Locally** (E-SBC handles the incoming REFER request itself without forwarding the REFER towards the SIP Trunk)

Figure 4-15: IP Profile for QSC AG SIP Trunk



   b. Click **Submit**.

4.7 Step 7: SIP TLS Connection

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

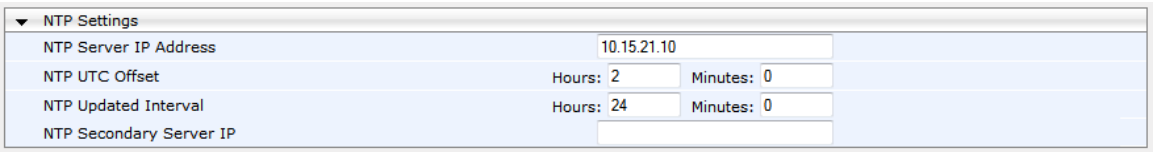
4.7.1 Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or third-party server) to ensure that the E-SBC receives 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** > **System** > **Application Settings**).
2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., "10.15.21.10").

Figure 4-16: Configuring NTP Server Address



3. Click **Submit**.

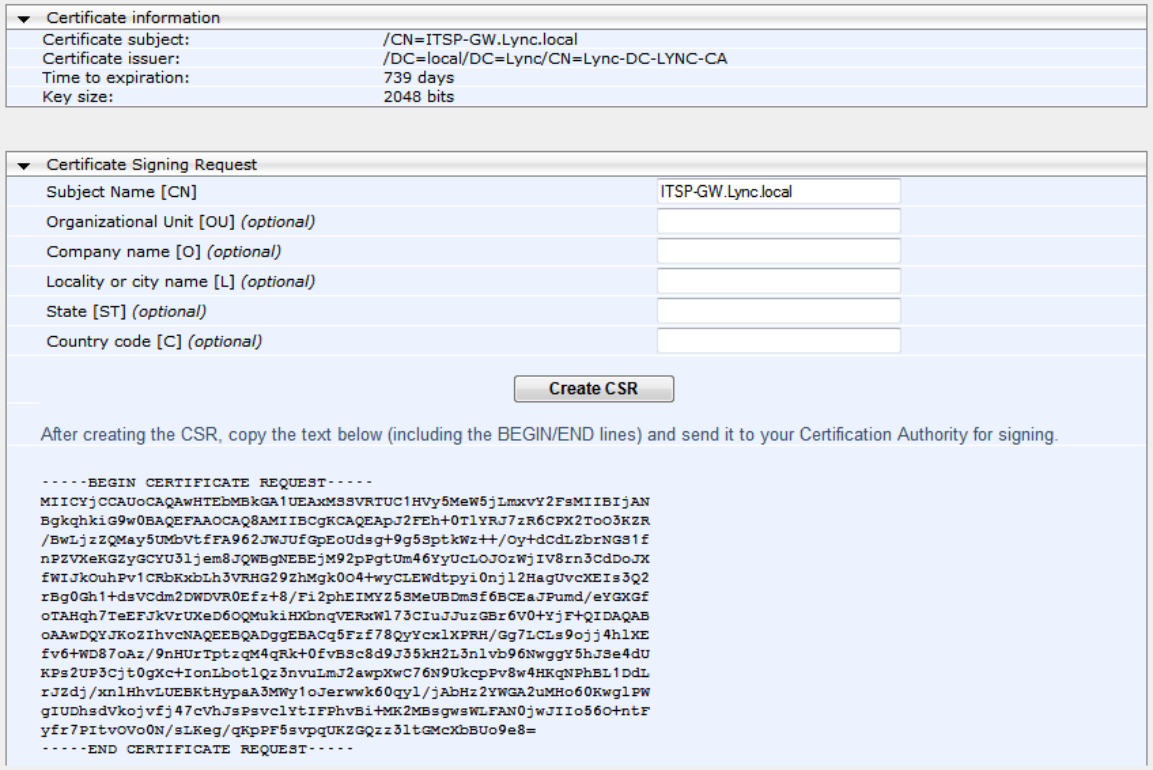
4.7.2 Configure a Certificate

This step describes how to exchange a certificate with the Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with the management station (i.e., the computer used to manage the E-SBC through its embedded Web server).

➢ **To configure a certificate:**

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

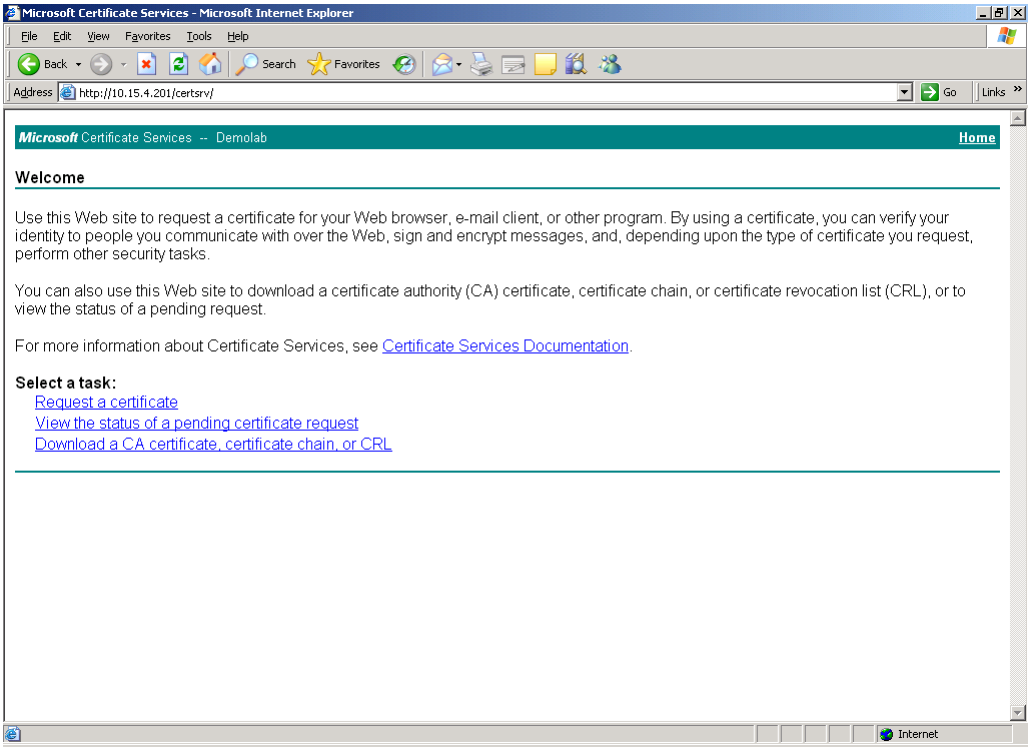
Figure 4-17: Certificates Page - Creating CSR



2. In the Subject Name field, enter the media gateway name (e.g., "ITSP-GW.Lync.local"). This name must be equivalent to the gateway name configured in the Topology Builder for Lync Server 2010 (see Section 3.1 on page 15).
3. Click **Create CSR**; a certificate request is generated.
4. Copy the CSR (from the line "----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----") to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.

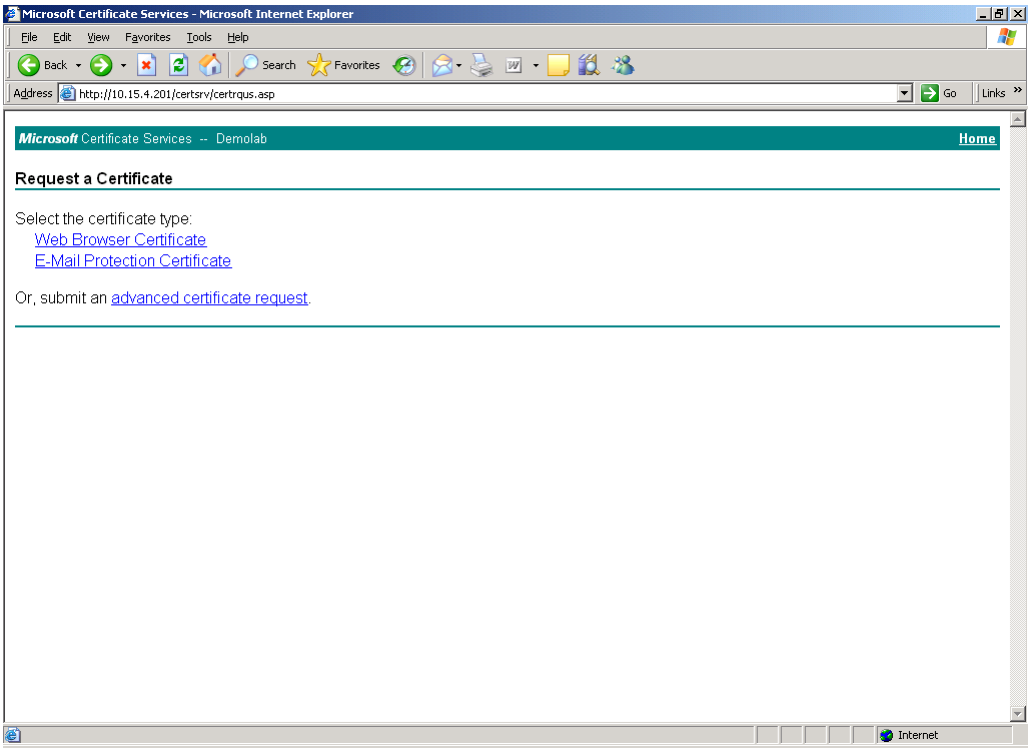
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-18: Microsoft Certificate Services Web Page



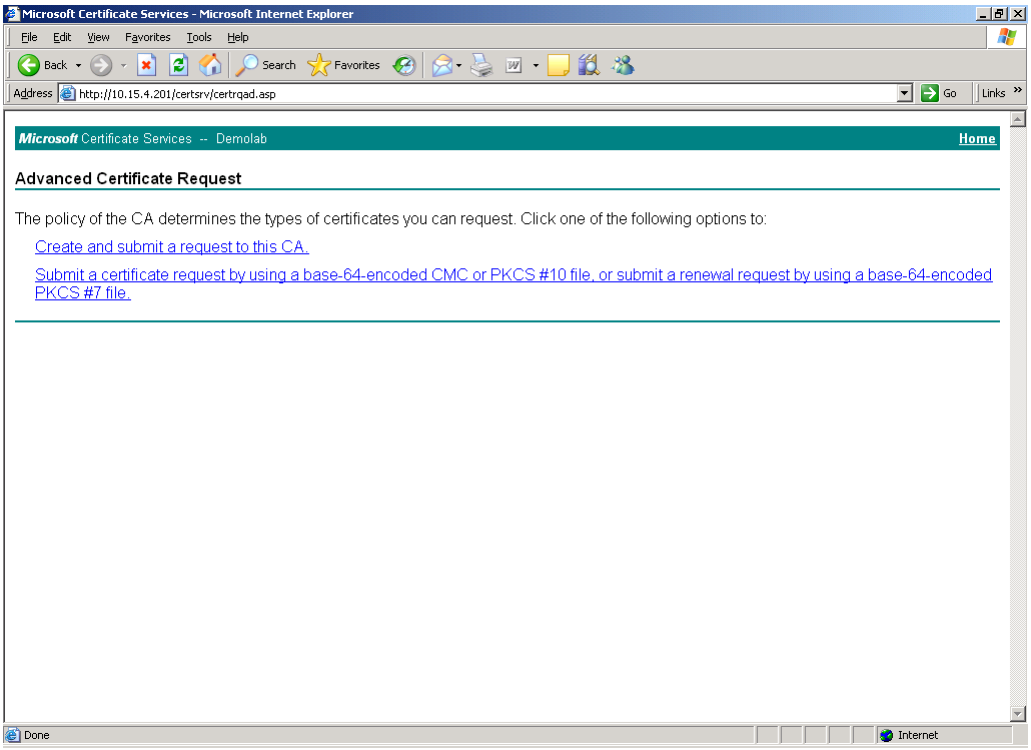
6. Click **Request a certificate**.

Figure 4-19: Request a Certificate Page



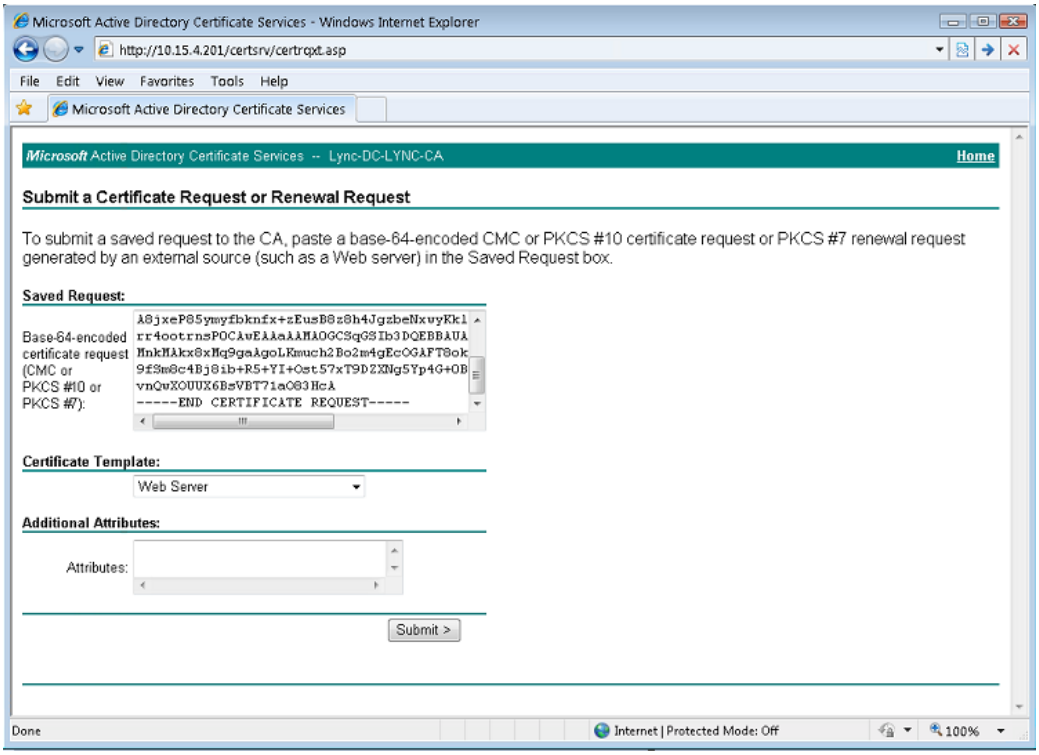
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-20: Advanced Certificate Request Page



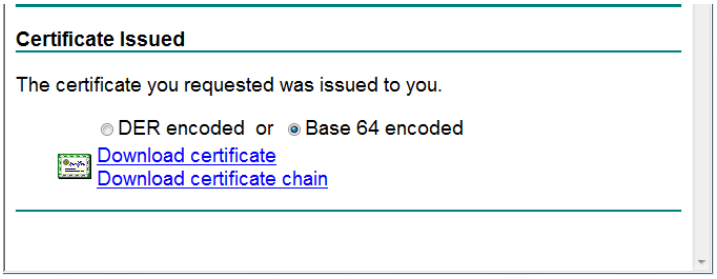
8. Click **Submit a certificate request ...**, and then click **Next**.

Figure 4-21: Submit a Certificate Request or Renewal Request Page



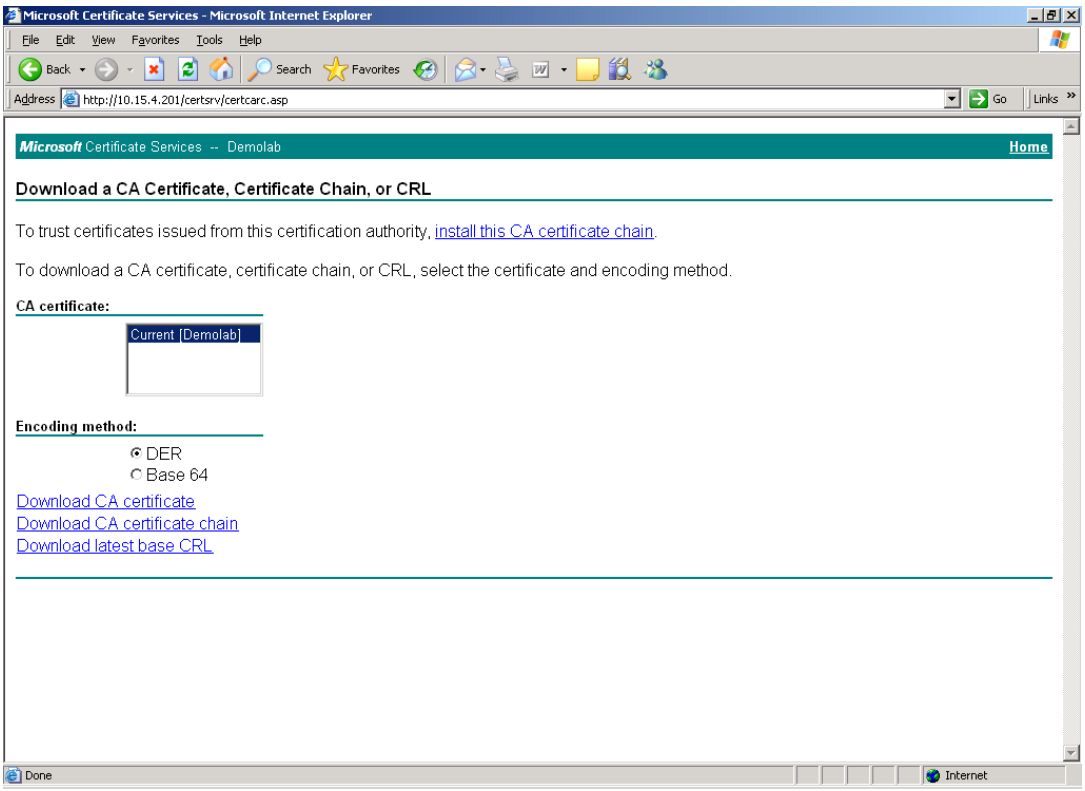
9. Open the *certreq.txt* file that you created and saved in Step 4, and then copy its contents to the 'Base64 Encoded Certificate Request' field.
10. From the 'Certificate Template' drop-down list, select **Web Server**.
11. Click **Submit**.

Figure 4-22: Certificate Issued Page



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

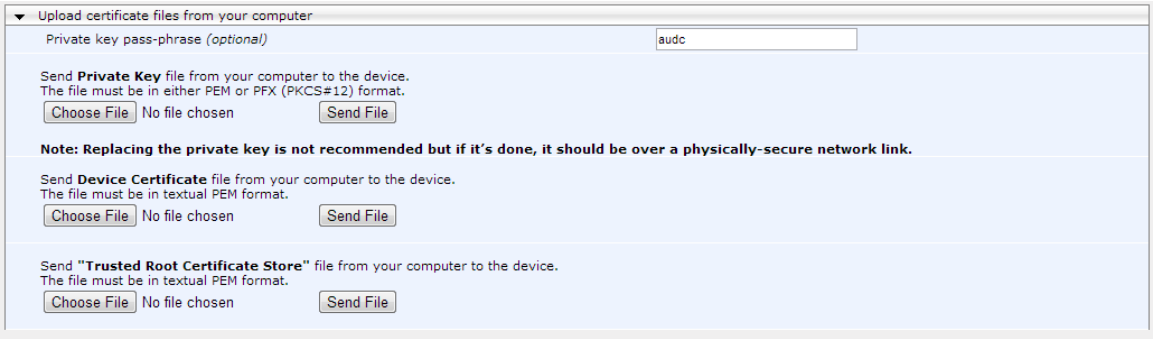
Figure 4-23: Download a CA Certificate, Certificate Chain, or CRL Page



16. Under the 'Encoding method' group, select the **Base 64** option for encoding.
17. Click **Download CA certificate**.

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

Figure 4-24: Certificates Page (Uploading Certificate)



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

4.8 Step 8: Configure SRTP

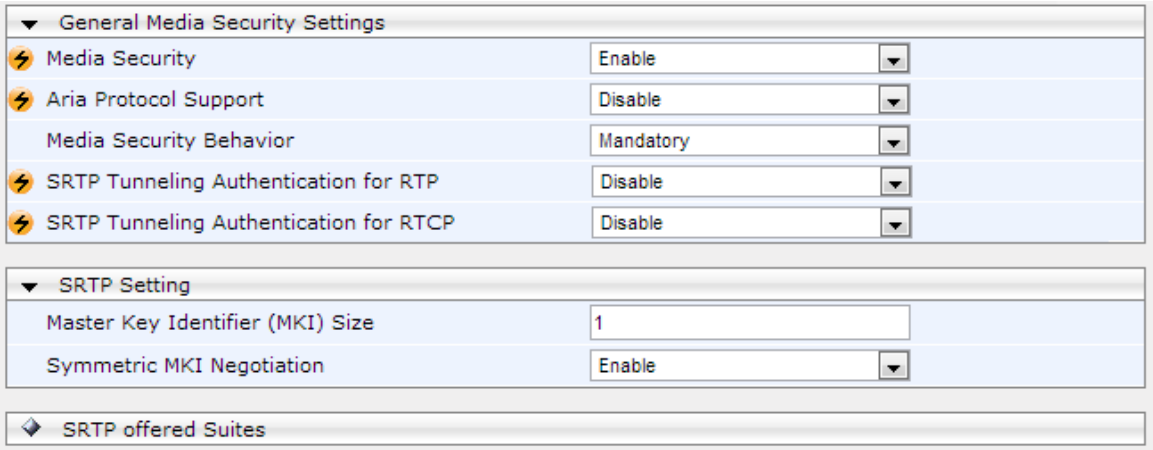
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), you need to configure the E-SBC to operate in the same manner.

Note: SRTP was enabled for Lync Server 2010 when you added an IP Profile for Lync Server 2010 (see Section 4.6 on page 45).

➢ **To configure media security:**

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

Figure 4-25: Media Security Page



2. Configure the parameters as follows:

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

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

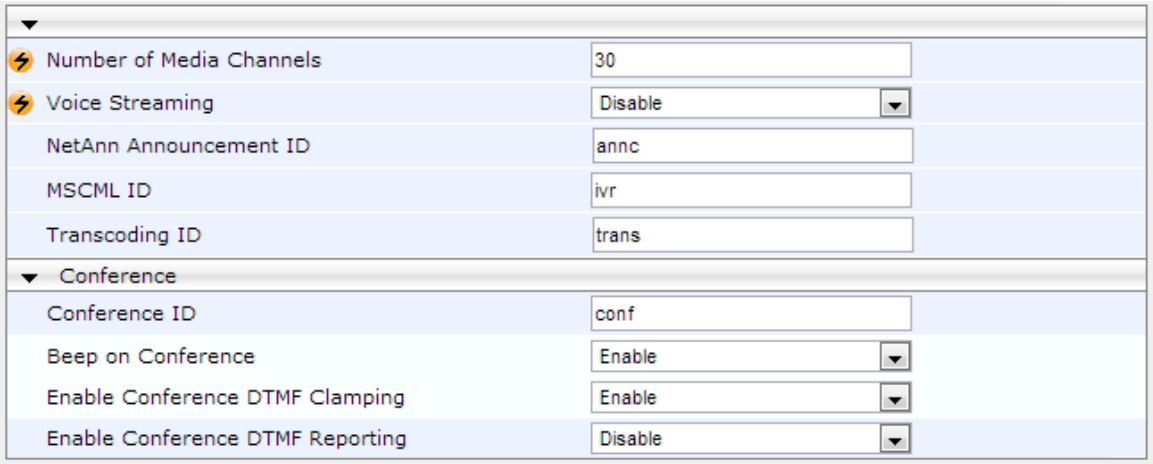
4.9 Step 9: Configure IP Media

This step describes how to configure the number of media channels for IP-based media. To perform coder transcoding, define digital signaling processors (DSP) channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to sessions.

➢ **To configure IP media:**

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

Figure 4-26: IP Media Settings



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environment transcoding (e.g., “30”)
3. Click **Submit**.

4.10 Step 10: Configure Account Table

This step describes how to configure SIP registration accounts (in the Account table). This is required so that the E-SBC can register with the QSC AG SIP Trunk on behalf of Lync Server 2010. Additionally, when the route is made and the QSC AG SIP Trunk challenges the INVITE (401/407 SIP message), the correct credentials (username and password) are chosen according to the Serving IP Group number (i.e., 2 or 3) in the account row.

The QSC AG SIP Trunk requires registration and authentication to provide service.

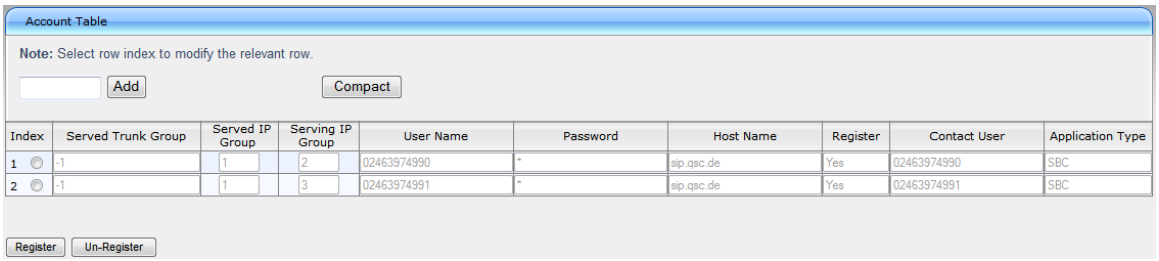
It registers every 10 client extensions in a separate user entry as shown in the table below. Each entry represents a QSC IP Group as defined in Section 4.5 on page 43.

In this example, there are 2 rows representing 20 client extensions.

➢ **To configure a registration account:**

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

Figure 4-27: Configuring SIP Registration Account



2. Enter an index number, and then click **Add**.
3. Configure the account according to the provided information from QSC AG, for example:

Parameter	Setting
Served IP Group	"1" (i.e., Lync Server 2010)
Serving IP Group	"2" and "3" (i.e., QSC AG SIP Trunk)
Username	Set username as provided by QSC AG
Password	Set password as provided by QSC AG
Host Name	"sip.qsc.de"
Register	**Yes**
Contact User	Set to trunk main line (e.g., "02463974990" and “02463974991”)
Application Type	**SBC**

4. Click **Apply**.

4.11 Step 11: Configure Conditions Rules

This step describes how to configure conditions rules (which are configured in the Condition table). Condition rules allow you to enhance the process of classifying an incoming SIP dialog to an IP Group by using SIP message rules. In this configuration, condition rules are assigned to the IP-to-IP Routing table (see Section 4.12 on page 58). When an IP-to-IP rule is associated with a Condition rule, the route is used only if the route rule and its associated Condition rule are matched.

In our example scenario, a condition rule is added for call transfer/forwarding for each of the following QSC AG range of numbers:

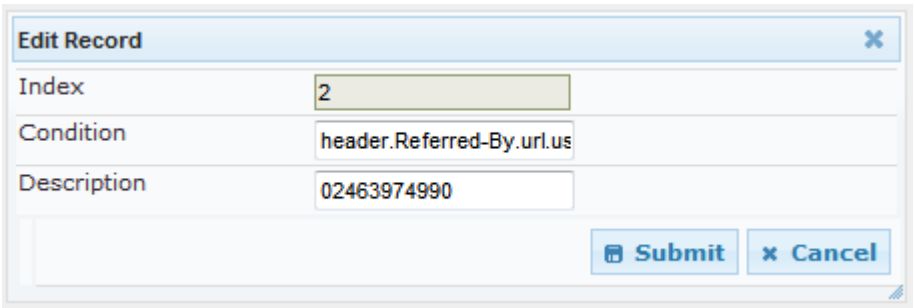
- Referred-By rule for number range A: **024639749900-024639749909**
- Referred-By rule for number range B: **024639749910-024639749919**

➢ **To add Condition rules:**

1. Open the Condition Table page (**Configuration** > **VoIP** > **SBC** > **Routing SBC** > **Condition Table**).
2. Add rule to match Referred-By header with number that contains 2463974990:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"2"
Condition	**header.Referred-By.url.user contains '2463974990'**
Description	"2463974990"

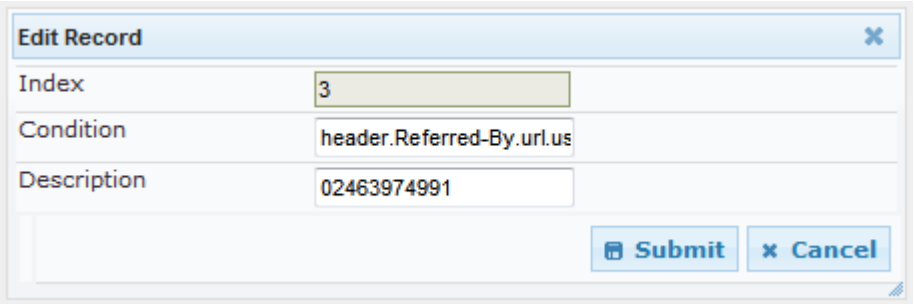
Figure 4-28: Condition Rule for Number Range A



3. Add a rule to match the Referred-By header with a number that contains 2463974991:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"3"
Condition	**header.Referred-By.url.user contains '2463974991'**
Description	"2463974991"

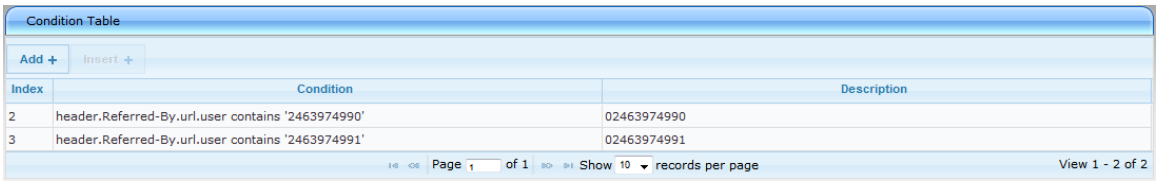
Figure 4-29: Condition Rule for number Range B



c. Click **Submit**.

The figure below shows the above configured routing rules in the Condition Table:

Figure 4-30: Condition Table



4.12 Step 12: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules (which is performed in the IP-to-IP Routing table). These rules define the route for forwarding SIP messages (e.g., INVITE) received on one IP interface to another.

The SIP message is routed according to a rule whose configured input characteristics (e.g., Source IP Group) match those of the message. If the characteristics of an incoming message do not match the first rule in the table, they are then compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

In our example scenario, you need to add the following IP-to-IP routing rules to route calls between Lync Server 2010 (LAN) and QSC AG SIP Trunk (WAN) range of numbers:

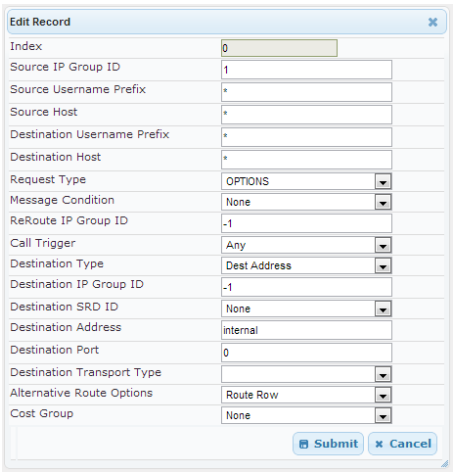
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from LAN with specific number range to WAN
- Calls from LAN with specific number range to WAN in case of Transfer/Forward
- Calls from WAN to LAN.

The routing rules use IP Groups to denote the source and destination of the call. These IP Groups were configured in Step 5 (see Section 4.5 on page 43); IP Group ID 1 was assigned to Lync Server 2010, and IP Group ID 2 and 3 to the QSC AG SIP Trunk.

➢ **To add IP-to-IP routing rules:**

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

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



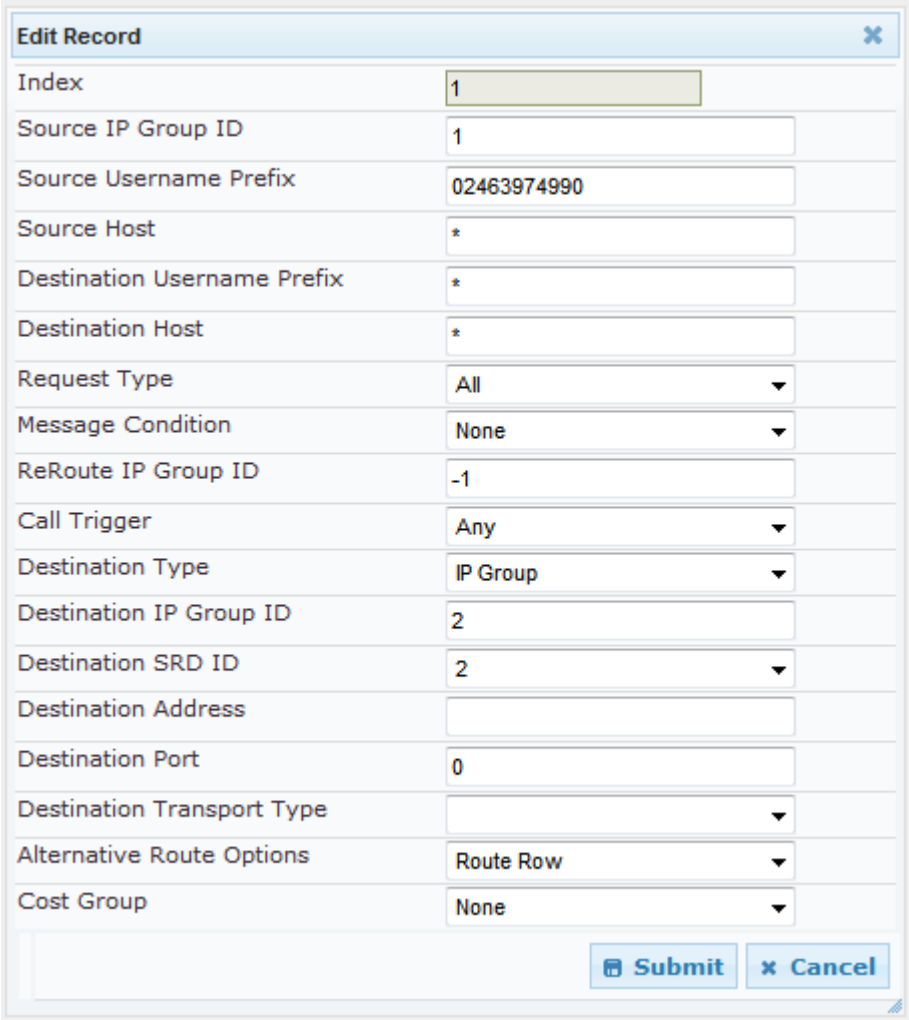
3. Add a rule to route calls from LAN with number range A (024639749900 to 024639749909) to WAN:

   a. Click **Add**.

   b. Configure the parameters as follows:

Parameter	Setting
Index	"1"
Source IP Group ID	"1"
Source Username Prefix	"02463974990"
Destination Type	**IP Group**
Destination IP Group ID	"2" Note: The destination IP Group is configured in the Account table in case of an authentication challenge.
Destination SRD ID	**2**

Figure 4-31: IP-to-IP Routing Rule for LAN Range A to WAN

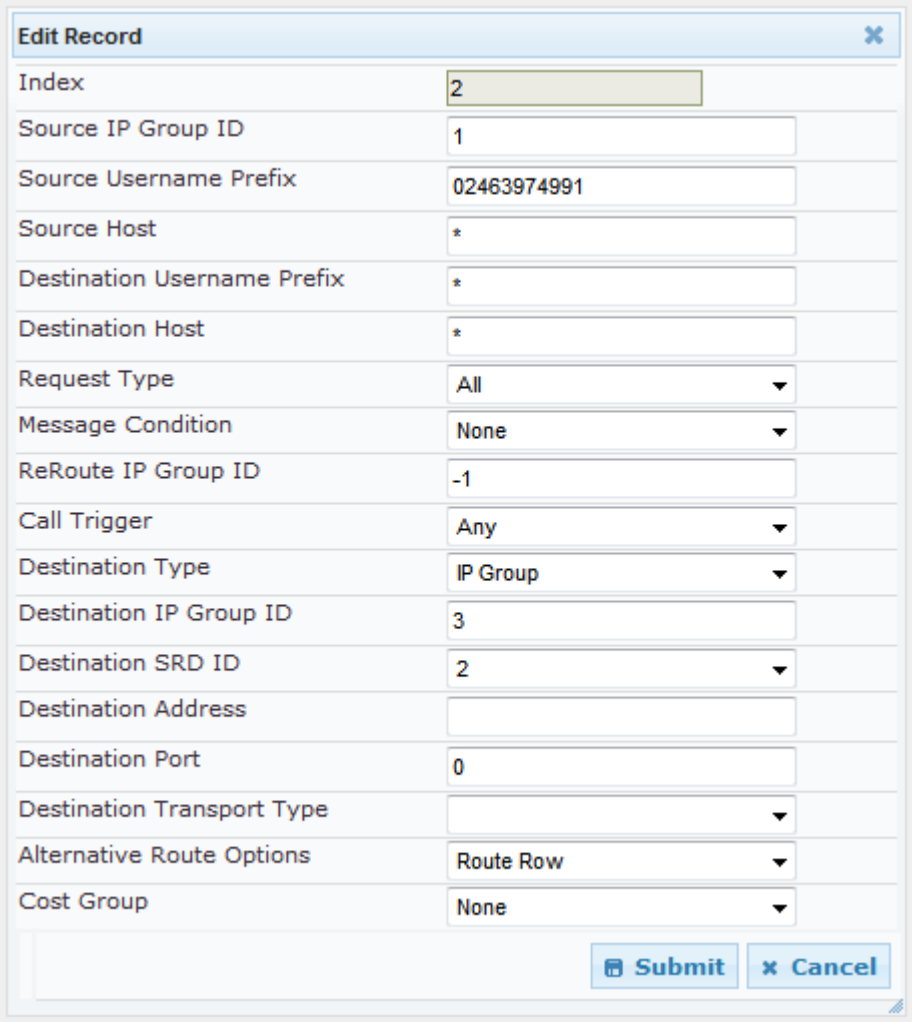


   c. Click **Submit**.

4. Add a rule to route calls from LAN with number range B (024639749910 to 024639749919) to WAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"2"
Source IP Group ID	"1"
Source Username Prefix	"02463974991"
Destination Type	**IP Group**
Destination IP Group ID	"3" Note: The destined IP Group is configured in the account table in case of an authentication challenge.
Destination SRD ID	**2**

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

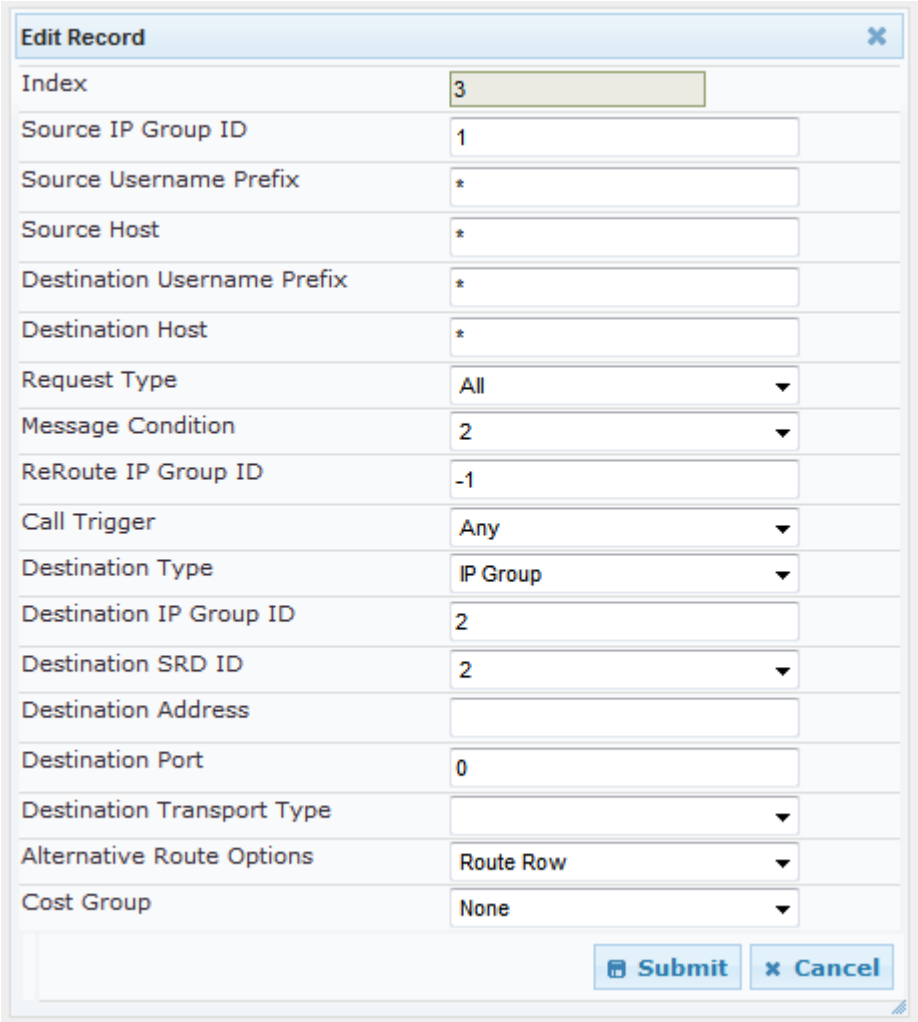


   c. Click **Submit**.

5. Add a rule to route calls from LAN with number range A to WAN in case of a matched Condition:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"3"
Source IP Group ID	"1"
Message Condition	**2** Note: Uses this routing rule if Condition rule **2** is matched. See Section 4.11 on page 56.
Destination Type	**IP Group**
Destination IP Group ID	"2"
Destination SRD ID	**2**

Figure 4-33: IP-to-IP Routing Rule for LAN Range A to WAN (Condition)

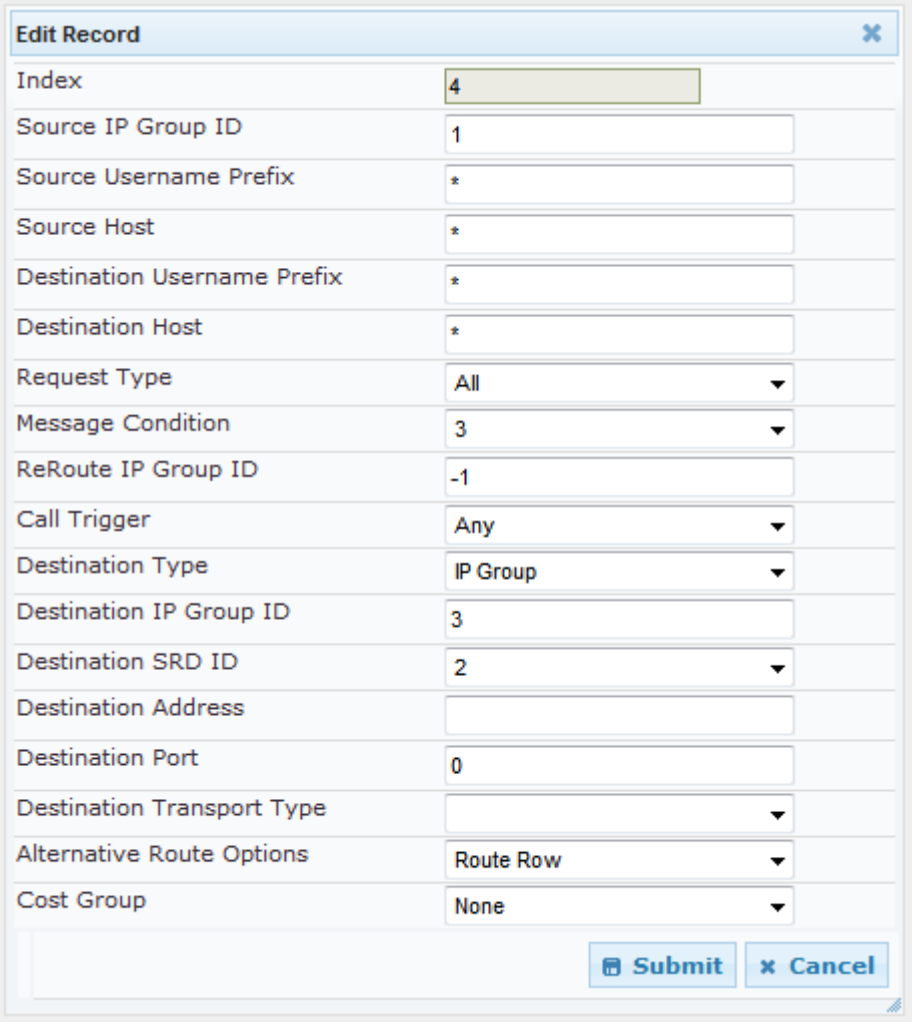


   c. Click **Submit**.

6. Add a rule to route calls from LAN with a number range B to WAN in case of a matched Condition:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"4"
Source IP Group ID	"1"
Message Condition	**3** Note: Uses this routing rule if Condition rule **3** is matched. See Section 4.11 on page 56.
Destination Type	**IP Group**
Destination IP Group ID	"3"
Destination SRD ID	**2**

Figure 4-34: IP-to-IP Routing Rule for LAN Range B to WAN (Condition)

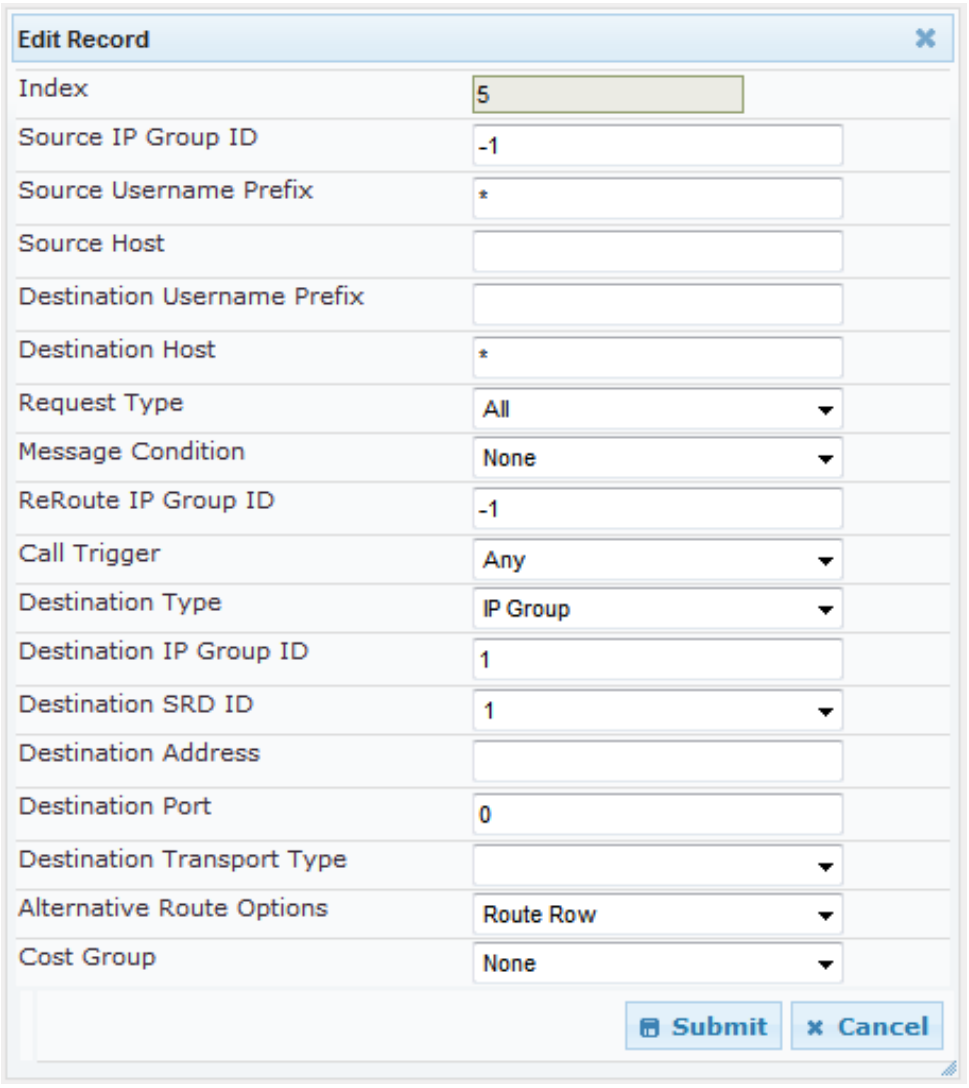


   c. Click **Submit**.

7. Add a rule to route calls from WAN to LAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Setting
Index	"5"
Source IP Group ID	"-1"
Destination Type	**IP Group**
Destination IP Group ID	"1"
Destination SRD ID	**1**

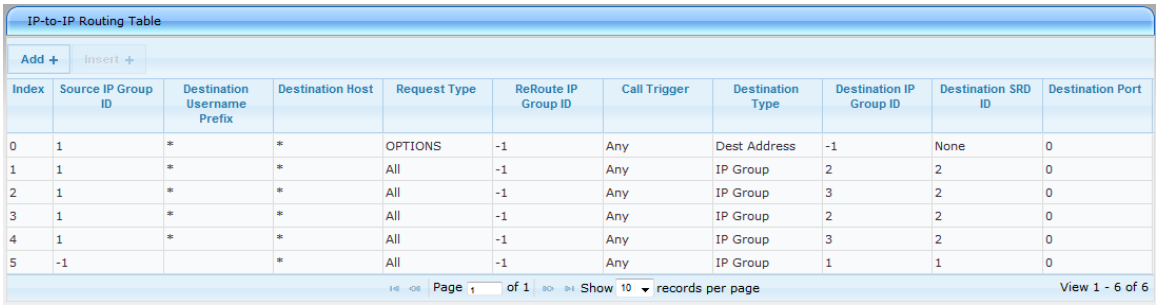
Figure 4-35: IP-to-IP Routing Rule for WAN to LAN



   c. Click **Submit**.

The figure below shows the above configured routing rules in the IP-to-IP Routing Table:

Figure 4-36: IP-to-IP Routing Table



IP-to-IP Routing Table

Add + | Insert +

Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	ReRoute IP Group ID	Call Trigger	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Port
0	1	*	*	OPTIONS	-1	Any	Dest Address	-1	None	0
1	1	*	*	All	-1	Any	IP Group	2	2	0
2	1	*	*	All	-1	Any	IP Group	3	2	0
3	1	*	*	All	-1	Any	IP Group	2	2	0
4	1	*	*	All	-1	Any	IP Group	3	2	0
5	-1		*	All	-1	Any	IP Group	1	1	0

Page 1 of 1 Show 10 records per page View 1 - 6 of 6

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

4.13 Step 13: Configure IP-to-IP Manipulation

This step describes how to configure IP-to-IP manipulation rules. These rules concern number manipulation of the source and / or destination number. The manipulation rules use IP Groups to denote the source and destination of the call. The IP Groups were configured in Step 5 (see Section 4.5 on page 43); IP Group ID 1 was assigned to Lync Server 2010 and IP Group ID 2 and 3 to the QSC AG SIP Trunk.

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

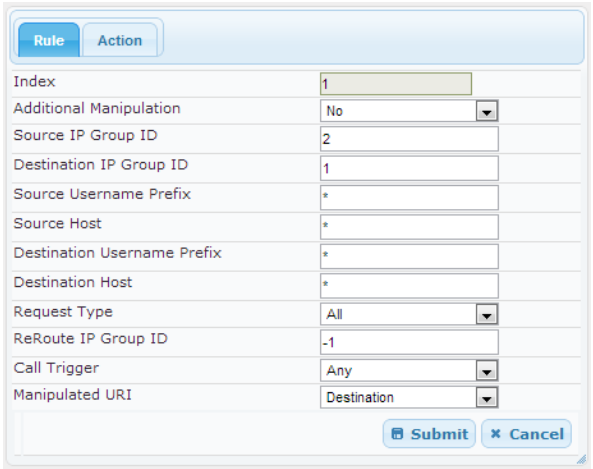
The procedure below provides an example of configuring a manipulation rule that adds the plus sign "+" to the destination number for calls from IP Group 2 (QSC AG SIP Trunk) destined to IP Group 1 (i.e., Lync Server 2010), when the destination number prefix is any number ("*").

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

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

Parameter	Setting
Index	"1"
Source IP Group	"2"
Destination IP Group	"1"
Destination Username Prefix	"*"
Manipulated URI	**Destination**

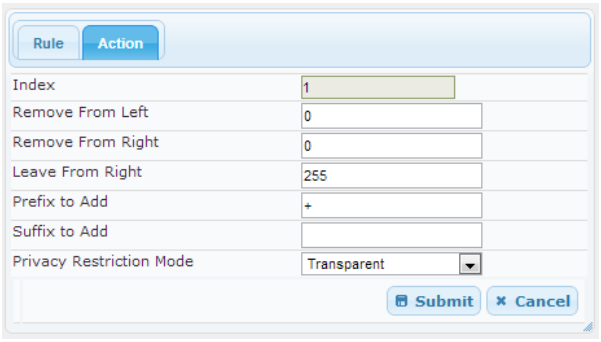
Figure 4-37: IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Setting
Prefix to Add	"+"

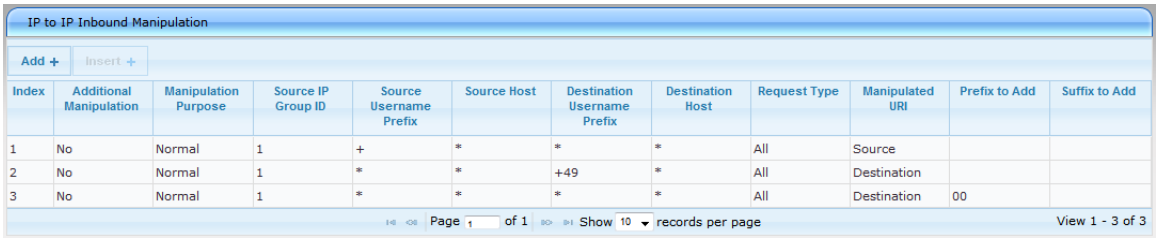
Figure 4-38: IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

The IP-to-IP Inbound table displayed below includes manipulation rules for calls from IP Group 1 (i.e., Lync Server 2010):

Figure 4-39: IP-to-IP Inbound Manipulation Table - Example



Rule Index	Description
1	Calls received from IP Group 1 with source number prefix of "+", remove the "+" from this prefix source number.
2	Calls received from IP Group 1 that have a prefix destination number of "+49", remove "+" from this prefix.
3	Calls received from IP Group 1 with destination number other than prefix "+49", remove the "+" from the prefix and add "00" as the prefix to the destination number.

4.14 Step 14: Configure Message Manipulation Rules

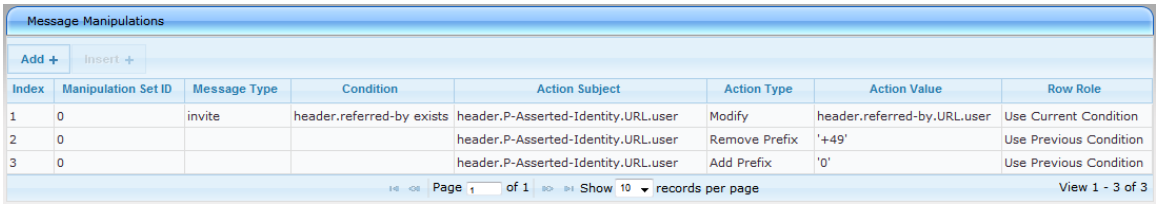
This step describes how to configure SIP message manipulation rules (done in the Message Manipulations table). SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message. Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

In our example scenario, SIP message manipulation is performed for messages sent to the QSC AG SIP Trunk (IP Group 2) in the Call Transfer / Forward scenario from Lync Server 2010.

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

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).

Figure 4-40: SIP Message Manipulation

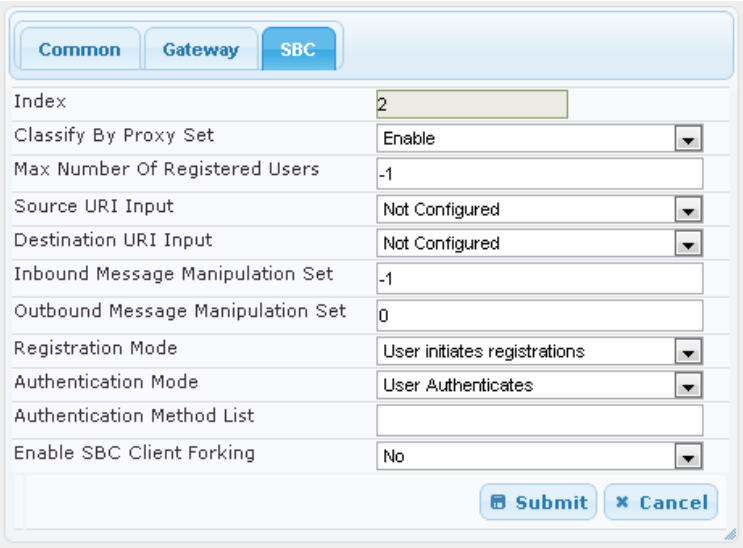


2. Add the following manipulation rules for Manipulation Set ID 0:

Rule Index	Description
1	SIP INVITE messages that contain a Referred-By header and are destined to the QSC AG SIP Trunk are modified as follows: the user part in the P-Asserted header is replaced with the user part in the Referred-By header.
2	If the manipulation rule Index 1 (above) is executed, then the following rule is also done on the same SIP message: the prefix "+49" is removed from the user part of the P-Asserted header.
3	If the manipulation rule Index 1 (above) is executed, then the following rule is also done on the same SIP message: the prefix "0" is added from the user part of the P-Asserted header.

3. Assign the Manipulation Set ID 0 to IP Group 2:
   a. Open the IP Group Table page (**Configuration** > **VoIP** > **Control Network** > **IP Group Table**).
   b. Select the row of IP Group 2, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Outbound Message Manipulation Set' field to "0".

Figure 4-41: Assigning Manipulation Rule to IP Group 2



   e. Click **Submit**.

4.15 Step 15: Miscellaneous Configuration

This step describes miscellaneous E-SBC configuration.

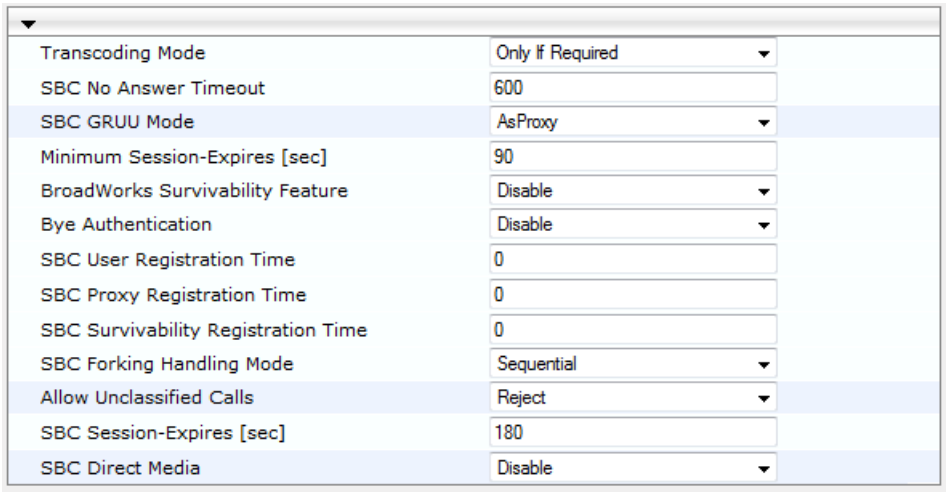
4.15.1 Configure Forking Mode

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

➢ **To configure call forking:**

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

Figure 4-42: Configuring Forking Mode



3. Click **Submit**.

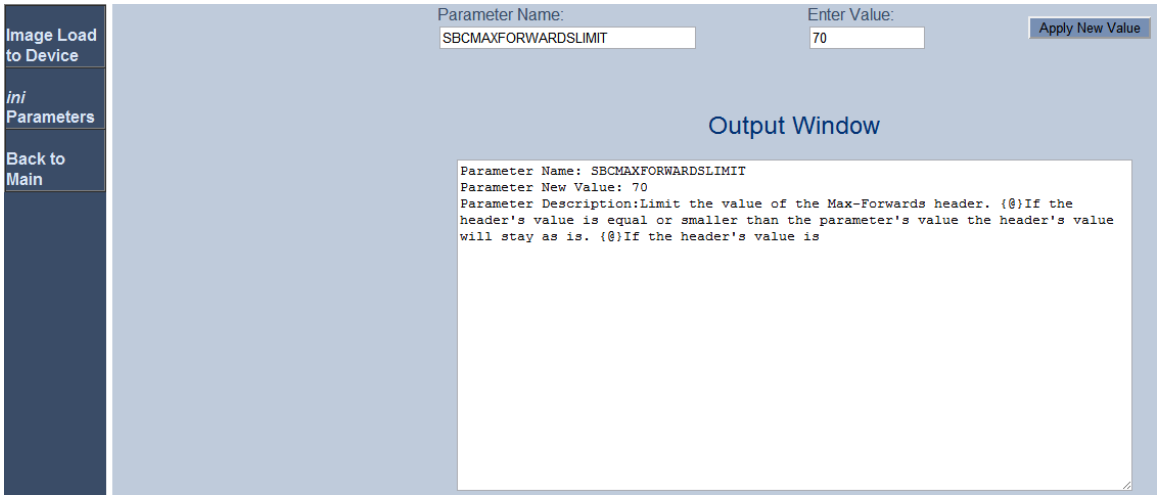
4.15.2 Configure Max-Forwards SIP Header

This step describes how to configure the Max-Forwards header. The Max-Forwards header is used to limit the number of servers (such as proxies) that can forward the SIP request. The Max-Forwards value indicates the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request.

➢ **To configure Max-Forwards SIP header:**

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://10.15.45.101/AdminPage).
2. In the left pane, click ***ini* Parameters**.

Figure 4-43: INI File Output Window



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

Parameter	Value
SBCMAXFORWARDSLIMIT	Enter **70**. Defines the Max-Forwards SIP header value. The Default sends Max- Forwards with a value of 10 and the QSC AG SIP Trunk requires a value of 70.

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

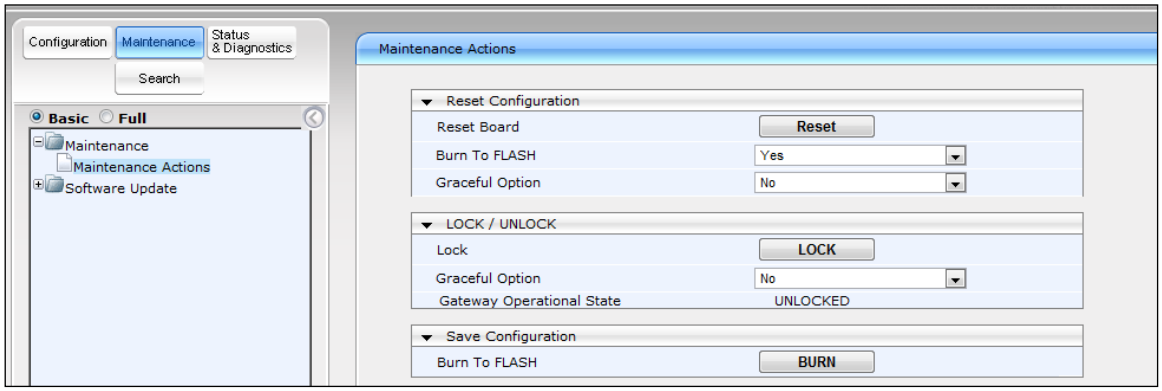
4.16 Step 16: Reset the E-SBC

After you have completed the E-SBC configuration as described in the previous steps, you need to 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 with a reset:**

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

Figure 4-44: Resetting the E-SBC



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

Reader's Notes

A AudioCodes INI File

The *ini* file configuration of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 33, is shown below:

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

;Board: Mediant 1000
;Serial Number: 3589366
;Slot Number: 1
;Software Version: 6.60A.022.003
;DSP Software Version: 624AE3 => 660.03
;Board IP Address: 10.15.45.101
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 495M  Flash size: 64M
;Num of DSP Cores: 14 Num DSP Channels: 30
;Profile: NONE
;Key features:;Board Type: Mediant 1000 ;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
;IP Media: Conf VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC
;PSTN Protocols: IUA=4 ;Channel Type: RTP DspCh=30 IPMediaDspCh=30
;DATA features: Eth-Port=6 ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;PSTN FALLBACK Supported
;E1Trunks=4 ;T1Trunks=4 ;FXSPorts=8 ;FXOPorts=8 ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;DSP Voice features:
IpmDetector RTCP-XR AMRPolicyManagement ;Control Protocols: MGCP
MEGACO H323 SIP SASurvivability SBC=120 MSFT TestCall=10 ;Default
features:;Coders: G711 G726;

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


[SYSTEM Params]
SyslogServerIP = 10.15.45.200
EnableSyslog = 1
NTPServerUTCOffset = 7200
TLSPkeySize = 1024
NTPServerIP = '10.15.21.10'
LDAPSEARCHDNSINPARALLEL = 0
```

```
[BSP Params]

PCMLawSelect = 3
[Analog Params]

[ControlProtocols Params]
AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]

[SS7 Params]

[Voice Engine Params]
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]
LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]
MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
MEDIASECURITYBEHAVIOUR = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENABLESYMMETRICMKI = 1
SBCFORKINGHANDLINGMODE = 1
SBCMAXFORWARDSLIMIT = 70
[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_4_1", 1, 1, 4, "User Port #0",
"GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "User Port #1",
"GROUP_1", "Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "User Port #2",
"GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3",
"GROUP_2", "Redundant";
PhysicalPortsTable 4 = "FE_5_1", 1, 1, 4, "User Port #4",
"GROUP_3", "Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 1, 4, "User Port #5",
"GROUP_3", "Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1,
EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, GE_4_1, GE_4_2;
EtherGroupTable 1 = "GROUP_2", 2, GE_4_3, GE_4_4;
EtherGroupTable 2 = "GROUP_3", 2, FE_5_1, FE_5_2;

[ \EtherGroupTable ]

[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 6, 10, 10.15.45.101, 16, 10.15.0.1, 1, "Voice",
10.15.21.10, , GROUP_1;
InterfaceTable 1 = 5, 10, 195.189.192.155, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, GROUP_2;
[ \InterfaceTable ]

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

[ CpMediaRealm ]
```

```
FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF,
CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault;
CpMediaRealm 1 = "MRLan", 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 = "FE-Lync.Lync.local:5067", 2, 1;
ProxyIp 1 = "213.148.136.218:5060", 0, 2;
[ \ProxyIp ]

[ IpProfile ]
FORMAT IpProfile_Index = IpProfile_ProfileName,
IpProfile_IpPreference, IpProfile_CodersGroupID,
IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay,
IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ,
IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport,
IpProfile_SBCRemoteReferBehavior, IpProfile_SBCRemote3xxBehavior,
IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
```

```
IpProfile_SBCRemoteEarlyMediaSupport,
IpProfile_EnableSymmetricMKI, IpProfile_MKISize,
IpProfile_SBCEnforceMKISize, IpProfile_SBCRemoteEarlyMediaRTP,
IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0,
0, 0, 0, -1, 1, 0, 1, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, -1,
0, 1, 1, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1,
0, 3, 2, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, -1;
IpProfile 2 = "QSC", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 1, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, -1, 0,
2, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1,
3, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, -1;
[ \IpProfile ]

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

[ IPGroup ]
FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet,
IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName;
IPGroup 1 = 0, "Lync", 1, "sip.qsc.de", "", 0, -1, -1, 0, -1, 1,
"", 1, 1, -1, -1, 1, 0, 0, "", 0, -1, -1, "";
IPGroup 2 = 0, "QSC - 02463974990 ", 2, "sip.qsc.de", "", 0, -1, -
1, 0, -1, 2, "", 1, 2, -1, -1, 0, 0, 0, "", 0, -1, 1, "";
IPGroup 3 = 0, "QSC - 02463974991", 2, "sip.qsc.de", "", 0, -1, -
1, 0, -1, 2, "", 1, 2, -1, -1, 0, 0, 0, "", 0, -1, 1, ""; [
\IPGroup ]

[ Account ]
; ** NOTE: Changes were made to active configuration.
; **    The data below is different from current values.
FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroup, Account_ServingIPGroup, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 1 = -1, 1, 2, "02463974990", *, "sip.qsc.de", 1,
"02463974990", 2;
```

```
Account 2 = -1, 1, 3, "02463974991", *, "sip.qsc.de", 1,
"02463974991", 2; [ \Account ]

[ ConditionTable ]

FORMAT ConditionTable_Index = ConditionTable_Condition,
ConditionTable_Description;
ConditionTable 2 = "header.Referred-By.url.user contains
'2463974990'", "02463974990";
ConditionTable 3 = "header.Referred-By.url.user contains
'2463974991'", "02463974991";

[ \ConditionTable ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress,
IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,
IP2IPRouting_AltRouteOptions, IP2IPRouting_CostGroup;
IP2IPRouting 0 = 1, "*", "*", "*", "*", 6, , -1, 0, 1, -1, ,
"internal", 0, -1, 0, ;
IP2IPRouting 1 = 1, "02463974990", "*", "*", "*", 0, , -1, 0, 0,
2, 2, "", 0, -1, 0, ;
IP2IPRouting 2 = 1, "02463974991", "*", "*", "*", 0, , -1, 0, 0,
3, 2, "", 0, -1, 0, ;
IP2IPRouting 3 = 1, "*", "*", "*", "*", 0, 2, -1, 0, 0, 2, 2, "",
0, -1, 0, ;
IP2IPRouting 4 = 1, "*", "*", "*", "*", 0, 3, -1, 0, 0, 3, 2, "",
0, -1, 0, ;
IP2IPRouting 5 = -1, "*", "", "", "*", 0, , -1, 0, 0, 1, 1, "", 0,
-1, 0, ;

[ \IP2IPRouting ]

[ SIPInterface ]
FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort,
SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD,
SIPInterface_MessagePolicy, SIPInterface_TLSMutualAuthentication;
SIPInterface 1 = "Voice", 2, 0, 0, 5067, 1, , -1;
SIPInterface 2 = "WANSP", 2, 5060, 0, 0, 2, , -1;
[ \SIPInterface ]

[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index =
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
```

```
IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix,
IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix,
IPInboundManipulation_DestHost, IPInboundManipulation_RequestType,
IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight,
IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 1 = 0, 0, 1, "+", "*", "*", "*", 0, 0, 1, 0,
255, "", "";
IPInboundManipulation 2 = 0, 0, 1, "*", "*", "+49", "*", 0, 1, 1,
0, 255, "", "";
IPInboundManipulation 3 = 0, 0, 1, "*", "*", "*", "*", 0, 1, 1, 0,
255, "00", "";

[ \IPInboundManipulation ]

[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix,
IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID,
IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight,
IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 3 = 0, 2, 1, "*", "*", "*", "*", 0, -1, 0,
1, 0, 0, 255, "+", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

; ** NOTE: Changes were made to active configuration.
; **    The data below is different from current values.
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0;
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 1;

[ \CodersGroup0 ]
```

```
[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 1 = 0, "invite", "header.referred-by exists",
"header.P-Asserted-Identity.URL.user", 2, "header.referred-
by.URL.user", 0;
MessageManipulations 2 = 0, "", "", "header.P-Asserted-
Identity.URL.user", 6, "'+49'", 1;
MessageManipulations 3 = 0, "", "", "header.P-Asserted-
Identity.URL.user", 3, "'0'", 1;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]

[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com