Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Microsoft® Lync™ Server 2010 & Alteva SIP Trunk using AudioCodes Mediant E-SBC

SBC

Microsoft Partner
Gold Unified Communications

Alteva
Formerly WVT

Microsoft® Lync™

AudioCodes

March 2013

Document #: LTRT-12240

Table of Contents

List of Figures

List of Tables

Notice

This document describes how to connect the Microsoft Lync Server 2010 and Alteva SIP Trunk using the 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: March-21-2013

Trademarks

WEEE EU Directive

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

Customer Support

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

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.

Note: Throughout this manual, unless otherwise specified, the term *E-SBC* refers to the AudioCodes device.

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 Alteva's SIP Trunking and Microsoft's Lync Communication platform (Lync Server 2010).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Alteva Partners who are responsible for installing and configuring Alteva's 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 Gateway platforms, or as a software-only solution for deployment with third-party hardware.

Reader's Notes

2 Component Information

The section below describes component information for connecting the Microsoft Lync Server 2010 and Alteva SIP Trunk using AudioCodes Mediant E-SBC.

2.1 AudioCodes E-SBC Version

The table below describes the 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.014.007
Protocol	▪ SIP/UDP (to the Alteva SIP Trunk) ▪ SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 Alteva SIP Trunking Version

The table below describes the Alteva SIP Trunking Version.

Table 2-2: Alteva SIP Trunk Version

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

2.3 Microsoft Lync Server 2010 Version

The table below describes the 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

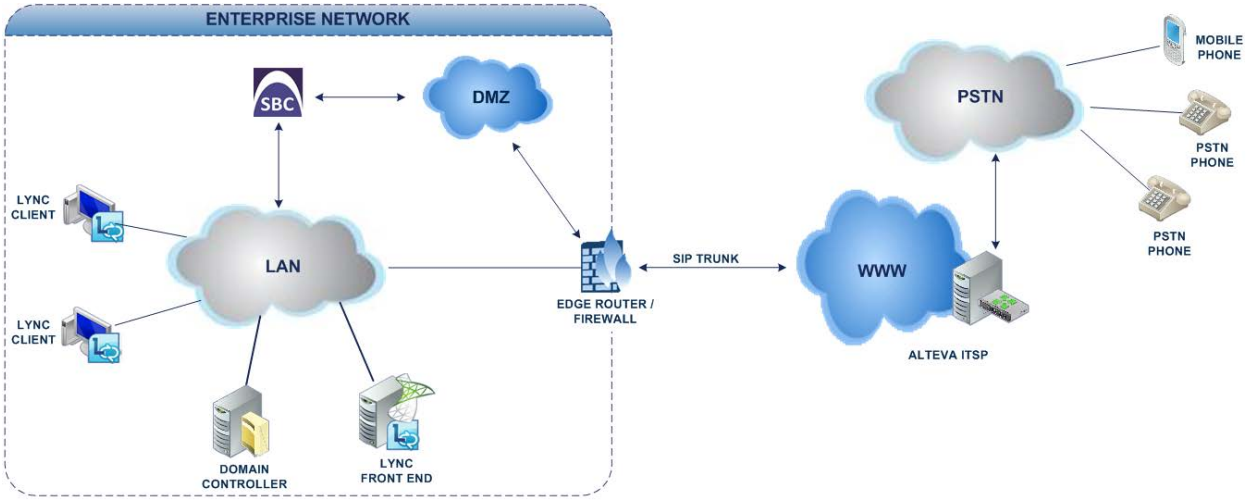
2.4 Deploying the E-SBC - Typical Topology

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 Alteva's 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 Alteva's SIP Trunk located in the public network.

The figure below illustrates E-SBC interworking between Lync Server 2010 and Alteva's SIP Trunking site.

Figure 2-1: E-SBC Interworking Microsoft Lync and Alteva 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 ▪ Alteva SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Lync Server 2010 functions with SIP-over-TLS transport type ▪ Alteva SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Microsoft Lync Server 2010 supports G.711A-law and G.711U-law coders ▪ Alteva SIP Trunk supports G.711U-law coder
Media Transcoding	▪ Microsoft Lync Server 2010 operates with the SRTP media type ▪ Alteva 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 Alteva SIP Trunk.

Reader's Notes

3 Configuring Lync Server 2010

This section shows how to configure the Lync Server 2010 to operate with the E-SBC device. Follow this procedure:

1. Configure the device as 'IP/PSTN Gateway' (see Section 3.1 on page 15).
2. Associate IP/PSTN Gateway with the Mediation Server (see Section 3.2 on page 19).
3. Configure a 'Route' to utilize the SIP Trunk connected to the E-SBC device (see Section 3.3 on page 25).

Note: Dial Plans, Voice Policies and PSTN usages are also necessary for enterprise voice deployment but they're beyond the scope of this Configuration Note.

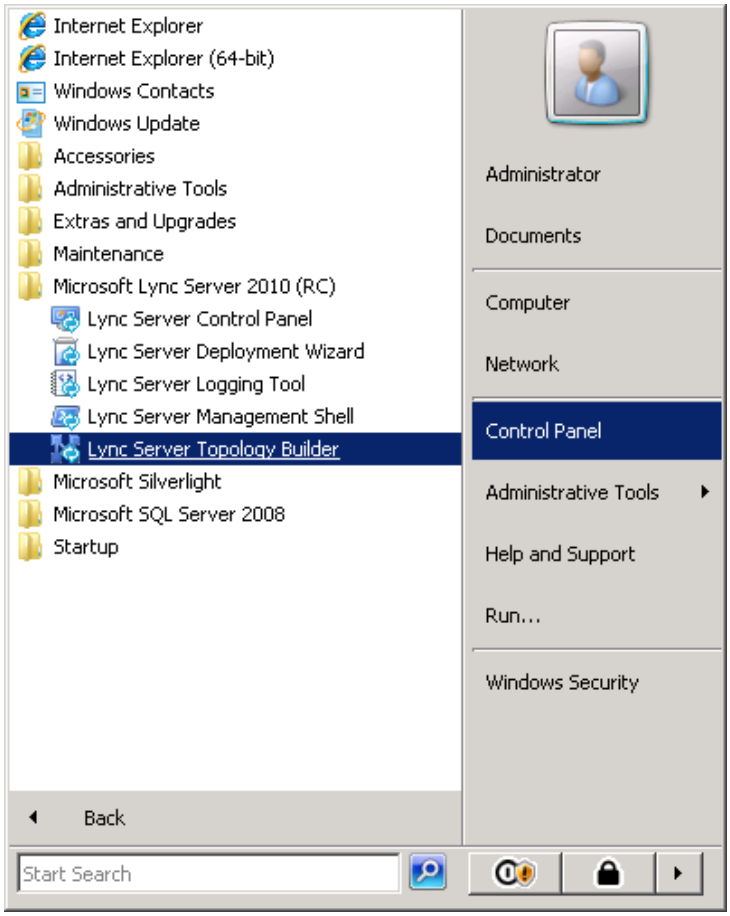
3.1 Configuring the E-SBC Device as IP/PSTN Gateway

This section shows how to configure the E-SBC device as an IP/PSTN Gateway.

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

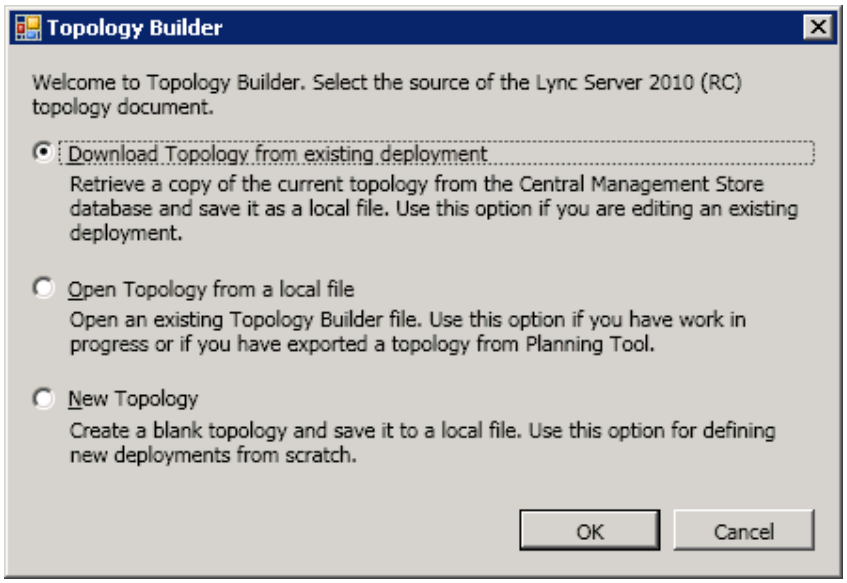
1. On the server where the Topology Builder is located, start the Lync Server 2010 **Topology Builder** (click **Start**, select **All Programs** and select **Lync Server Topology Builder**).

Figure 3-1: Opening the Lync Server Topology Builder



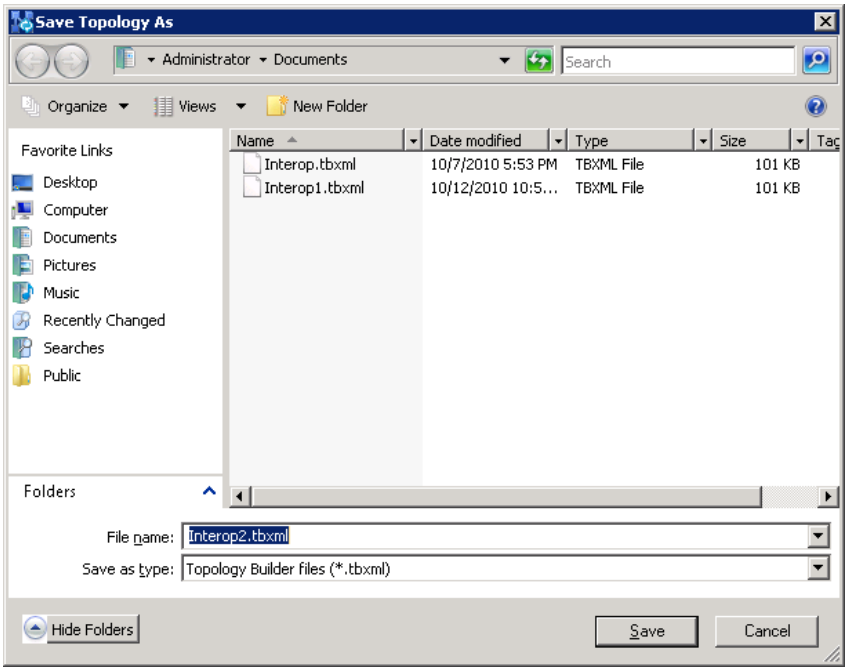
The following screen is displayed:

Figure 3-2: Topology Builder Options



2. Select the option 'Download Topology from the existing deployment' and click **OK**. You're prompted to save the Topology.

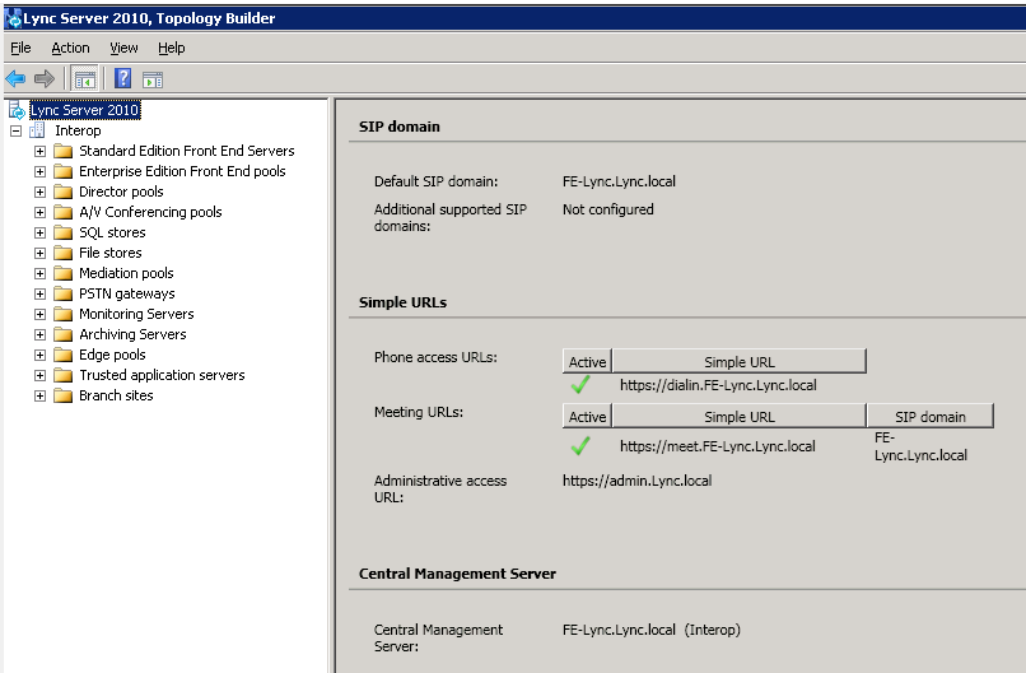
Figure 3-3: Saving the Topology



3. Enter the new **File name** and **Save**. This action enables you to roll back from any changes you make during the installation.

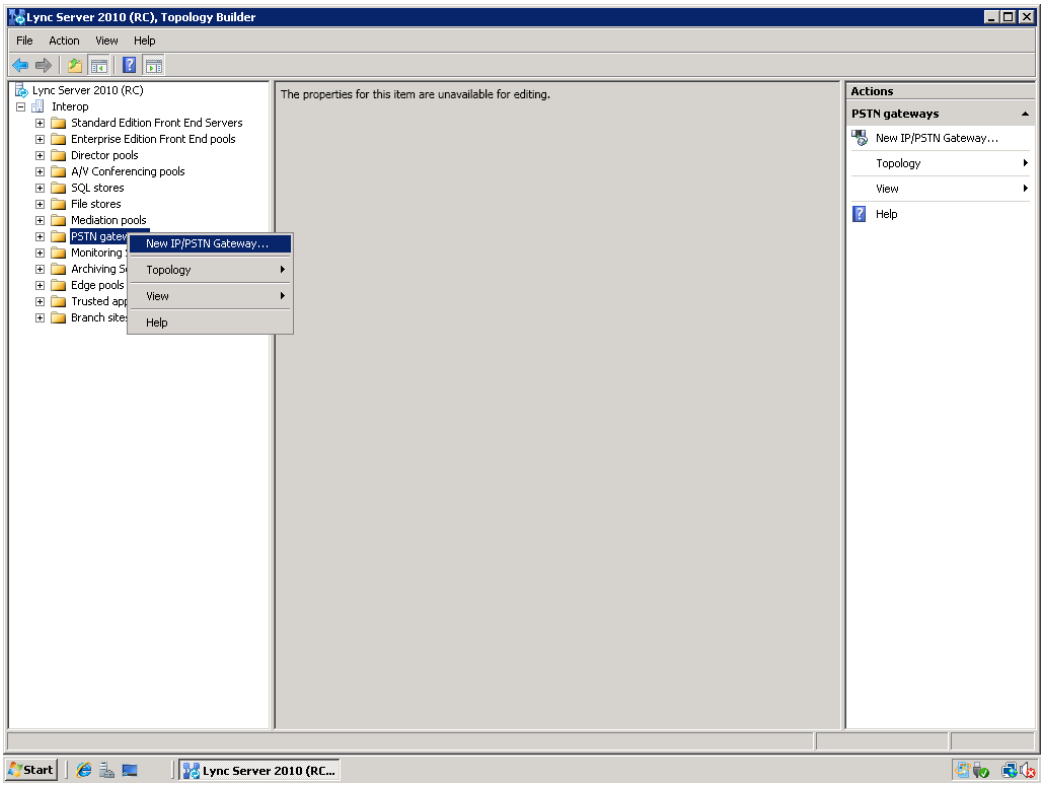
The Topology Builder screen with the topology downloaded is displayed.

Figure 3-4: Downloaded Topology



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

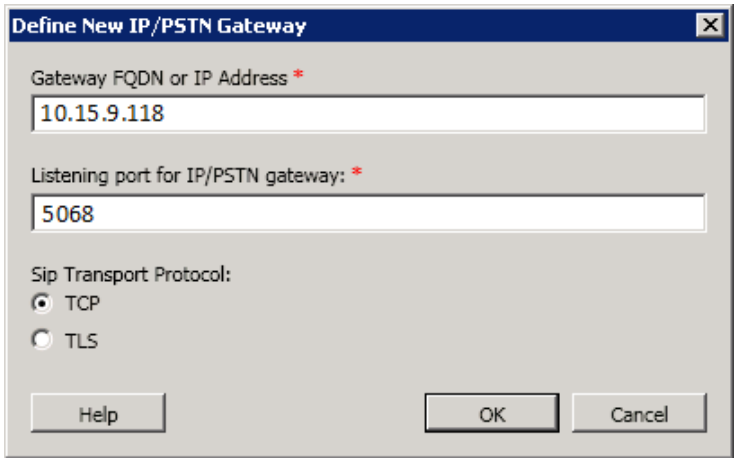
Figure 3-5: Choosing New IP/PSTN Gateway



5. Enter the IP address or FQDN of the E-SBC, i.e., 10.15.9.118, and click **OK**.

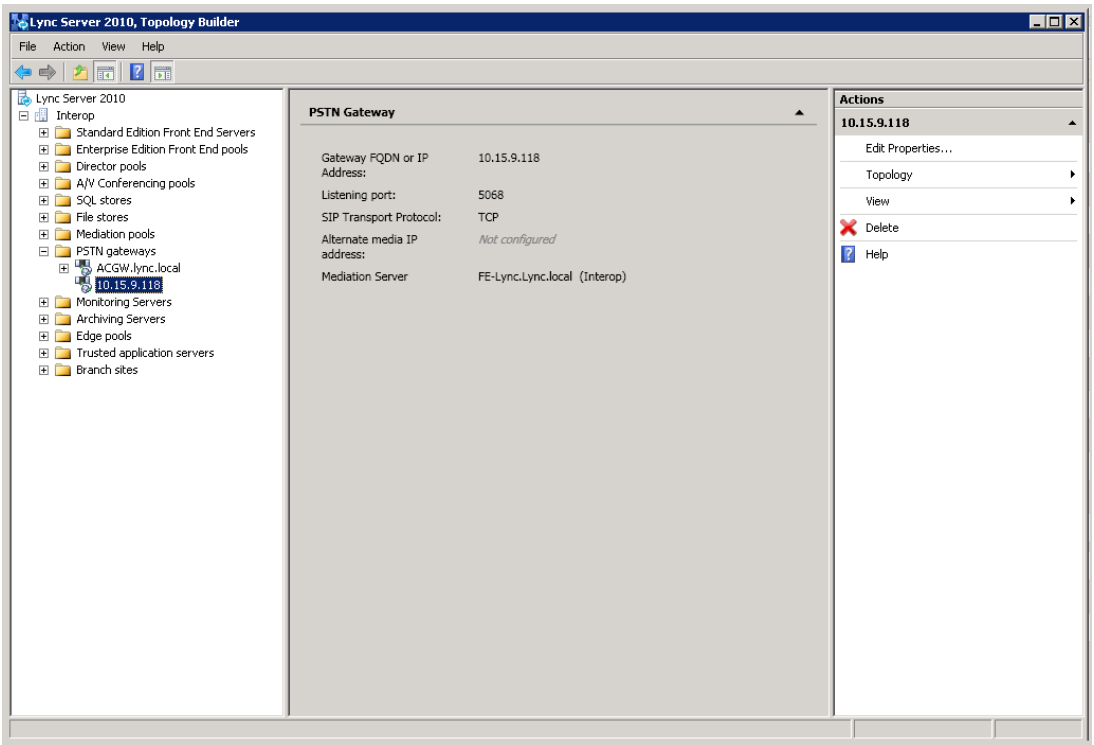
Note: The 'Listening port' for the device is **5068** and 'SIP Transport Protocol' is **TCP**.

Figure 3-6: Defining New IP/PSTN Gateway



The E-SBC device is now added as an 'IP/PSTN Gateway'.

Figure 3-7: Adding the device as IP/PSTN Gateway



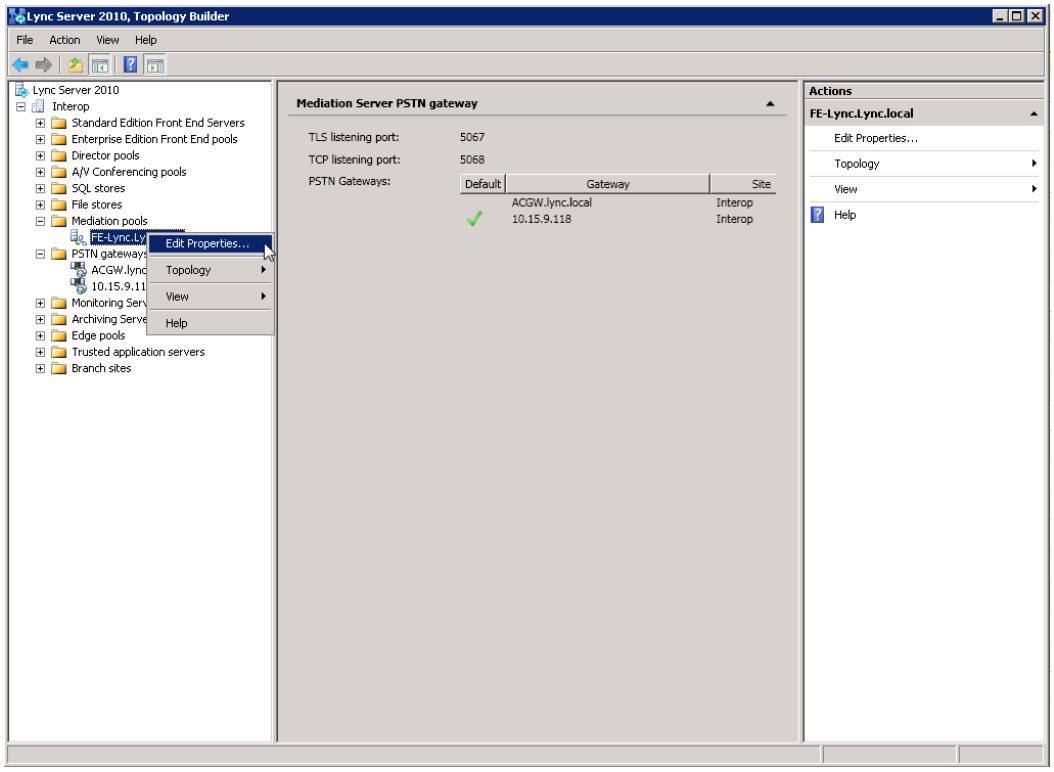
3.2 Associating the IP/PSTN Gateway with the Mediation Server

This section shows how to associate the 'IP/PSTN Gateway' with the Mediation Server.

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

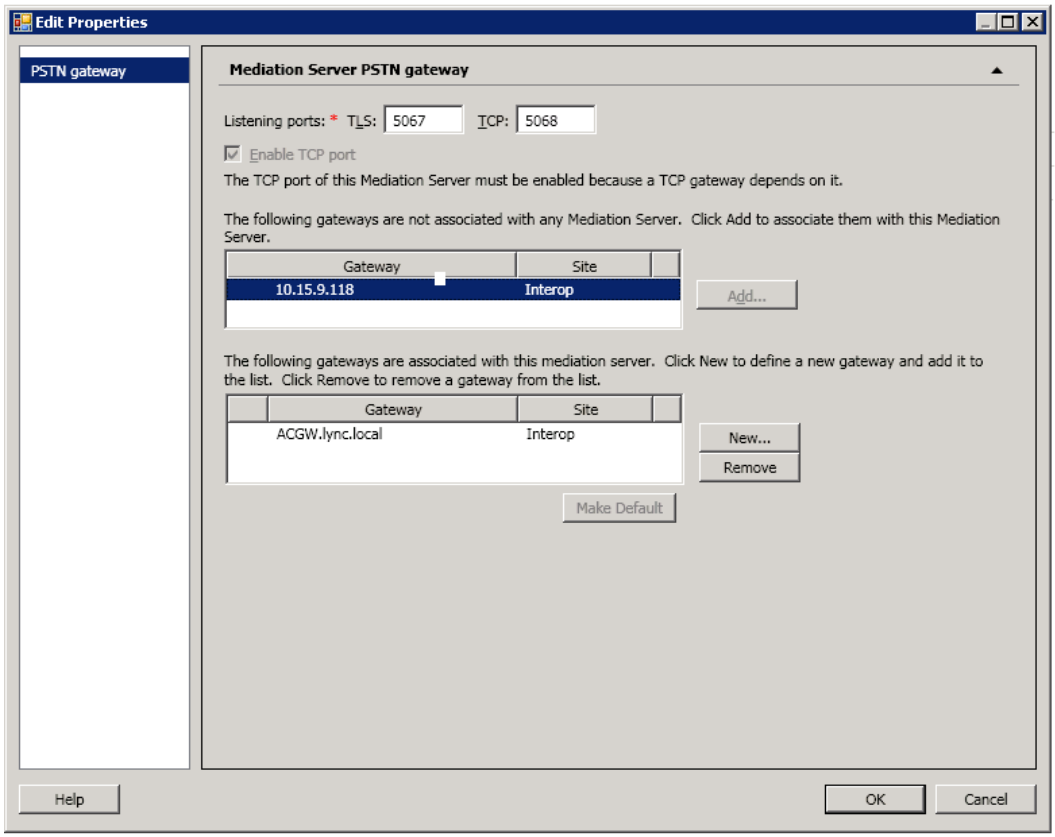
1. Right-click the Mediation Server that uses the E-SBC device, i.e., FE-Lync.Lync.local, and select **Edit Properties**.

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



The following screen is displayed:

Figure 3-9: Editing PSTN Gateway Properties

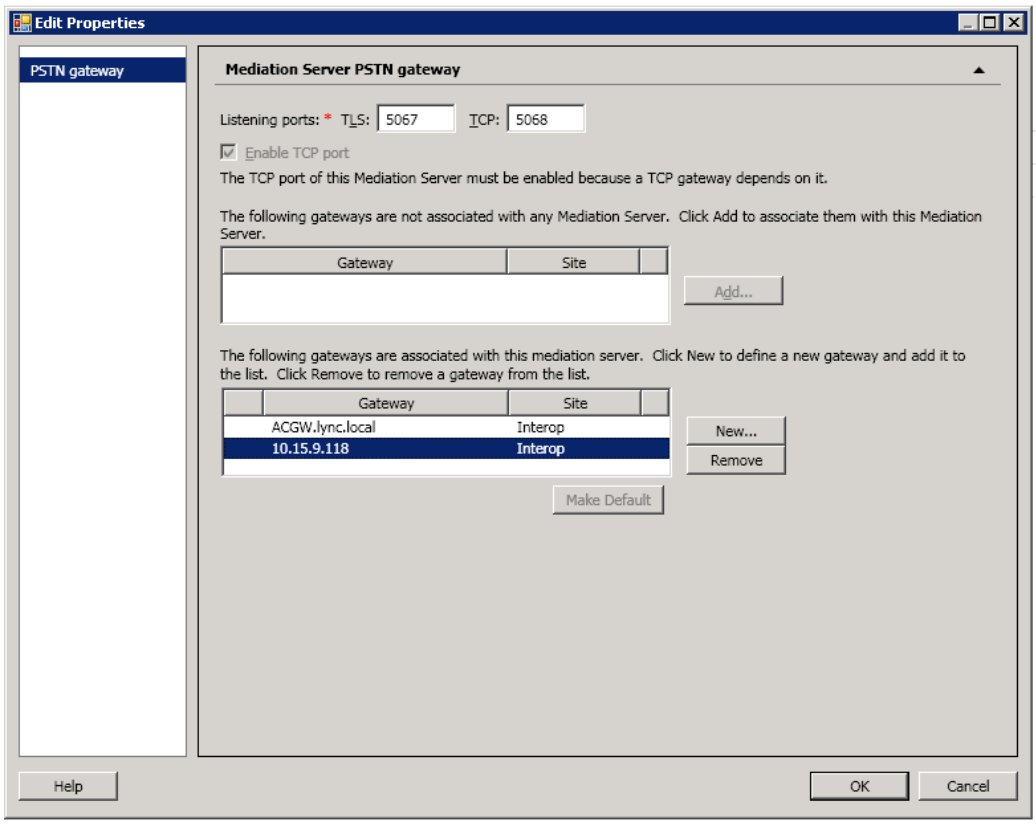


2. In the uppermost left corner, choose **PSTN gateway**.

   In the pane listing *gateways not associated with any Mediation Server*, select the device, i.e., 10.15.9.118, in this example, and click the **Add** button to associate it with this Mediation Server.

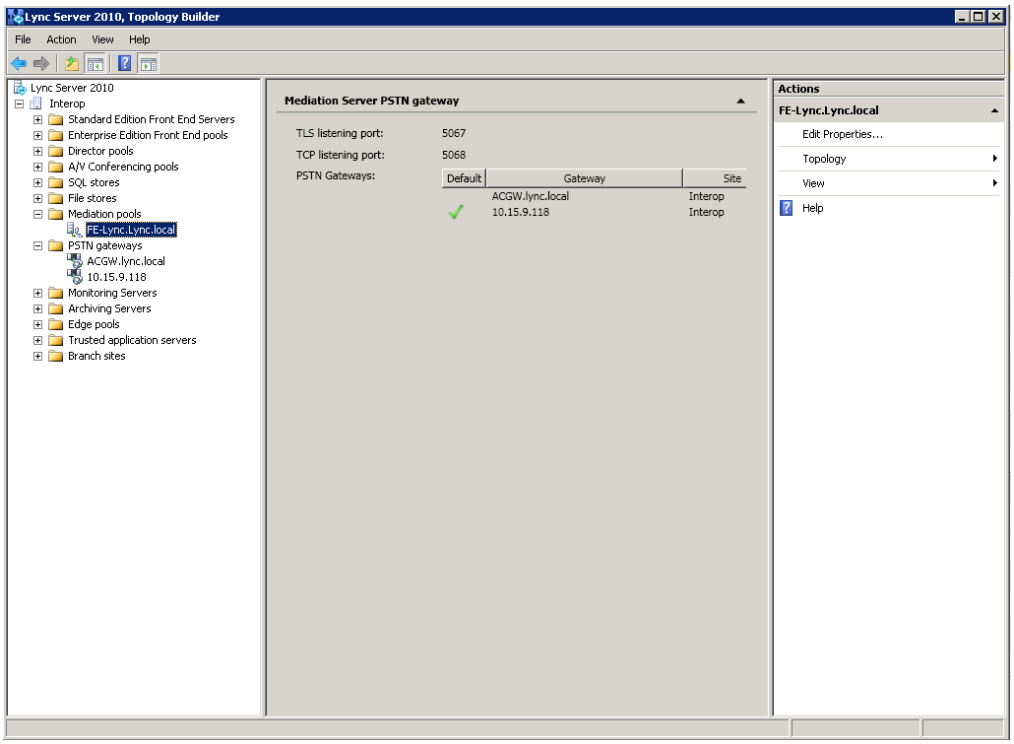
Note: The screen shows two panes - a pane listing *gateways not associated with any Mediation Server* and below it, a pane listing *gateways associated with this mediation server*.

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



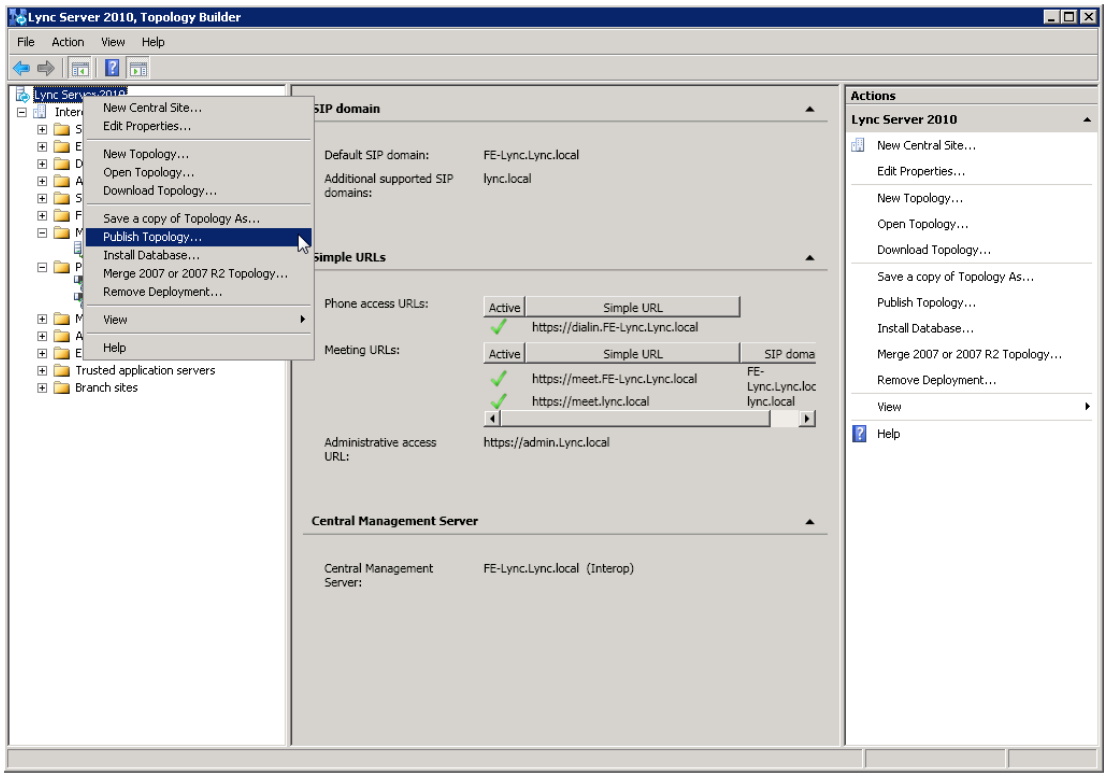
3. Click **OK**.

Figure 3-11: Displaying Media Server PSTN Gateway Association Properties



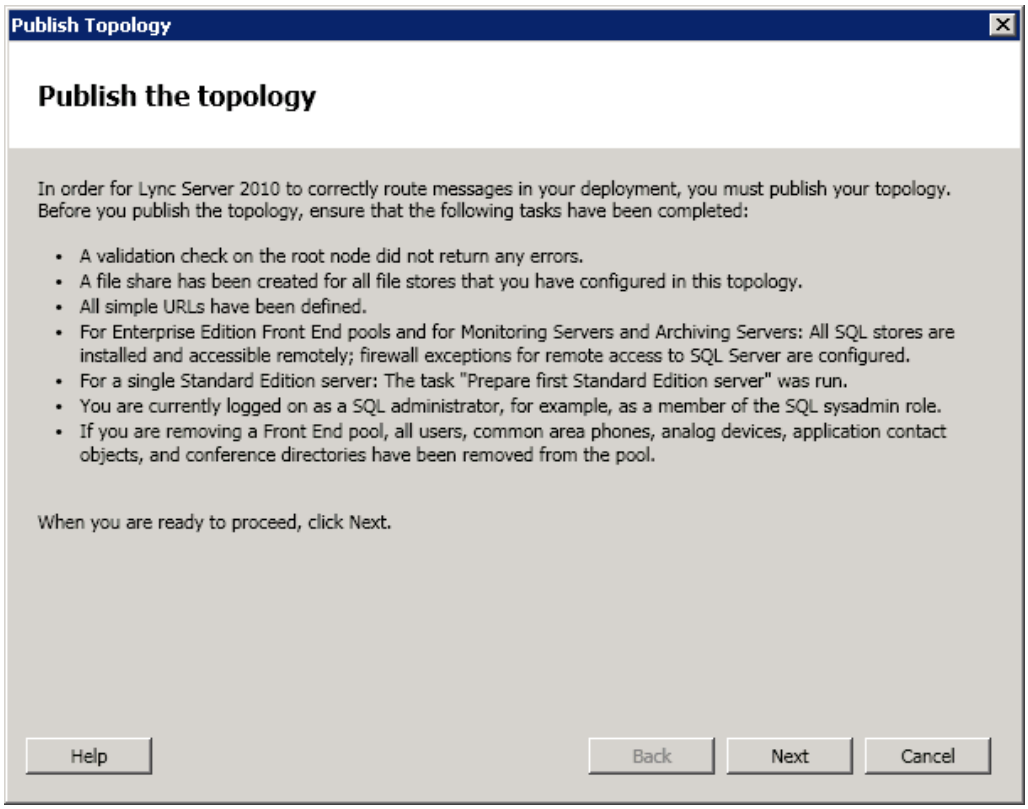
4. In the Lync Server main menu, choose **Action > Publish Topology**.

Figure 3-12: Publishing Topology



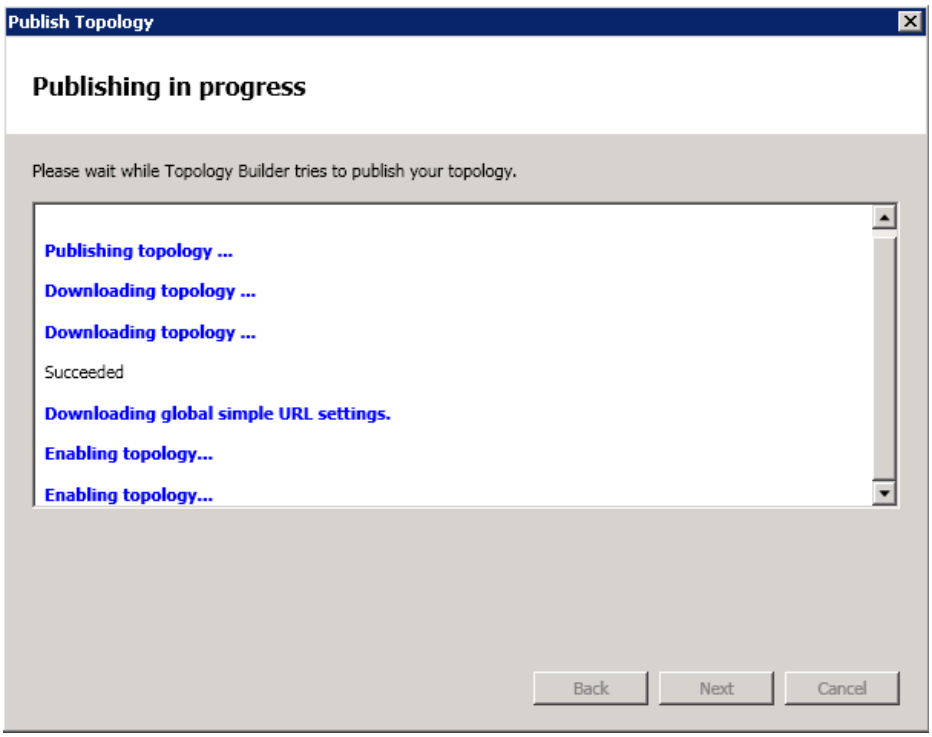
The Publish Topology screen is displayed:

Figure 3-13: Displaying Publish Topology Confirmation



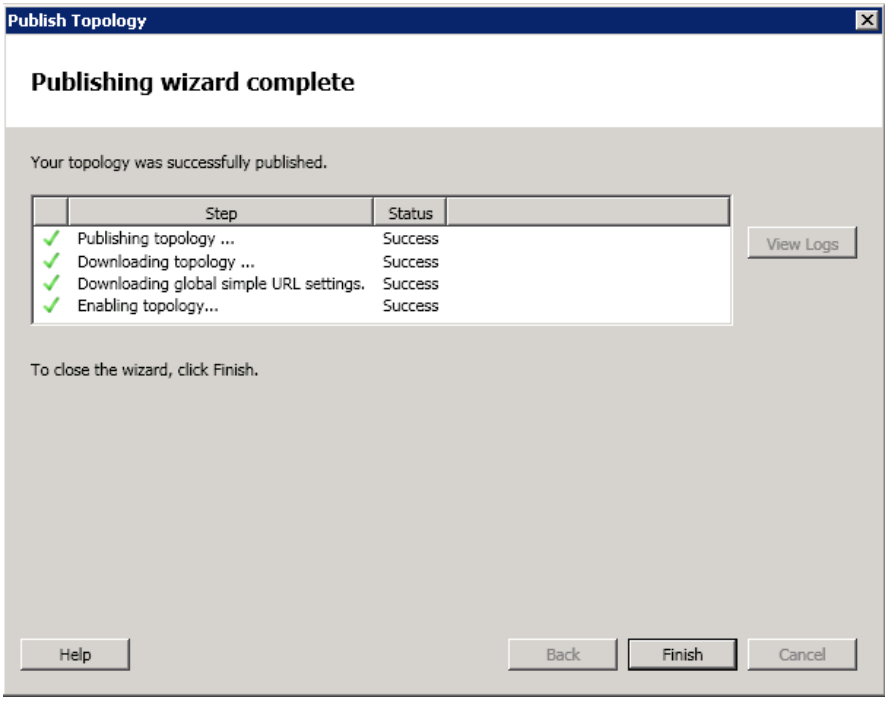
5. Click **Next**. The Topology Builder attempts to publish your topology.

Figure 3-14: Publishing Topology Progress



6. Wait until the topology publishing process ends successfully.

Figure 3-15: Displaying Publish Topology Successfully Completed



7. Click **Finish**.

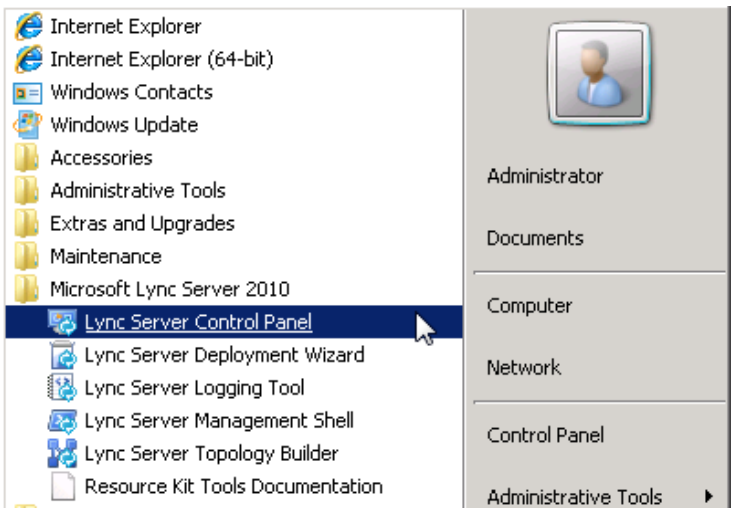
3.3 Configuring the 'Route' on the Lync Server 2010

This section shows how to configure a 'Route' on the Lync server and to associate it with the E-SBC (now defined in the Microsoft Lync environment as a 'PSTN gateway').

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

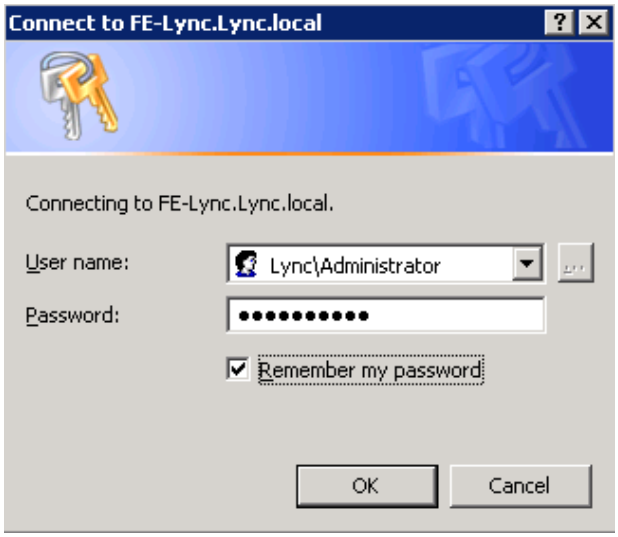
1. Open the Communication Server Control Panel (CSCP), click **Start**, select **All Programs** and select **Lync Server Control Panel**.

Figure 3-16: Opening the Lync Server Control Panel



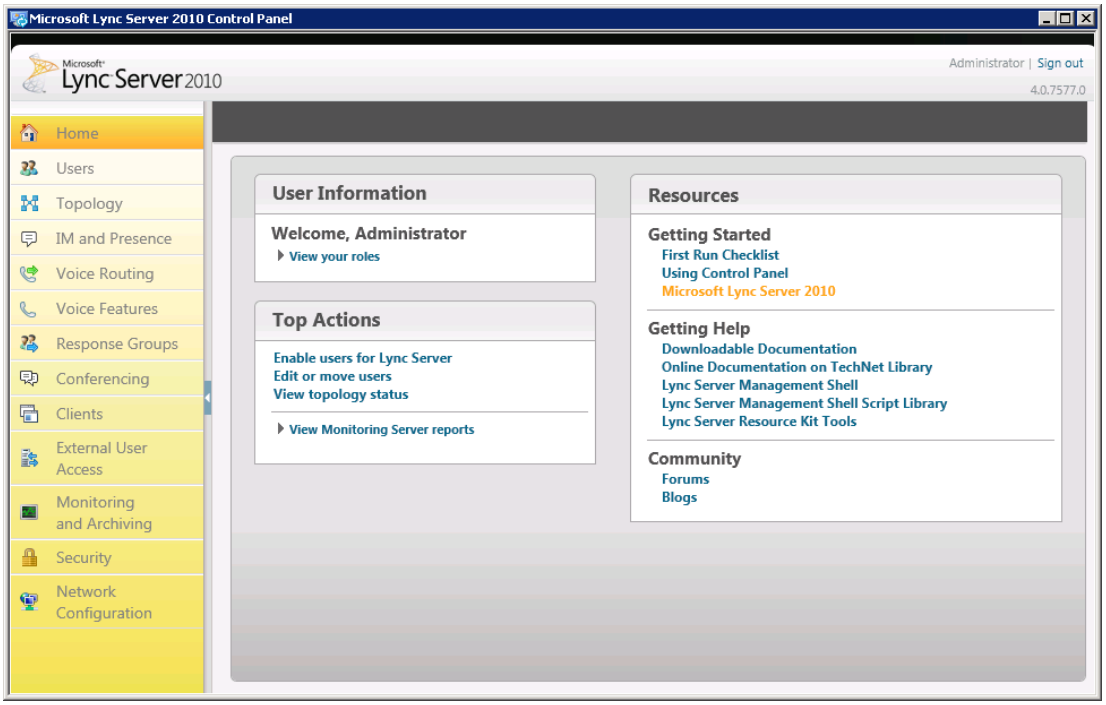
2. In the credentials prompt; enter your domain 'User name' and 'Password'.

Figure 3-17: Entering Lync Server Credentials



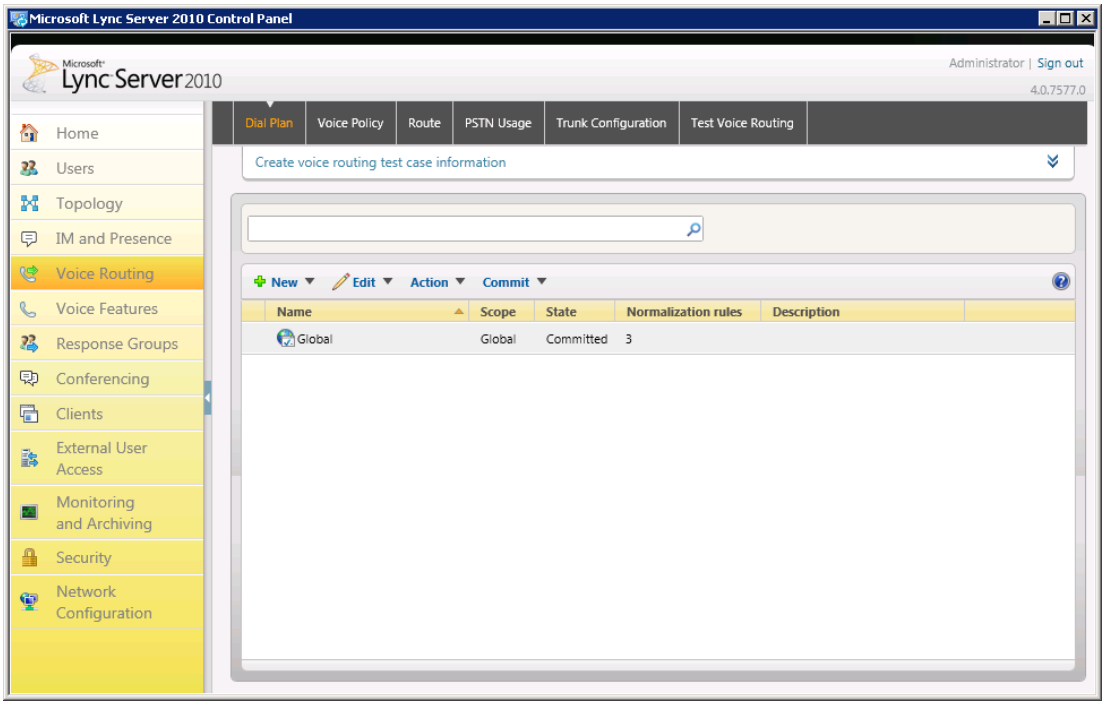
The CSCP Home page is displayed:

Figure 3-18: Displaying CSCP Home Page



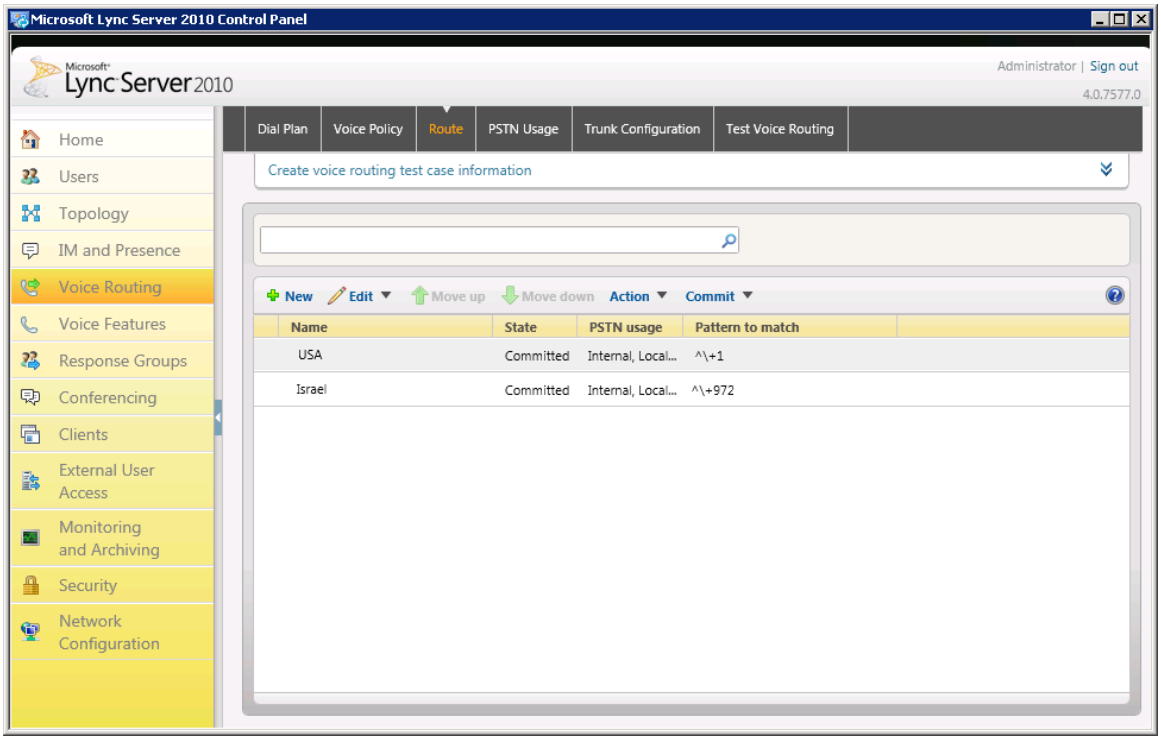
3. In the Navigation pane, select the **Voice Routing** option.

Figure 3-19: Selecting Voice Routing Option



4. Select the **Route** tab:

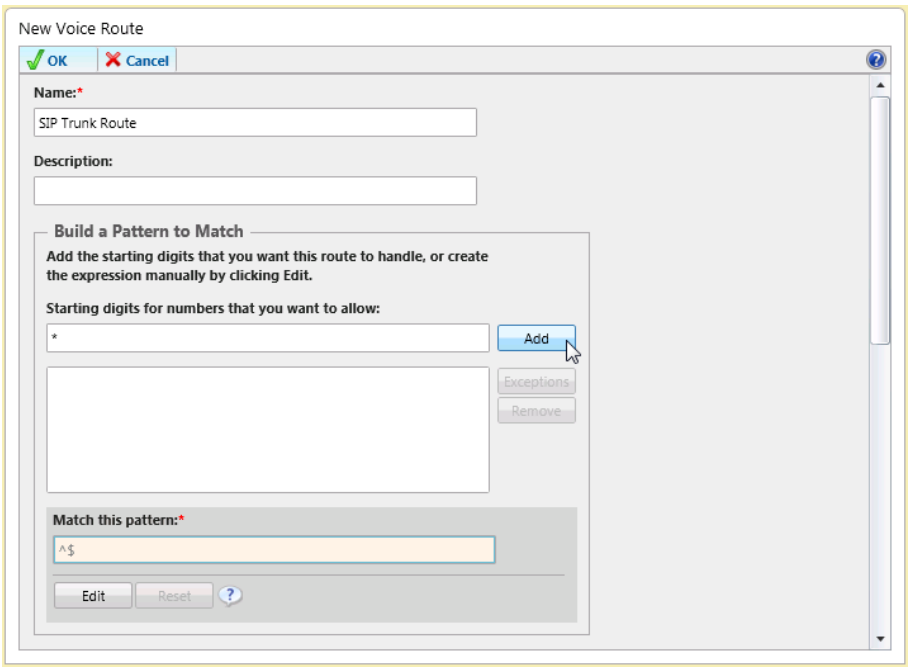
Figure 3-20: Selecting Route Tab



5. Click 

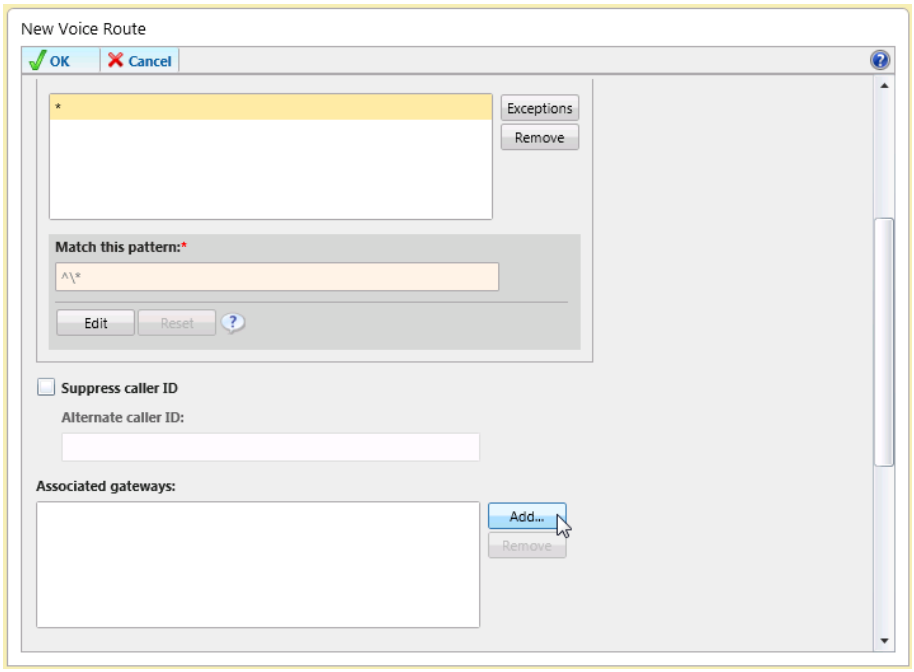
6. In the New Voice Route screen, define a Name for this route, e.g., SIP Trunk Route.
7. Under 'Build a Pattern to Match', add the starting digits you want this route to handle, e.g., '*', which means 'to match all numbers', and click **Add**.

Figure 3-21: Defining New Voice Route



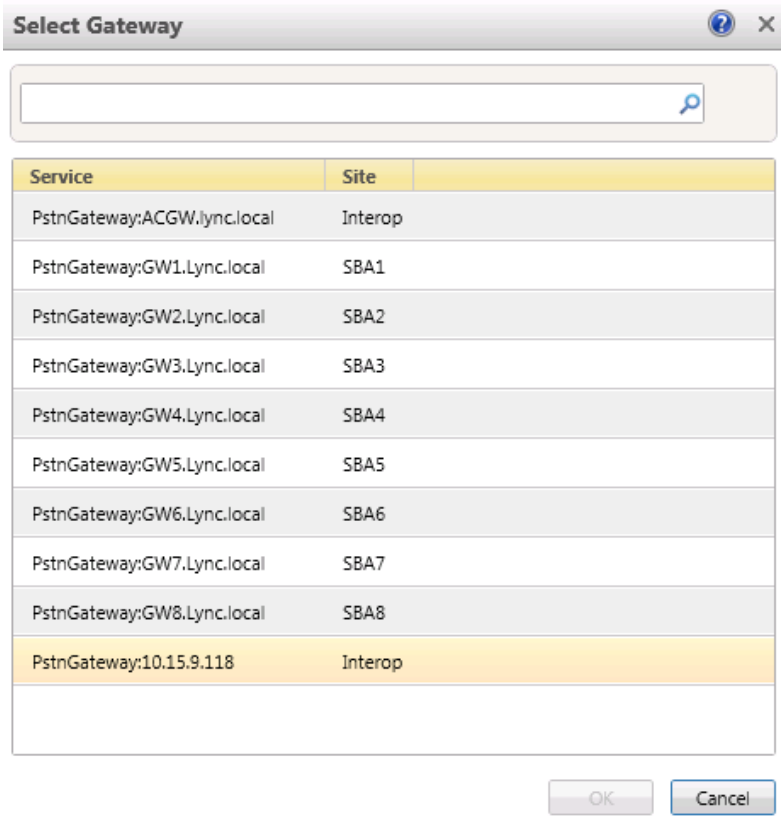
8. Associate the route with the E-SBC IP/PSTN gateway you created above: Scroll down to the Associated Gateways pane and click **Add**.

Figure 3-22: Adding the New Device



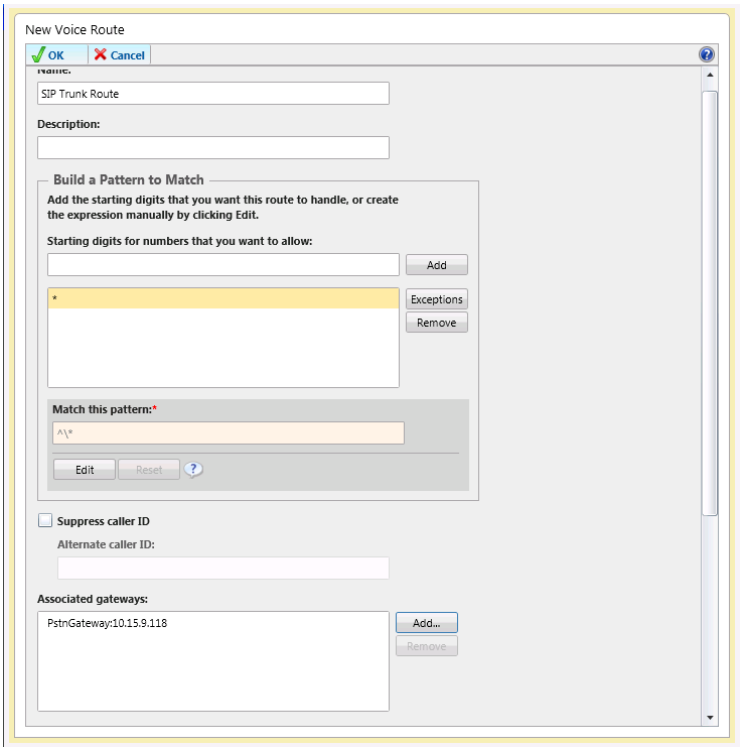
A list of all gateways deployed is displayed:

Figure 3-23: Displaying List of Deployed Devices



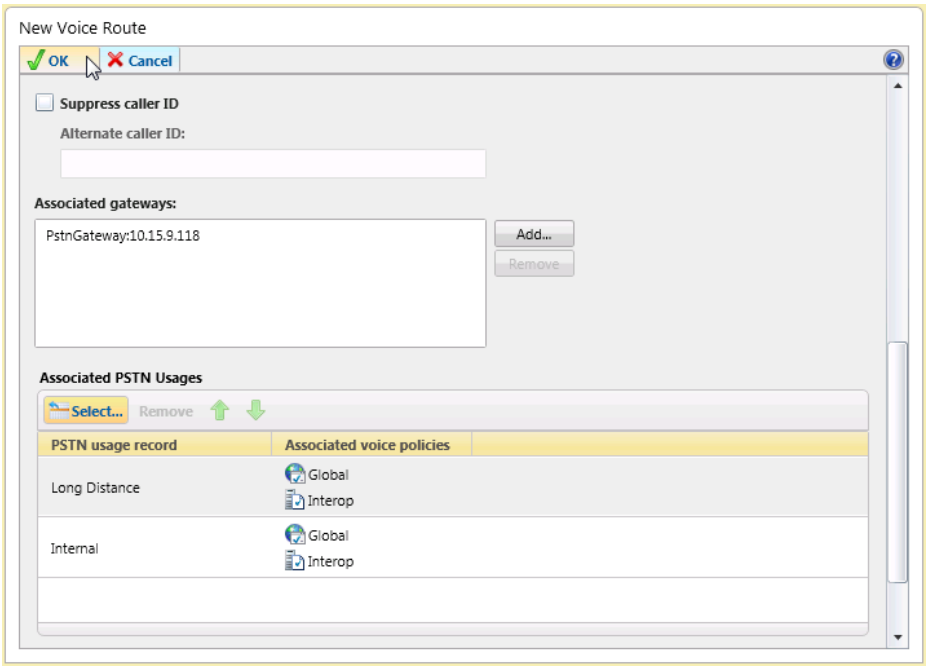
9. Select the device you created above and click **OK**.

Figure 3-24: Selecting the Device



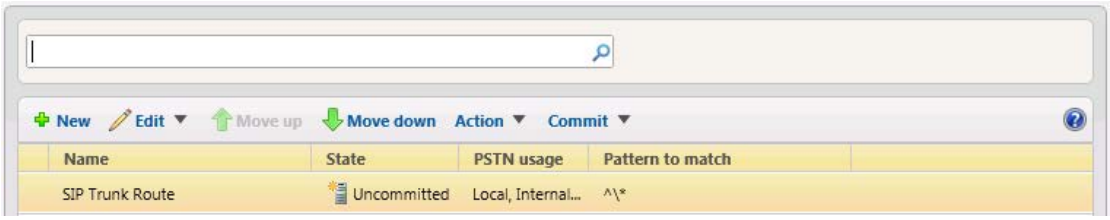
10. Associate a PSTN Usage with this route. In the Associated PSTN Usages toolbar, click **Select** and add the associated PSTN Usage.

Figure 3-25: Associating PSTN Usage with the Device



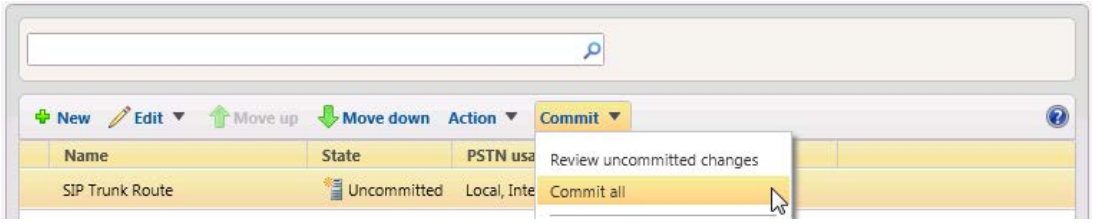
11. Click the **OK** button in the toolbar at the top of the New Voice Route pane. The New Voice Route (Uncommitted) is displayed.

Figure 3-26: Confirming New Voice Route



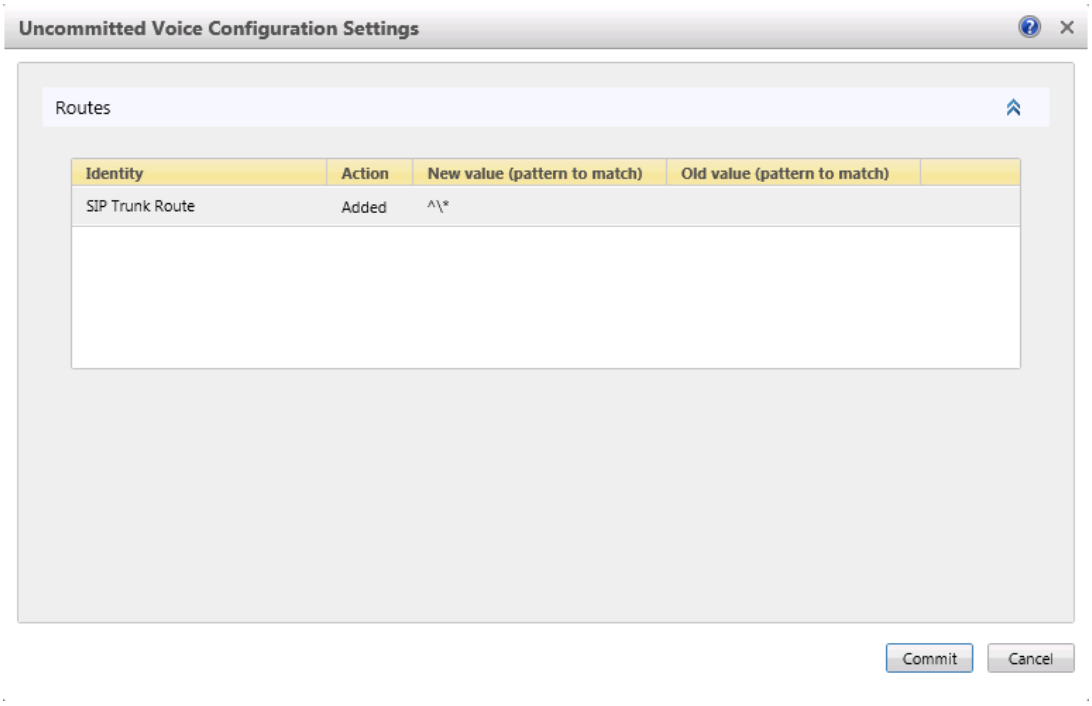
12. From the **Commit** drop-down menu, select the **Commit All** option.

Figure 3-27: Committing Voice Routes



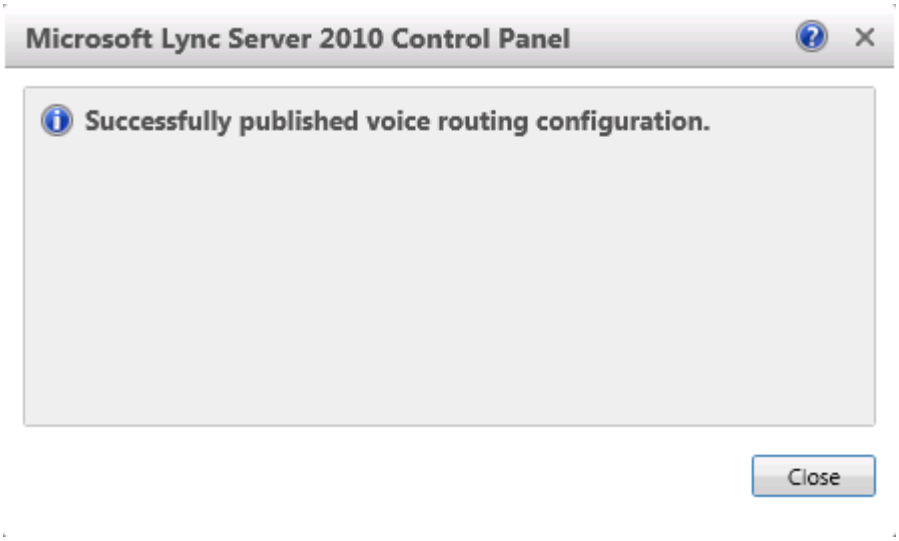
13. In the Uncommitted Voice Configuration Settings window, click the **Commit** button.

Figure 3-28: Configuring Uncommitted Voice Configuration Settings



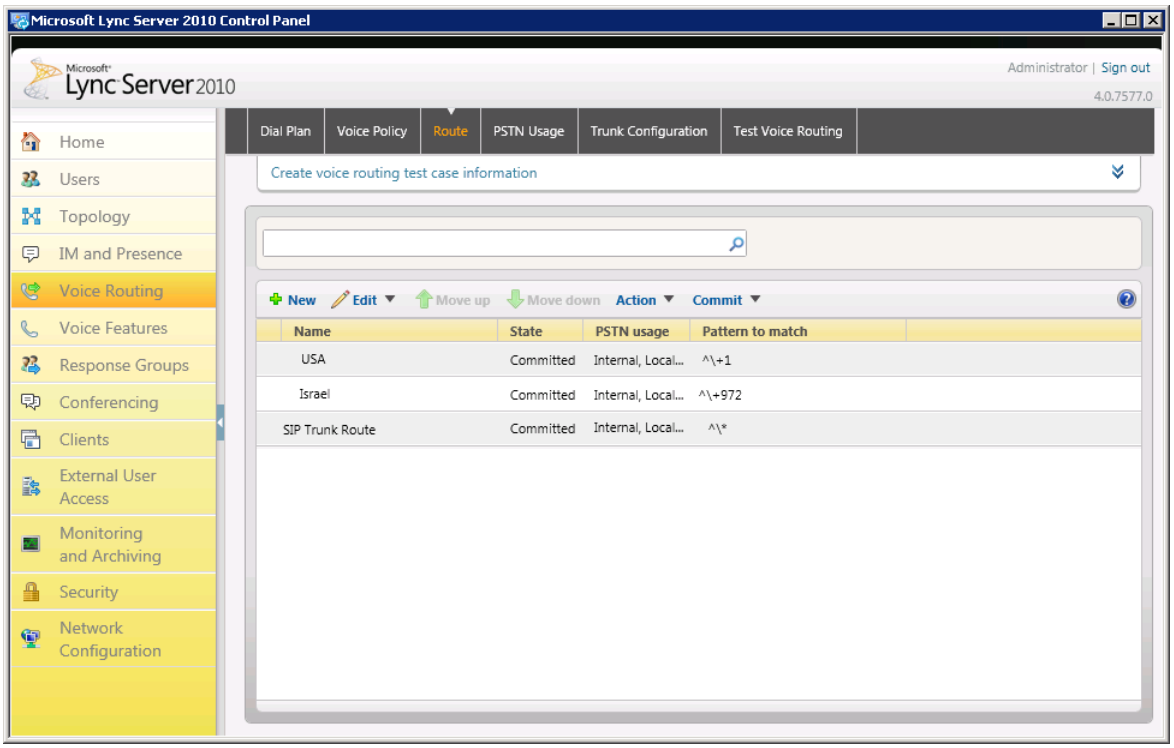
The following message is displayed:

Figure 3-29: Confirming Voice Routing Configuration



14. In the **Microsoft Lync Server 2010 Control Panel** prompt, click **Close**. The new committed Route is now displayed in the Voice Routing screen.

Figure 3-30: Displaying Committed Routes



Reader's Notes

4 Configuring AudioCodes E-SBC

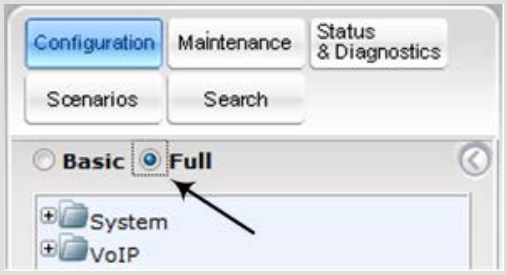
This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2010 and Alteva SIP Trunk:

- **E-SBC WAN interface**: Alteva 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:

- 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

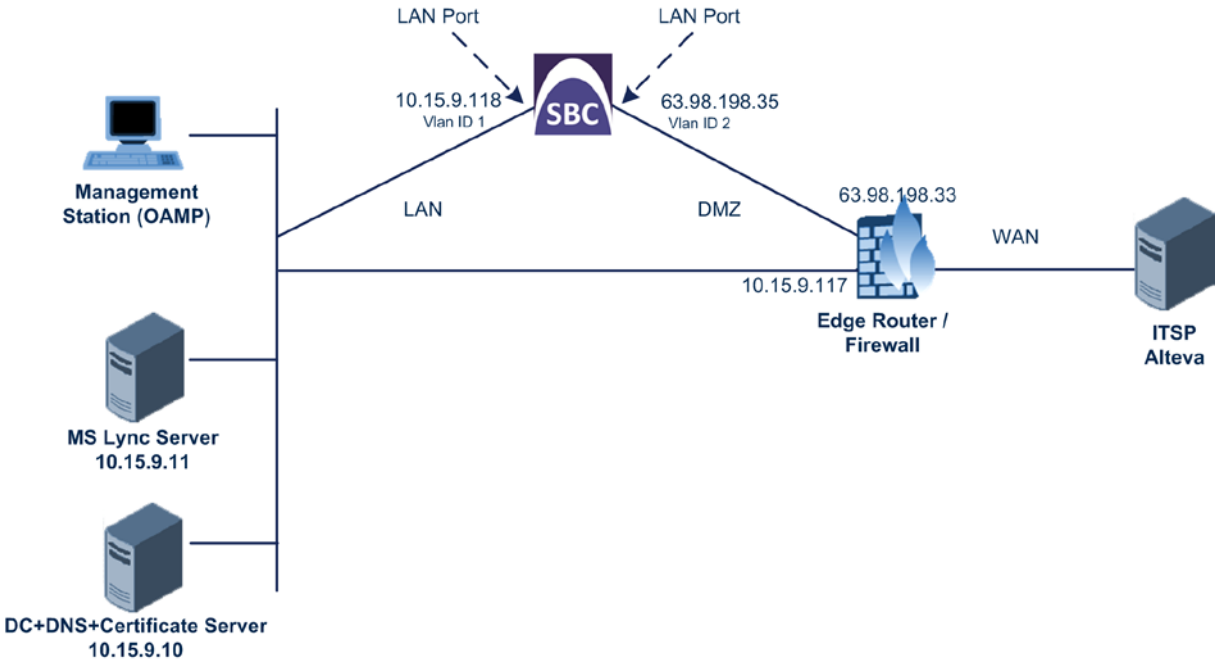
This step describes how to configure the E-SBC's network interfaces. There are several ways to deploy the E-SBC. However, the example scenario in this document uses the following deployment method:

- The E-SBC interfaces are between the Lync servers located on the LAN and the Alteva 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: Configuring Network Interfaces



4.1.1 Step 1a: Configure IP Network Interfaces

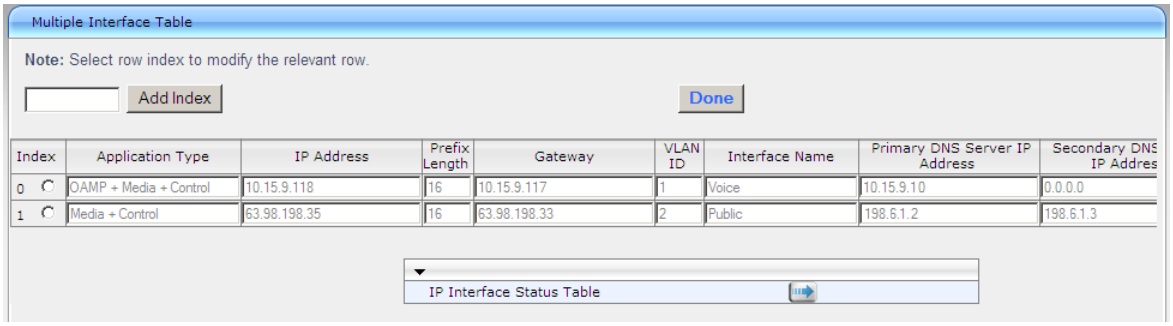
The procedure below describes how to configure the IP network interfaces for each of the following interfaces:

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

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

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

Figure 4-2: Configuring IP Network Interfaces



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	Settings
IP Address	**10.15.9.118**
Prefix Length	**16** This is the subnet mask in bits for 255.255.0.0.
Gateway	**10.15.9.117**
VLAN ID	**1**
Interface Name	**Voice** This is an arbitrary descriptive name.
Primary DNS Server IP Address	**10.15.9.10**
Underlying Interface	**GROUP_1** This is the Ethernet port group.

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

Parameter	Settings
Application Type	**Media + Control**
IP Address	**63.98.198.35** This is the WAN IP address.
Prefix Length	**16** This is the subnet mask in bits for 255.255.0.0.
Gateway	**63.98.198.33** This is the default gateway - router's IP address.
VLAN ID	**2**
Interface Name	**Public** This is the arbitrary descriptive name of the WAN interface.
Primary DNS Server IP Address	**198.6.1.2**
Secondary DNS Server IP Address	**198.6.1.3**
Underlying Interface	**GROUP_2** This is the Ethernet port group.

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

4.1.2 Step 1b: Configure the Native VLAN ID

The procedure below describes how to configure the Native VLAN ID for the two network interfaces (LAN and WAN).

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

1. Open the Physical Ports Settings page (**Configuration** tab> **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 "Public".

Figure 4-3: Configuring Native VLAN ID

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_0_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Redundant
2	GE_0_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
3	GE_7_1	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
4	GE_7_2	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant
5	GE_7_3	Enable	1	Auto Negotiation	User Port #4	GROUP_3	Active
6	GE_7_4	Enable	1	Auto Negotiation	User Port #5	GROUP_3	Redundant

4.2 Step 2: Verify Software Enabled Features

This section shows how to verify the configuration of the supplied Feature Key. The minimum software version installed on your device must be **SIP_F6.60A.014.007**.

The following features must be enabled on your device:

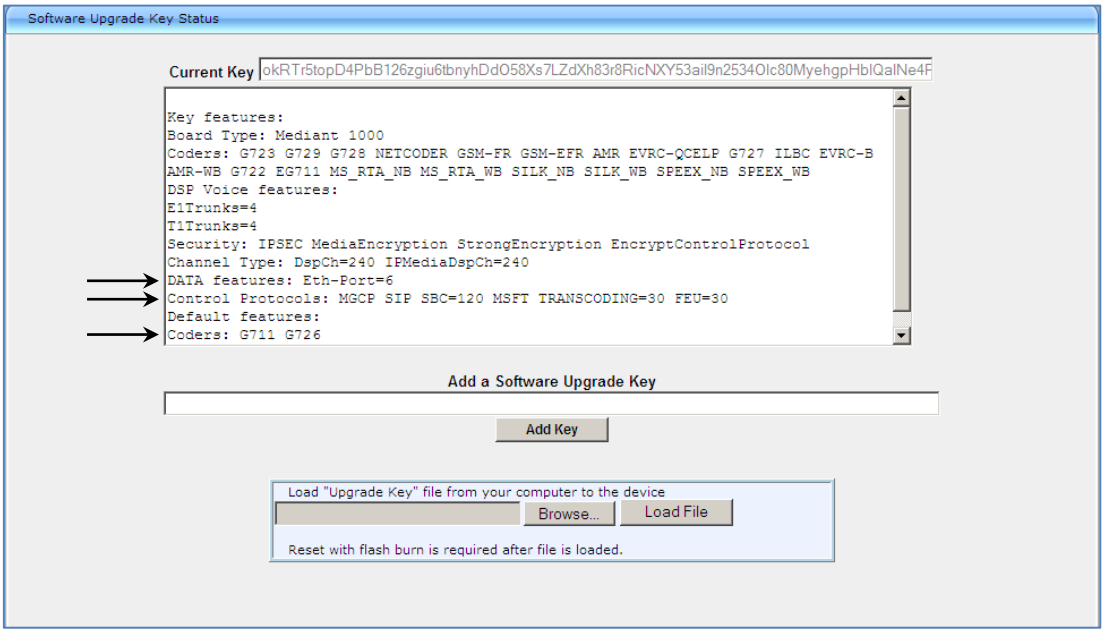
- **Data features**: Eth-Port = 6
- **Coders**: G711
- **Control Protocols**: SIP
- **Microsoft compatible**: MSFT
- **SBC enabled**: SBC=120

Note: If the required features specified above are not configured on the supplied Feature Key, contact your AudioCodes Sales Representative to verify that all required features were ordered and purchased correctly.

➢ **To verify software enabled features:**

1. Open the Software Upgrade Key Status page (**Management** tab > **Software Update** menu > **Software Upgrade Key**). The configured features are displayed.

Figure 4-4: Verifying Software Enabled Features



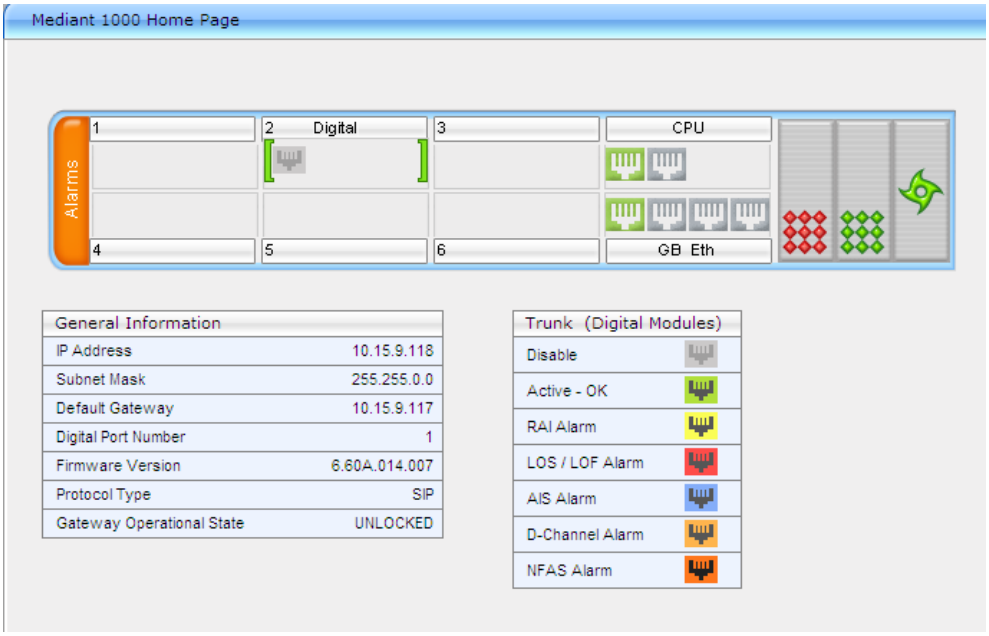
4.3 Step 3: Verify the Firmware Version

This section shows how to verify the firmware version.

➢ **To verify the firmware version:**

- Open the Home page, by using Internet Explorer with the device's IP address in your Web browser's URL field, e.g., http://10.15.9.118.
- Verify that 'Firmware Version' is at least **6.60A.014.007**.

Figure 4-5: Verifying Firmware Version



4.4 Step 4: Enable the SBC Application

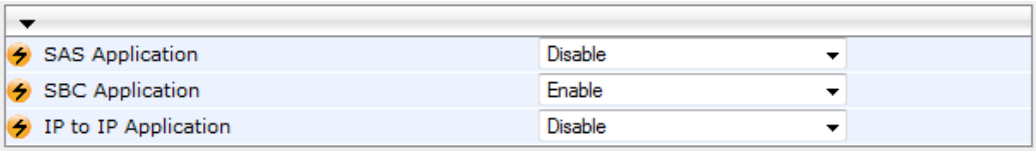
This step describes how to enable the SBC application.

Note: To enable the SBC capabilities on the E-SBC, it must be installed with the SBC Feature Key.

➢ **To enable the SBC application:**

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

Figure 4-6: Enabling the SBC Application



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 4.20 on page 80).

4.5 Step 5: Signaling Routing Domains

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

4.5.1 Step 5a: Configure 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.

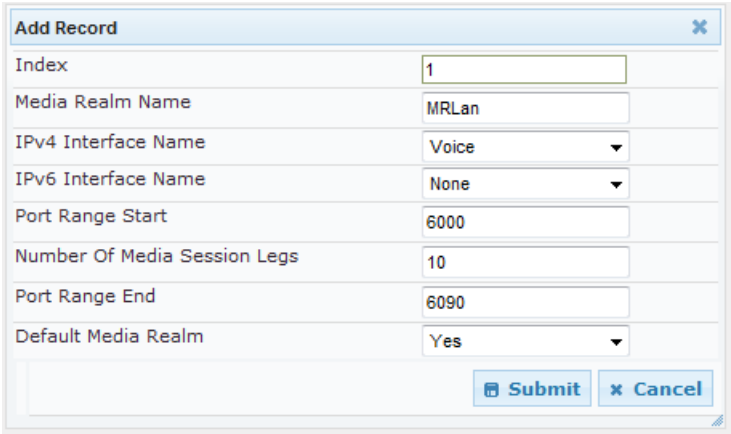
The simplest configuration is to create one Media Realm for internal (LAN) traffic and another for external (WAN) traffic, which is described in the procedure below for our example scenario.

➢ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **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	Settings
Index	**1**
Media Realm Name	**MRLan** This is an arbitrary name.
IPv4 Interface Name	**Voice**
Port Range Start	**6000** This number is the lowest UDP port number used for media on the LAN.
Number of Media Session Legs	**10** This is the number of media sessions that are assigned with the port range.

Figure 4-7: Configuring LAN Media Realms

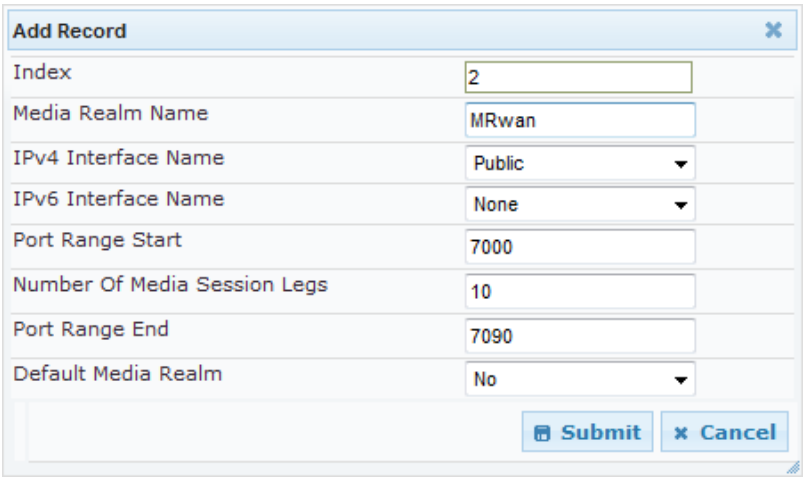


   c. Click **Submit**.

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

Parameter	Settings
Index	**2**
Media Realm Name	**MRwan** This is an arbitrary name.
IPv4 Interface Name	**Public**
Port Range Start	**7000** This number is the lowest UDP port number used for media on the WAN.
Number of Media Session Legs	**10** This is number of media sessions assigned with the port range.

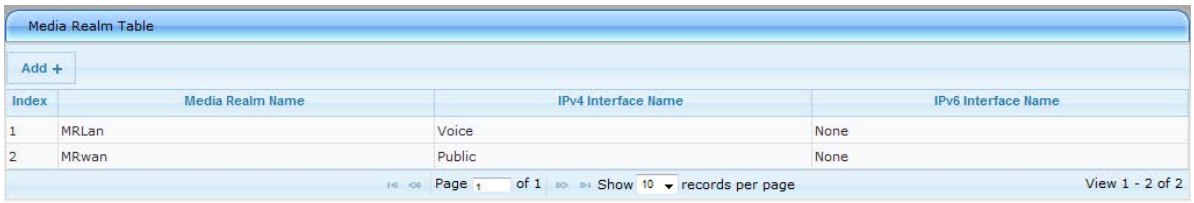
Figure 4-8: Configuring WAN Media Realms



   c. Click **Submit**.

The configured Media Realm table is shown below:

Figure 4-9: Displaying Configured Media Realms



4.5.2 Step 5b: Configure SRDs

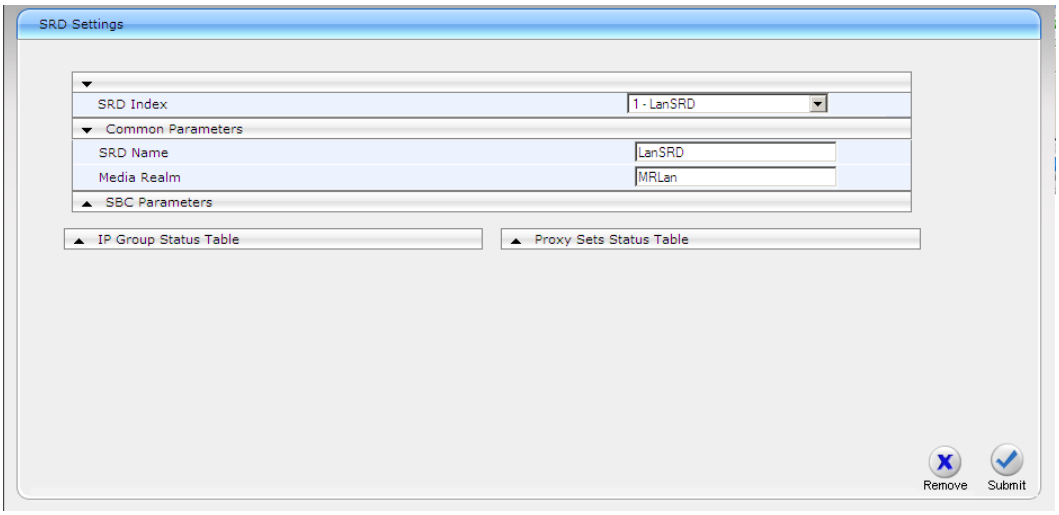
The procedure below describes how to configure the SRDs.

➢ **To configure SRDs:**

1. Open the SRD Table page (**Configuration** tab > **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	Settings
SRD Index	**1**
SRD Name	**LanSRD**
Media Realm	**MRLan** This associates the SRD with a Media Realm**.**

Figure 4-10: Configuring LAN SRDs

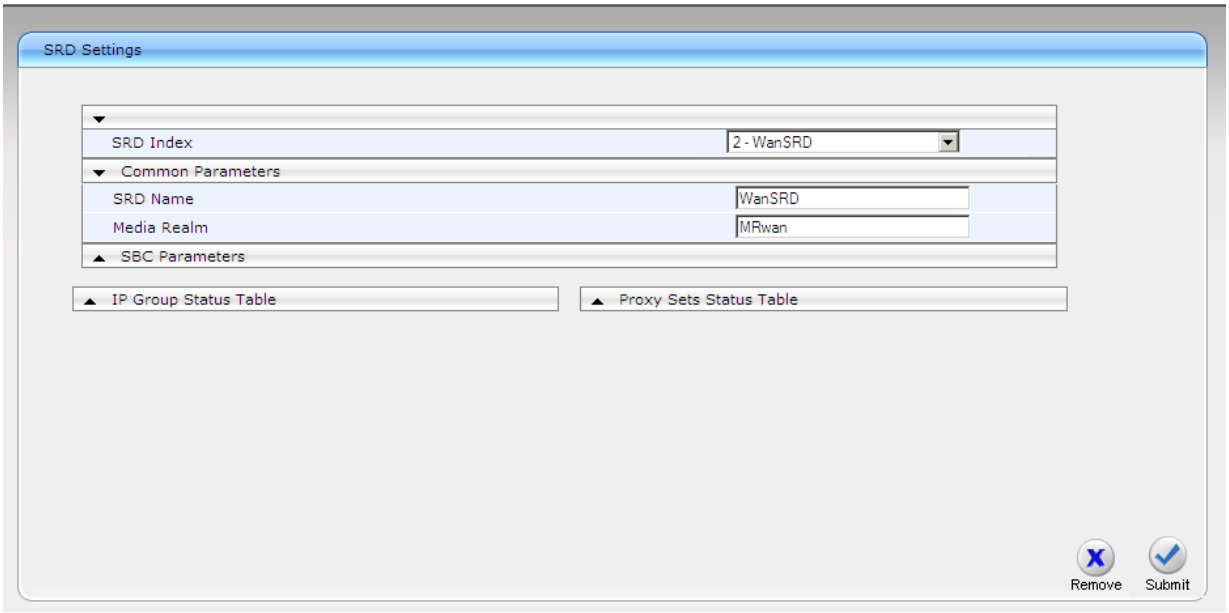


   b. Click **Submit**.

3. Add an SRD for the E-SBC's external interface (toward the Alteva SIP Trunk):
   a. Configure the following parameters:

Parameter	Settings
SRD Index	**2**
SRD Name	**WanSRD**
Media Realm	**MRwan** This associates the SRD with a Media Realm.

Figure 4-11: Configuring WAN SRDs



   b. Click **Submit**.

4.5.3 Step 5c: Configure SIP 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 configure SIP interfaces:**

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

Parameter	Settings
Index	**1**
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**5068 & 5060** UDP is left as default.
SRD	**1**

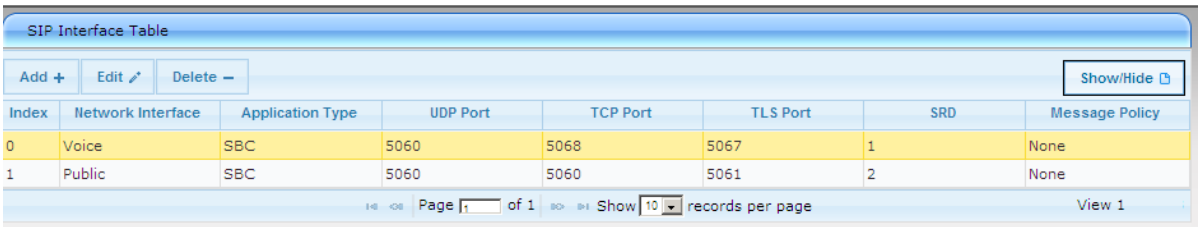
   c. Click **Submit**.
3. Add a SIP interface for the WAN:
   a. Click **Add**.
   b. Configure the following parameters:

Parameter	Settings
Index	**2**
Network Interface	**Public**
Application Type	**SBC**
UDP Port	**5060**
TCP and TLS	Left as default
SRD	**2**

   c. Click **Submit**.

The configured SIP Interface table is shown below:

Figure 4-12: Displaying Configured SIP Interfaces



4.6 Step 6: 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
- Alteva SIP Trunk

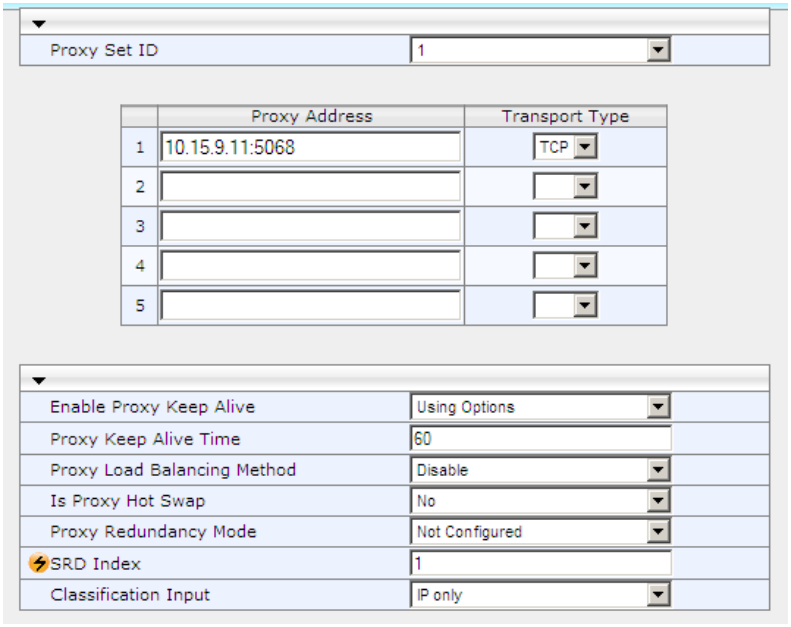
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

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

Parameter	Settings
Proxy Set ID	**1**
Proxy Address	**10.15.9.11:5068 or FE-Lync.Lync.local:5067** This is the Lync Server 2010 SIP Trunking IP address or FQDN and destination port. FQDN is required to support TLS.
Transport Type	**TCP** Select *TLS* when TLS is required. *TLS* is the preferred method.
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Disable** Select *Round Robin* if you are using more than one Proxy Address or the FQDN resolves to more than one IP Address.
Is Proxy Hot Swap	**No** Select *Yes* if you are using more than one Proxy Address or if the FQDN resolves to more than one IP Address.
SRD Index	**1**

Figure 4-13: Configuring Proxy Set for Microsoft Lync Server 2010

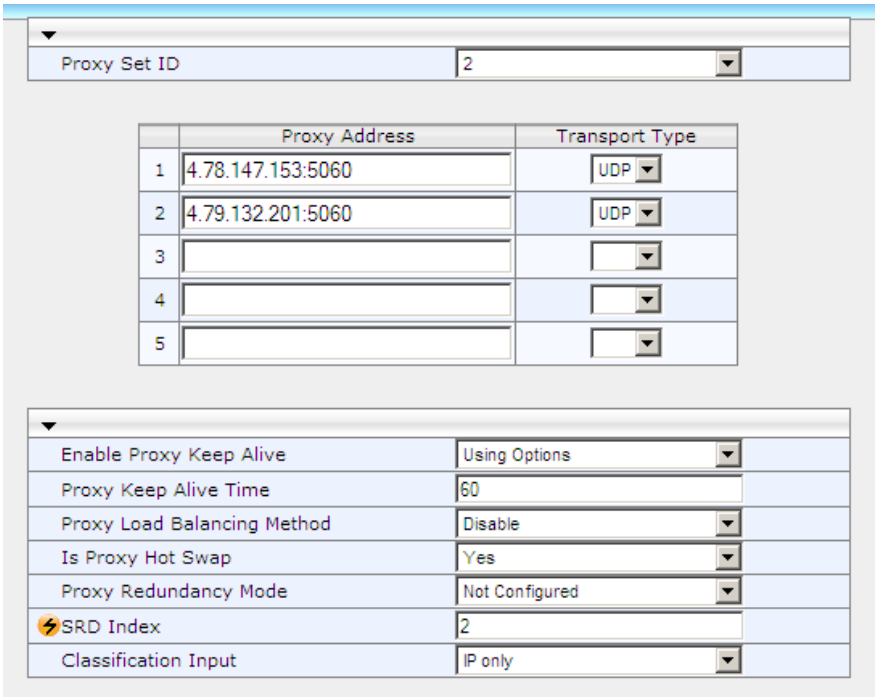


b. Click **Submit**.

3. Add a Proxy Set for the Alteva SIP Trunk:

Parameter	Settings
Proxy Set ID	**2**
Proxy Address	**4.78.147.153:5060** and **4.79.132.201:5060** or **sip.altevaip.com** Alteva IP address or FQDN and destination port
Transport Type	**UDP**
Is Proxy Hot Swap	**Yes**
SRD Index	**2** This enables classification by Proxy Set for this SRD in the IP Group belonging to the Alteva SIP Trunk.

Figure 4-14: Configuring Proxy Set for Alteva SIP Trunk



c. Click **Submit**.

4.7 Step 7: 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
- Alteva SIP Trunk on the WAN

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** tab > **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	Settings
Index	**1**
Type	**Server**
Description	**Lync**
Proxy Set ID	**1**
SIP Group Name	**10.15.9.118**
Media Realm Name	**MRLan**
IP Profile ID	**2**

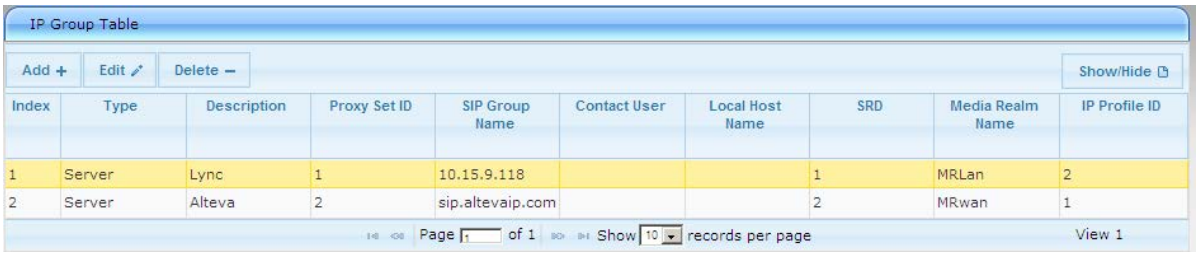
   c. Click **Submit**.
3. Add an IP Group for the Alteva SIP Trunk:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**2**
Type	**Server**
Description	**Alteva**
Proxy Set ID	**2**
SIP Group Name	**sip.altevaip.com**
Media Realm Name	**MRwan**
IP Profile ID	**1**

   c. Click **Submit**.

The configured IP Group table is shown below:

Figure 4-15: Displaying Configured IP Groups



IP Group Table

Add + | Edit | Delete − | Show/Hide

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	Local Host Name	SRD	Media Realm Name	IP Profile ID
1	Server	Lync	1	10.15.9.118			1	MRLan	2
2	Server	Alteva	2	sip.altevaip.com			2	MRwan	1

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

4.8 Step 8: Configure IP Profiles

This step describes how to configure IP Profiles. In our example scenario, the IP Profiles are used to configure the specific associated parameters that enable each of the entities to be supported by the device while allowing interworking of functionality that differ between the two entities - Lync Server 2010 and Alteva SIP Trunk. This enables the interworking between the two separate and distinct architectures. Note that the IP Profiles were assigned to the relevant IP Group in the previous step (see Section 4.7 on page 49).

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

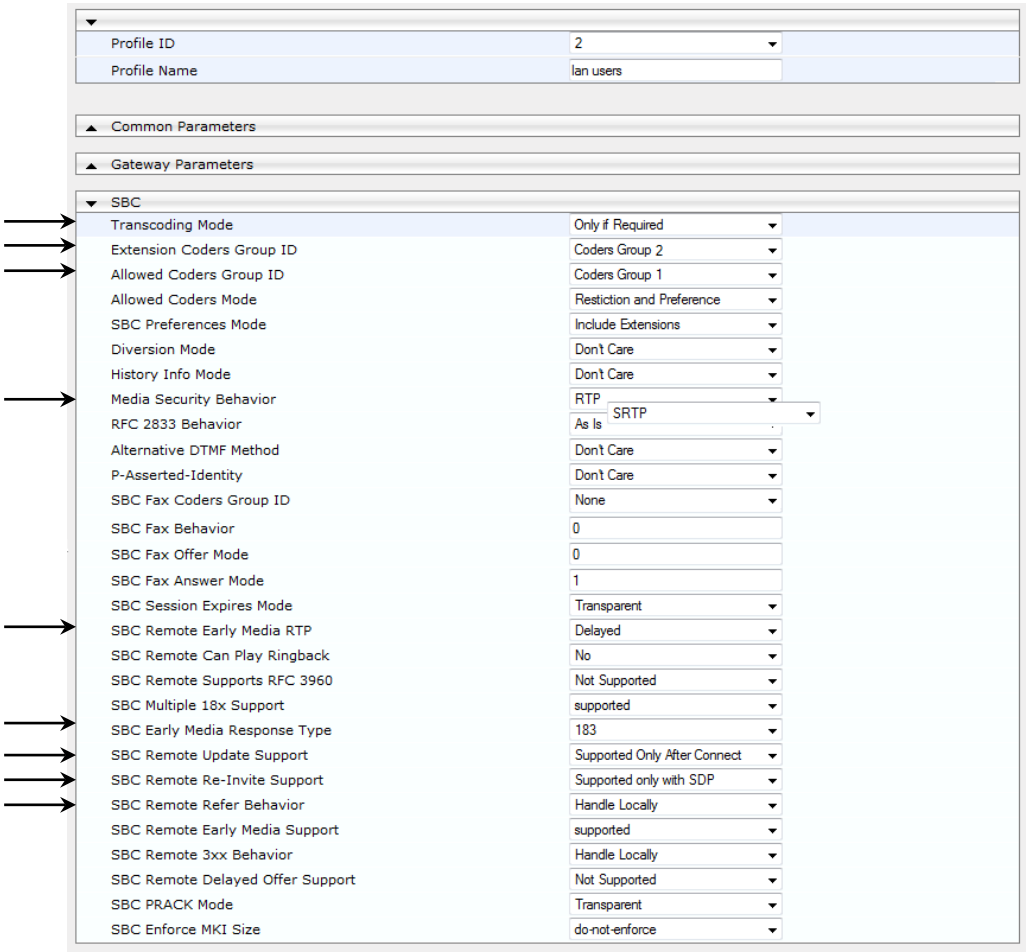
- Microsoft Lync Server 2010 – IP Profile 2
- Alteva SIP trunk – IP Profile 1

➢ **To configure IP Profiles:**

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

Parameter	Settings
Profile ID	**2**
Transcoding Mode	**Only if Required**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 1**
Media Security Behavior	**RTP** The preferred method is to select SRTP when using TLS.
SBC Remote Early Media RTP	**Delayed** This is required when Lync Server 2010 sends a SIP 18x response. It does not send an RTP immediately to the remote side.
SBC Early Media Response Type	**183**
SBC Remote Update Support	**Supported Only After Connect**
SBC Remote Re-Invite Support	**Supported Only With SDP**
SBC Remote Refer Behavior	**Handle Locally**

Figure 4-16: Configuring IP Profile for Lync Server 2010



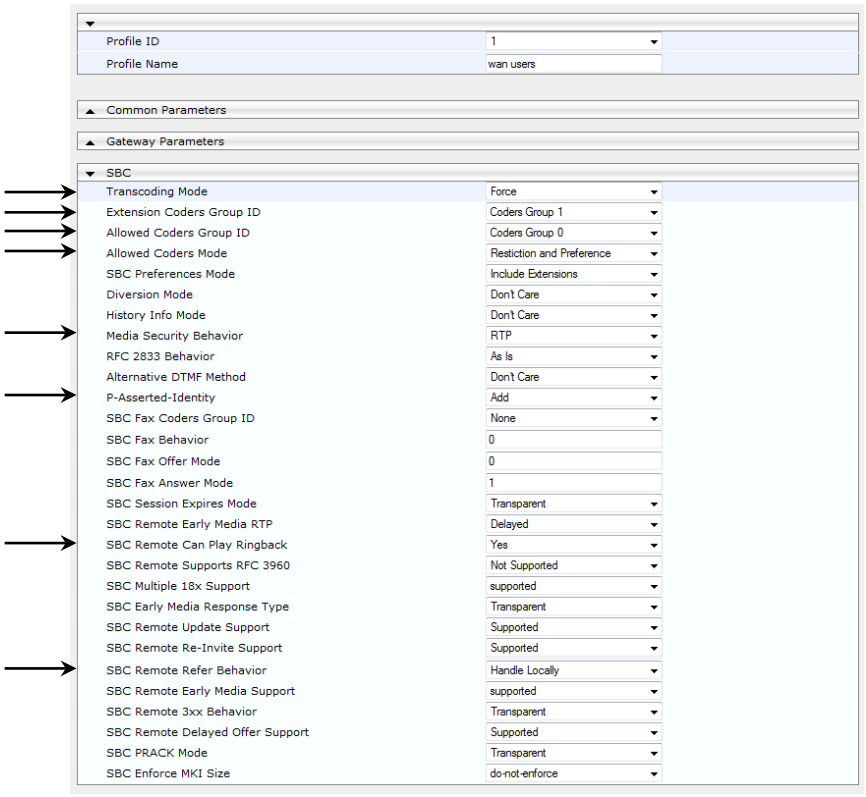
b. Click **Submit**.

3. Add an IP Profile for the Alteva SIP Trunk:

a. Configure the parameters as follows:

Parameter	Settings
Profile ID	**1**
Transcoding Mode	**Force** This is required as the Lync Server 2010 does not send RTP packets immediately when the codec is negotiated on G.711.
Extension Coders Group ID	**Coders Group 1**
Allowed Coders Group ID	**Coders Group 0**
Allowed Coders Mode	**Restrict and Preference**
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** This is required for anonymous calls.
SBC Remote Can Play Ringback	**Yes** This is required as Lync Server 2010 does not provide a Ringback tone for incoming calls, while Alteva does.
SBC Remote Refer Behavior	**Handle Locally** E-SBC handles the incoming REFER request itself without forwarding the REFER. It generates a new INVITE to the alternative destination

Figure 4-17: Configuring IP Profile for Alteva SIP Trunk



b. Click **Submit**.

4.9 Step 9: Configure the Coders Group

This step shows how to configure the voice Coders Group Settings table. Since the Mediation Server supports both G.711U-law and G.711A-law voice coders while Alteva SIP trunk service supports the G.711U-law voice coder, configuration of multiple coder table references for both services are required in utilizing the device to support correct transcoding.

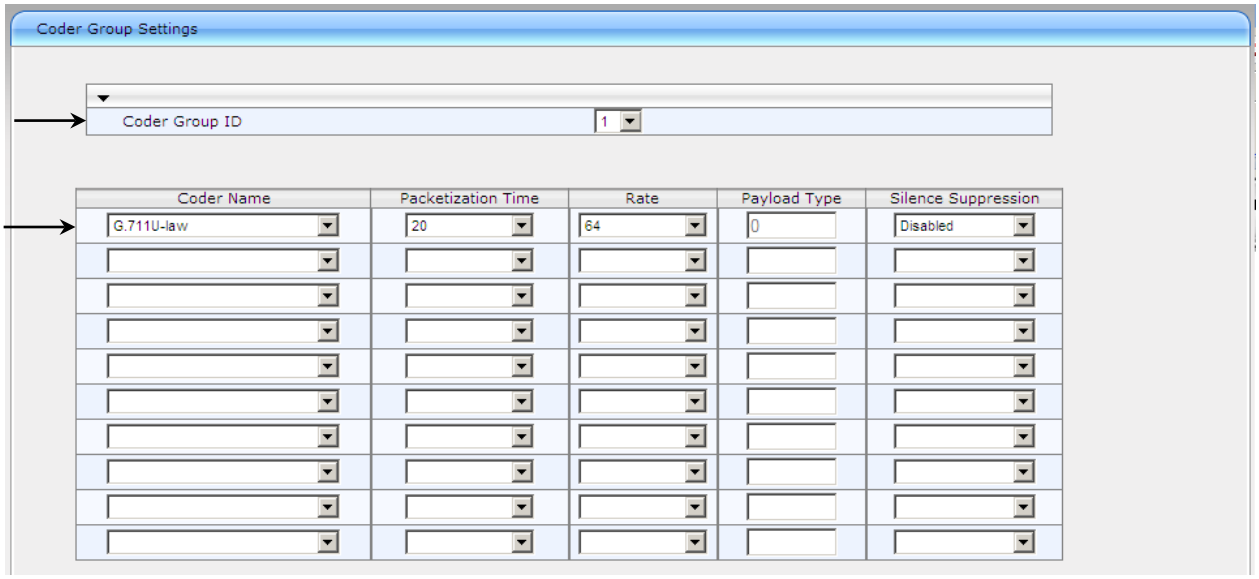
The Coders Group Settings are associated with the following IP Profiles.

- IP Profile Index 1 (see Section 4.7 on page 49) references 'Coder Group 1' (see Figure 4-18) which is associated with the IP Group 2 (see Section 4.7 on page 49).
- IP Profile Index 2 (see under Section 4.7 on page 49) references 'Coder Group 2' as discussed in Section 4.9 (see Figure 4-19), which is associated with IP Group 1(see under Section 4.7 on page 49).

➢ **To configure Coders Group for Alteva SIP Trunk service:**

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

Figure 4-18: Configuring Coders Group – Alteva SIP Trunk Service

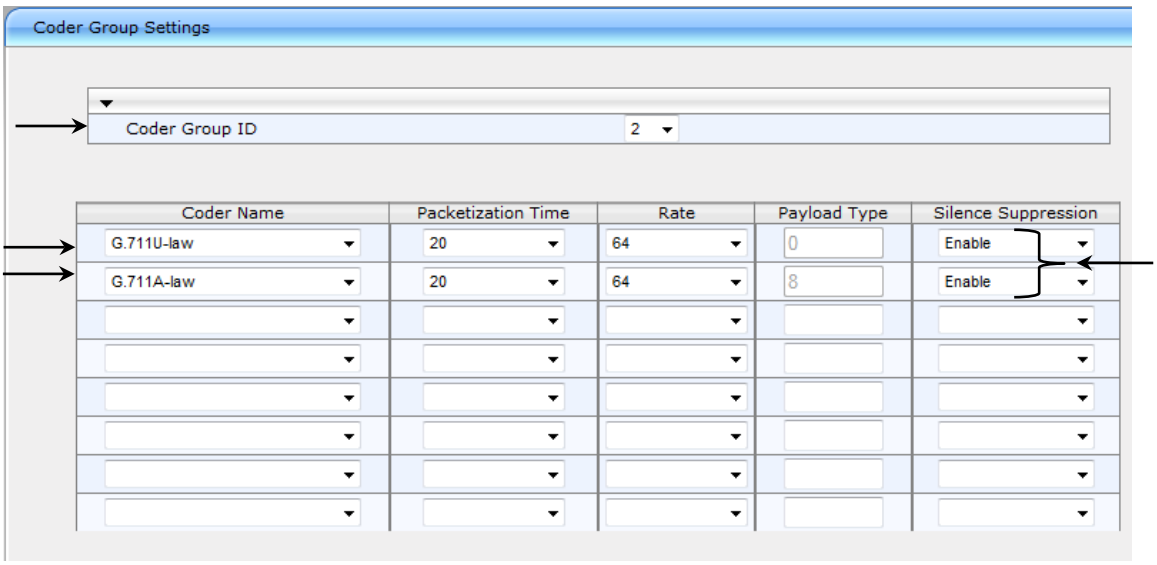


2. From the 'Coder Group ID' drop-down, select Index **1**.
3. From the 'Coder Name' drop-down, select **G.711U-law**.

➢ **To configure Coder Group for Mediation Server usage:**

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

Figure 4-19: Configuring Coder Group - Mediation Server



2. From the 'Coder Group ID' drop-down list, select Index **2**. Index **2** is referenced by the datafill of field 'Coders Group Index' of IP Profile Index '2'. This allows a user to list the allowed vocoders in a supported grouping to be available for utilization. As shown above, Coder Group 2 is declared to support G.711U-law and G.711A-law.
3. Select **G.711U-law** and **G.711A-law** coders.
4. From 'Silence Suppression' drop-down list, select **Enable**.

4.10 Step 10: Configure the SBC Allowed Coders Group

This step shows how to configure the SBC Allowed (Voice) Coders Group Settings table. Since the Mediation Server supports G.711 A-law *and* G.711 U-law voice coders, while Alteva SIP trunk service supports G.711 U-law voice coders, configuration of multiple coder table references for both services are required in utilizing the device to support correct transcoding.

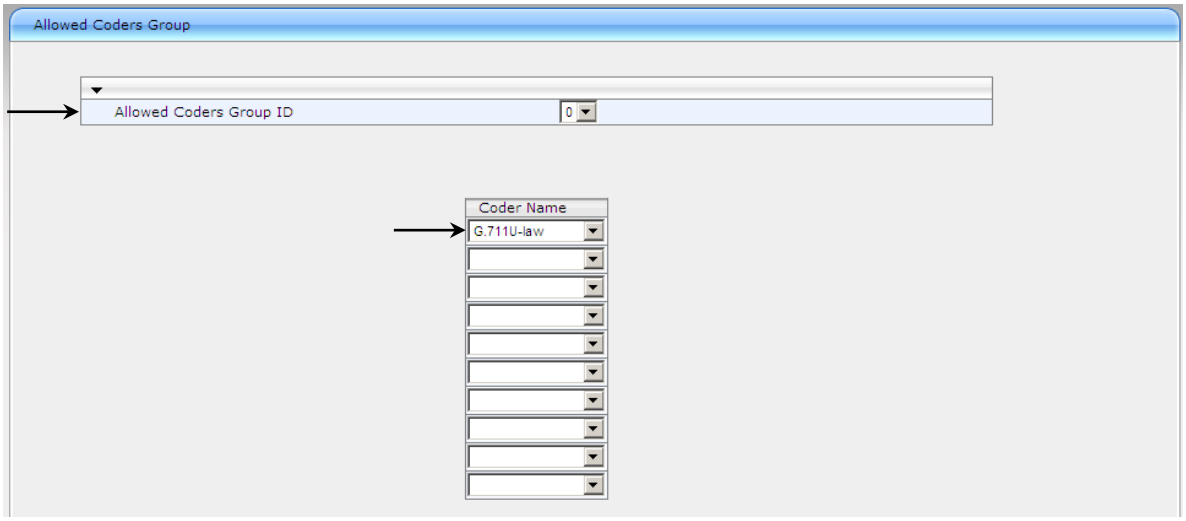
The Coder table is associated with the following IP Profiles.

- IP Profile Index 2 (under Section 4.7 on page 49) references Allowed Coder Group ID 'Coder Group 1' (see Figure 4-18) which is associated with interworking with the Microsoft Lync environment.
- IP Profile Index 1 (under Section 4.7 on page 49) references Allowed Coder Group ID 'Coder Group 0' (see Figure 4-19), which is associated with interworking with Alteva SIP trunk service.

➢ **To configure the Allowed Coders Group for Alteva SIP Trunk service:**

1. Open the Coders Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).

Figure 4-20: Configuring Allowed Coders Group – Alteva SIP Trunk

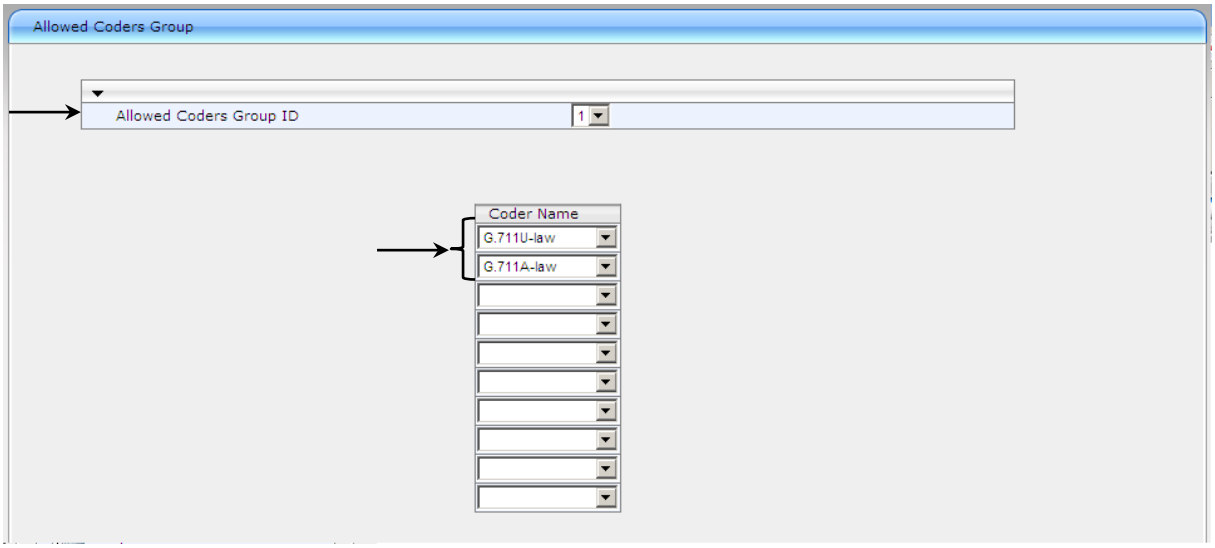


2. From the 'Allowed Coders Group ID' drop-down, select Index **0**.
3. Select **G.711U-law** coder.

➢ **To configure the Allowed Coders Group for Mediation Server usage:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).

Figure 4-21: Configuring Allowed Coders Group Setting - Mediation Server



2. From the 'Allowed Coders Group ID' drop-down list, select Index **1**.
3. Select **G.711U-law** and **G.711A-law** coders.

4.11 Step 11: 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.

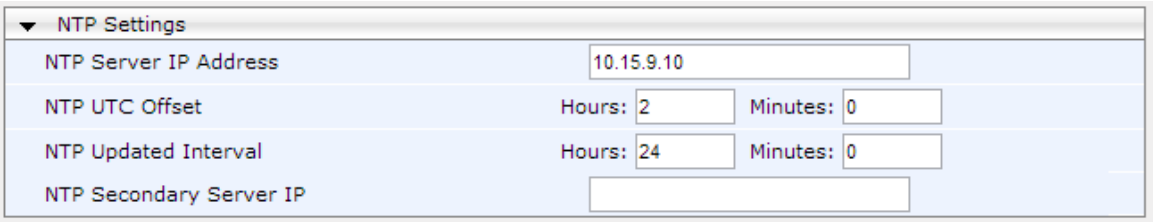
4.11.1 Step 11a: Configure the NTP Server Address

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** tab > **System** > **Application Settings**).
2. In the 'NTP Server IP Address' field, enter the IP address of the NTP server (e.g., "10.15.9.10").

Figure 4-22: Configuring NTP Server Address



3. Click **Submit**.

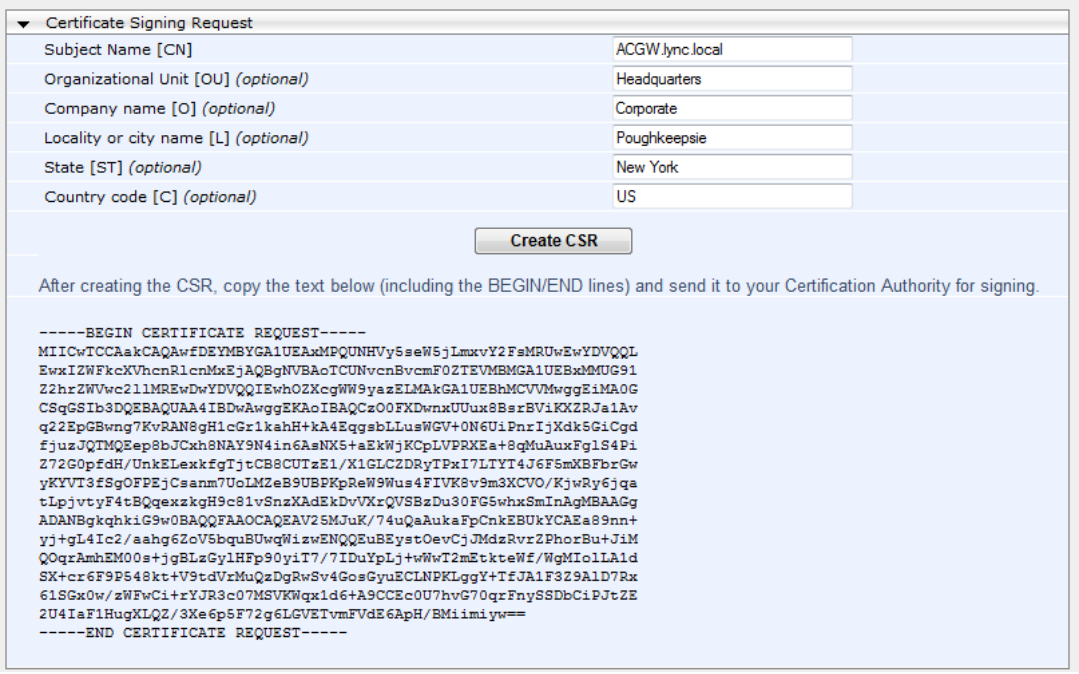
4.11.2 Step 11b: Configure a Certificate

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 MS Lync 2010 environment.

➢ **To configure a certificate:**

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

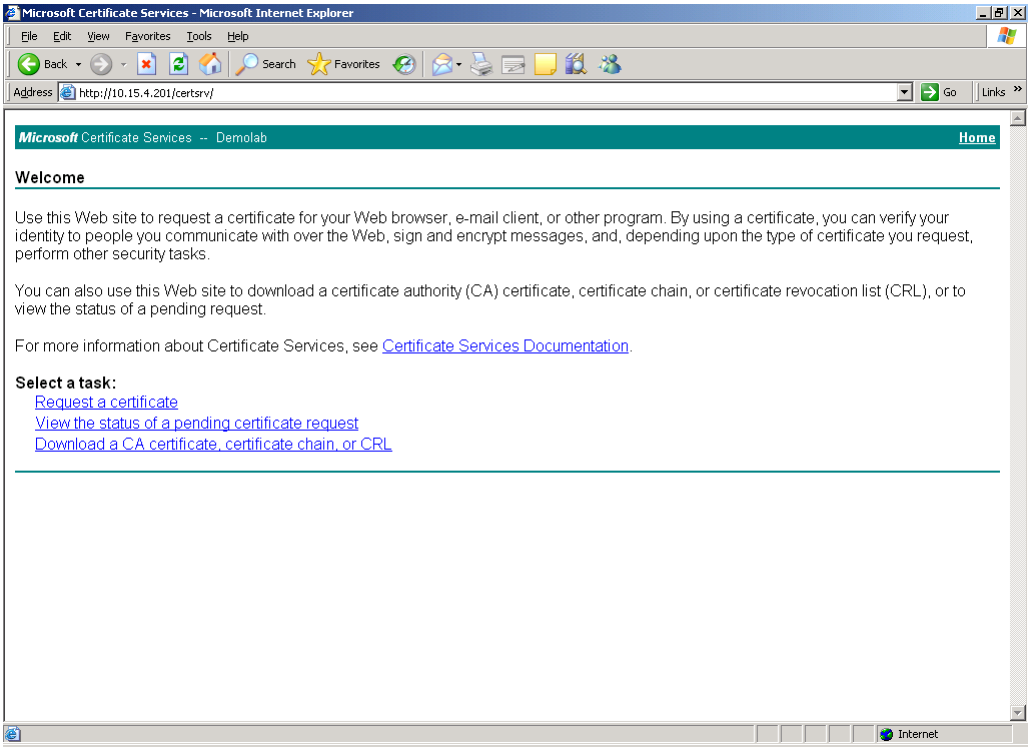
Figure 4-23: Configuring a Certificate



2. In the Subject Name field, enter the media gateway name (e.g., "ACGW.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*.

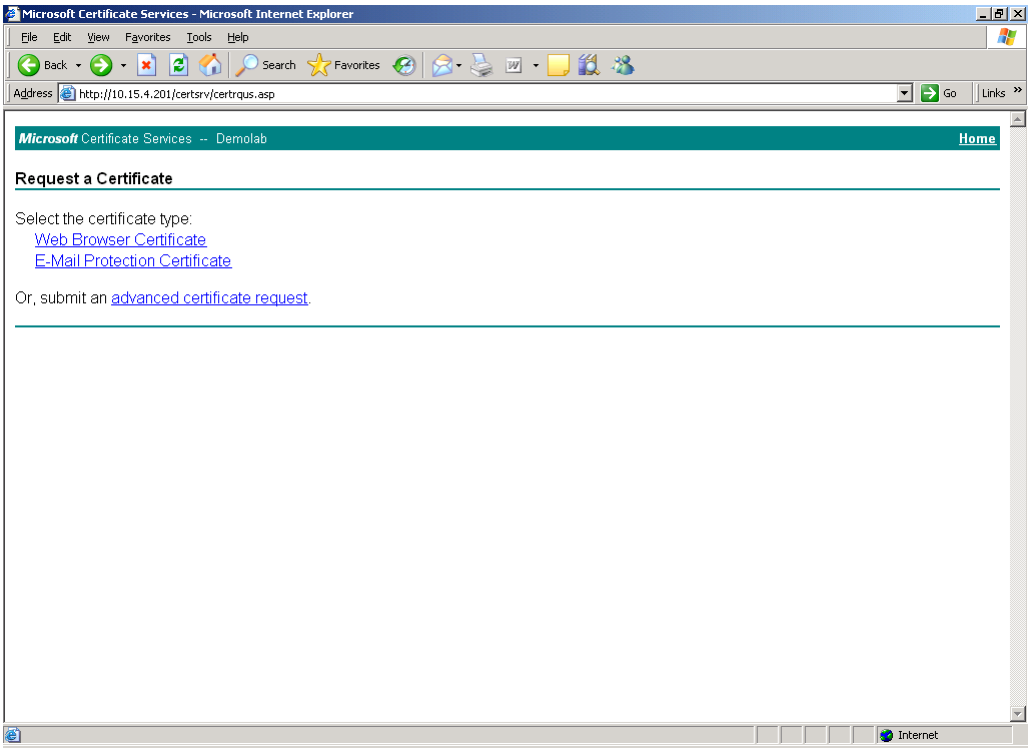
5. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 4-24: Navigating to Microsoft Certificate Services Web Site



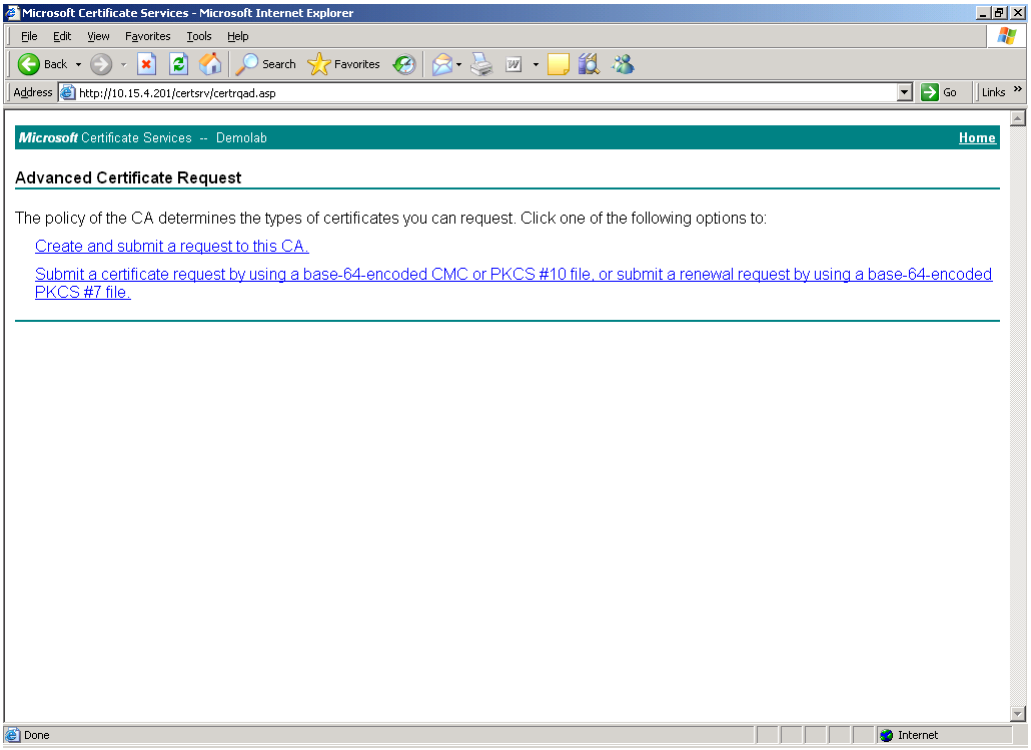
6. Click **Request a certificate**.

Figure 4-25: Requesting a Certificate



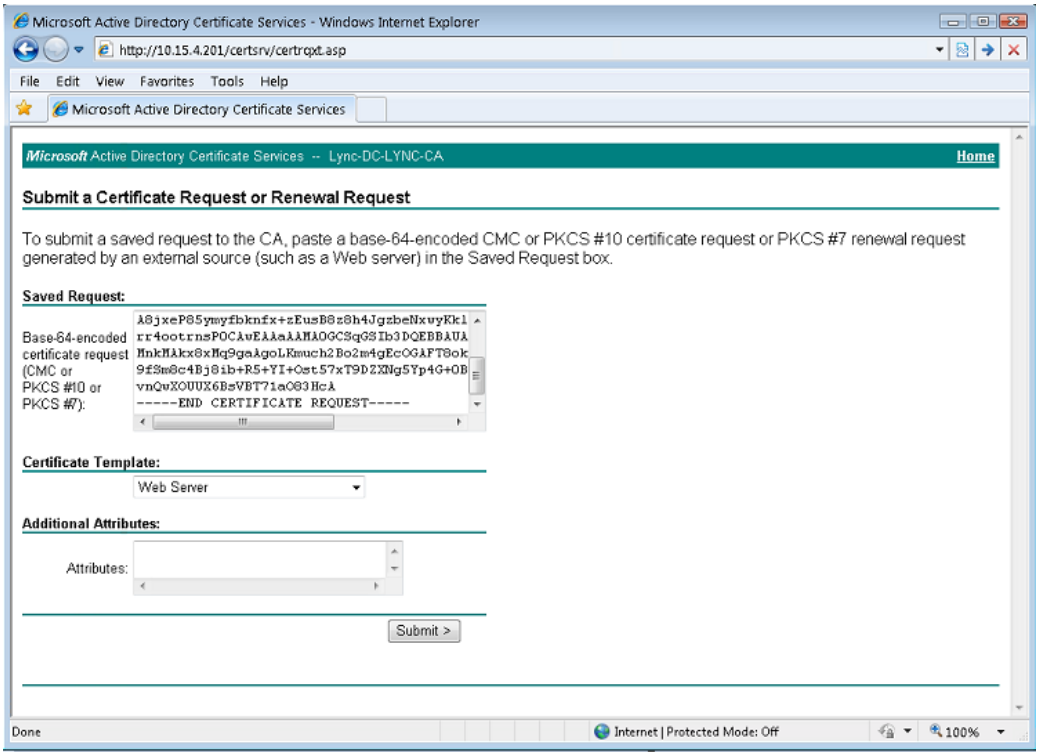
7. Click **advanced certificate request**, and then click **Next**.

Figure 4-26: Submitting Advanced Certificate Request



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

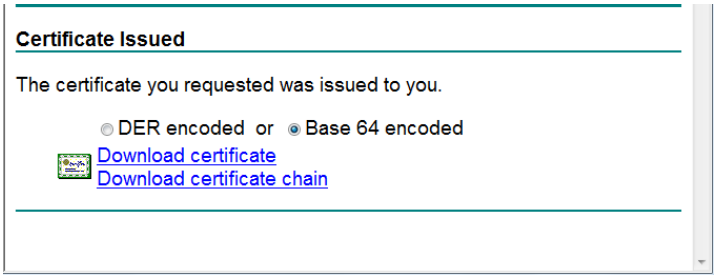
Figure 4-27: Submitting Certificate Request or Renewal Request



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**.

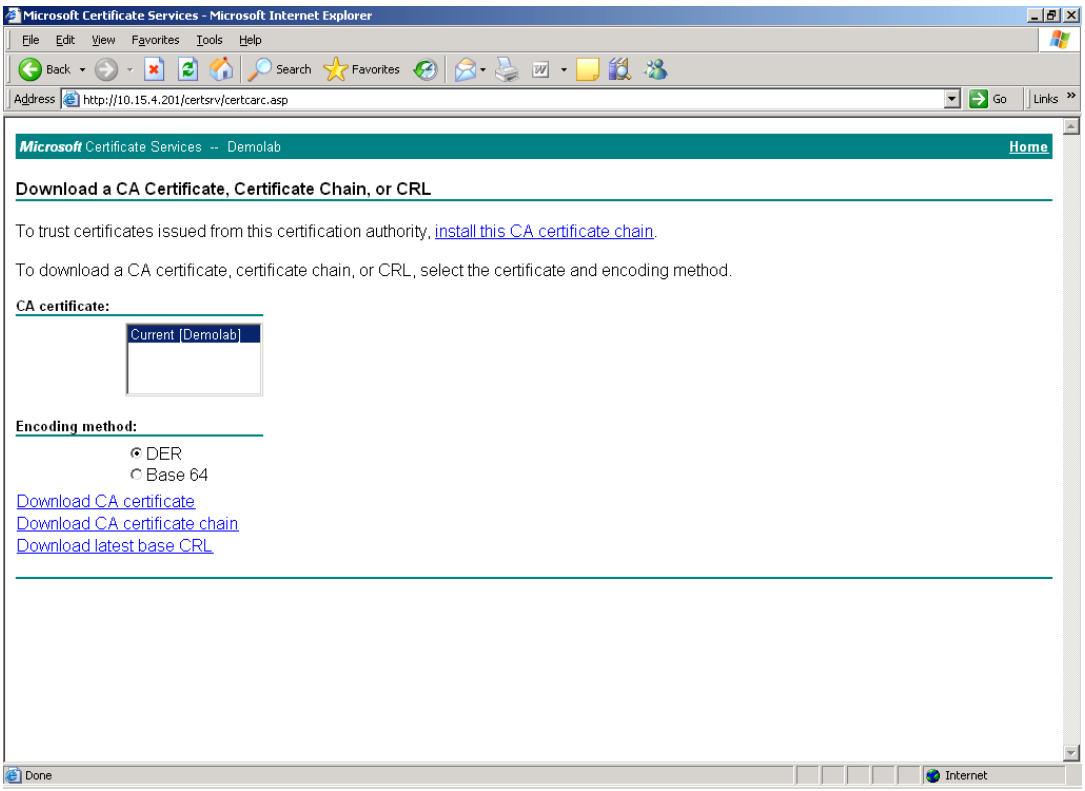
11. Click **Submit**.

Figure 4-28: Displaying 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**.

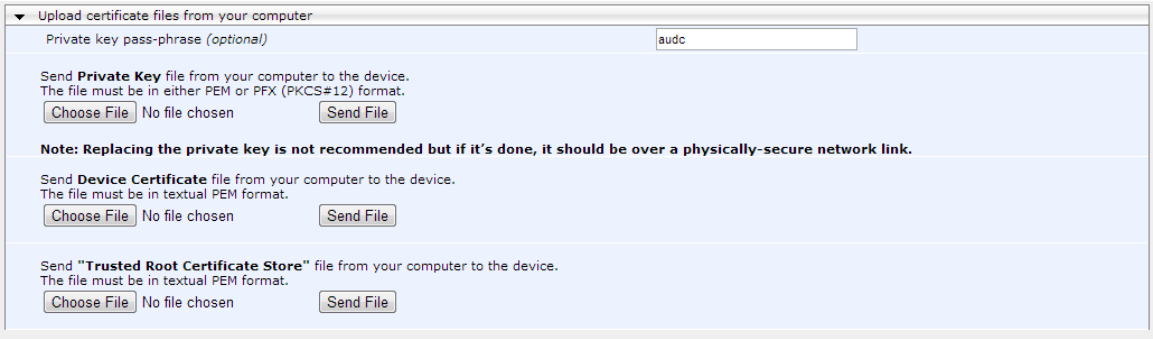
Figure 4-29: Downloading a CA Certificate



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 4-30: Uploading Certificates



20. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.20 on page 80).

4.12 Step 12: Configure Media Security

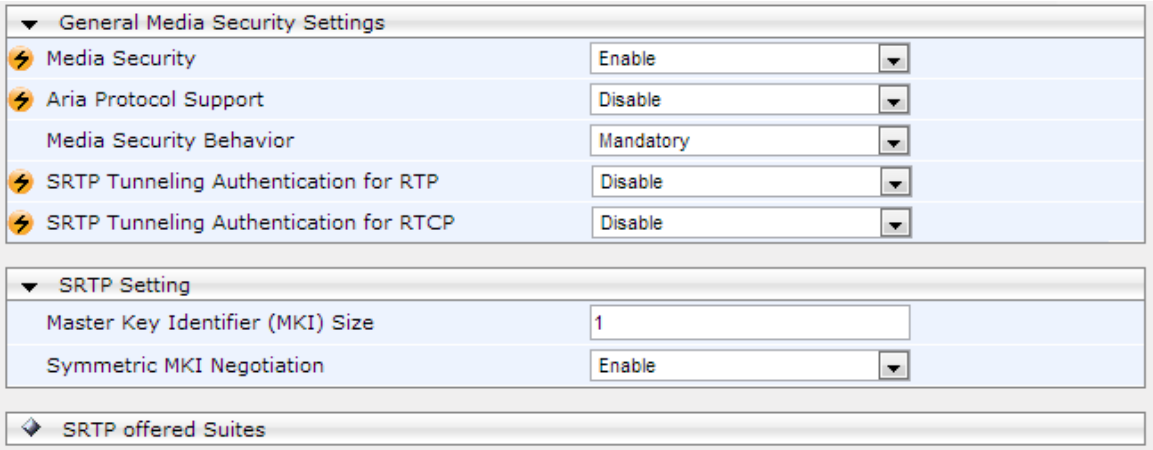
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use Secure Real-Time Transport Protocol (SRTP), you need to configure the E-SBC to operate in the same manner.

Note: SRTP was enabled for Lync Server 2010 when you added an IP Profile for Lync Server 2010 (see Section 4.8 on page 51).

➢ **To configure media security:**

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

Figure 4-31: Configuring Media Security



2. Configure the parameters as follows:

Parameter	Settings
Media Security	**Enable**
Media Security Behavior	Select one of the following: ▪ **Mandatory** (if Mediation Server is configured to *SRTP Required*) ▪ **Preferable** Single media (if Mediation Server is configured to *SRTP Optional*)
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 4.20 on page 80).

4.13 Step 13: 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.

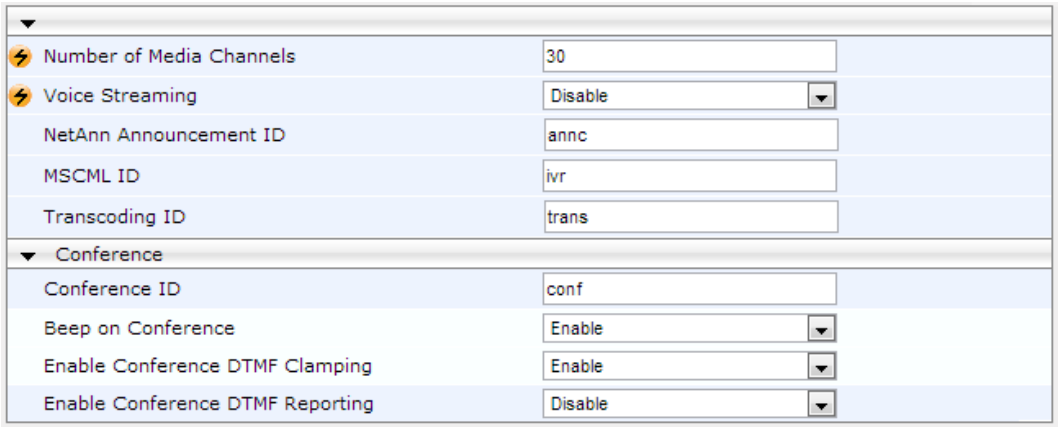
This is required for coder transcoding, where two IP media channels are used per call.

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

➢ **To configure IP media:**

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

Figure 4-32: Configuring IP Media



2. In the 'Number of Media Channels' field, enter "30".
3. Click **Submit**.

4.14 Step 14: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules (which are done 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 Alteva SIP Trunk (WAN):

- Calls from LAN to WAN
- Calls from WAN to LAN

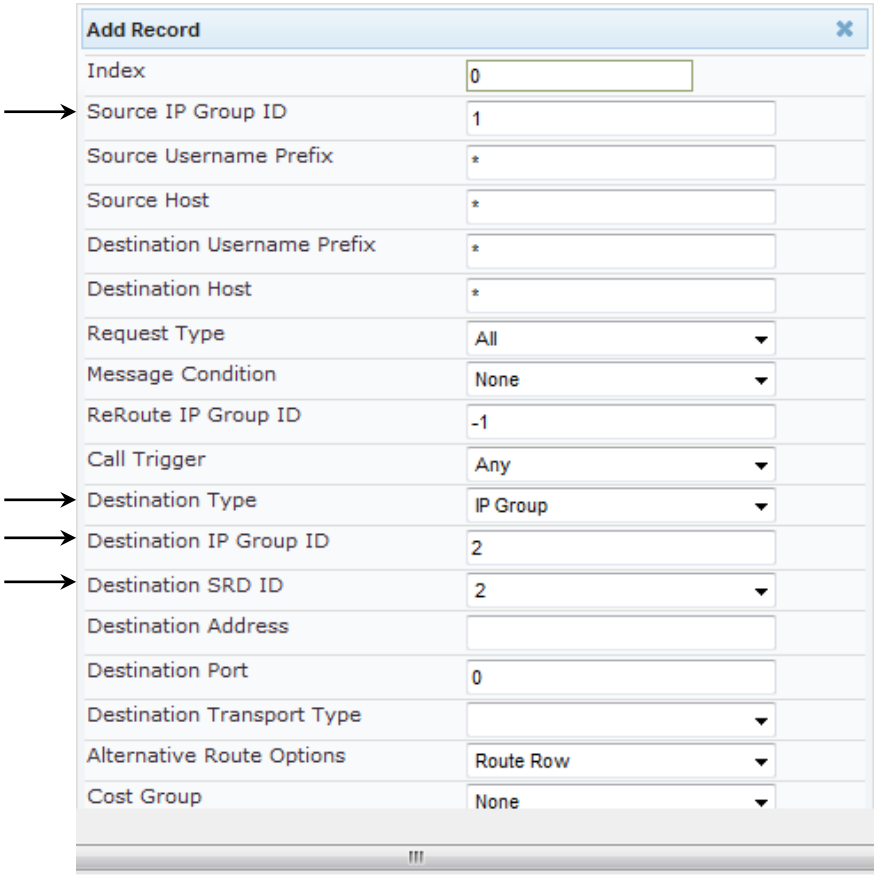
The routing rules use IP Groups to denote the source and destination of the call. IP Group ID 1 was assigned to Lync Server 2010, and IP Group ID 2 to Alteva SIP Trunk as shown in Section 4.7 on page 49.

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

1. Open the IP2IP Routing Table page (**Configuration** > **VoIP** > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to route calls from LAN to WAN:
   a. Click **Add**.
   b. Configure the parameters as follows:

Parameter	Settings
Index	**0**
Source IP Group ID	**1**
Destination Type	**IP Group**
Destination IP Group ID	**2**
Destination SRD ID	**2**

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

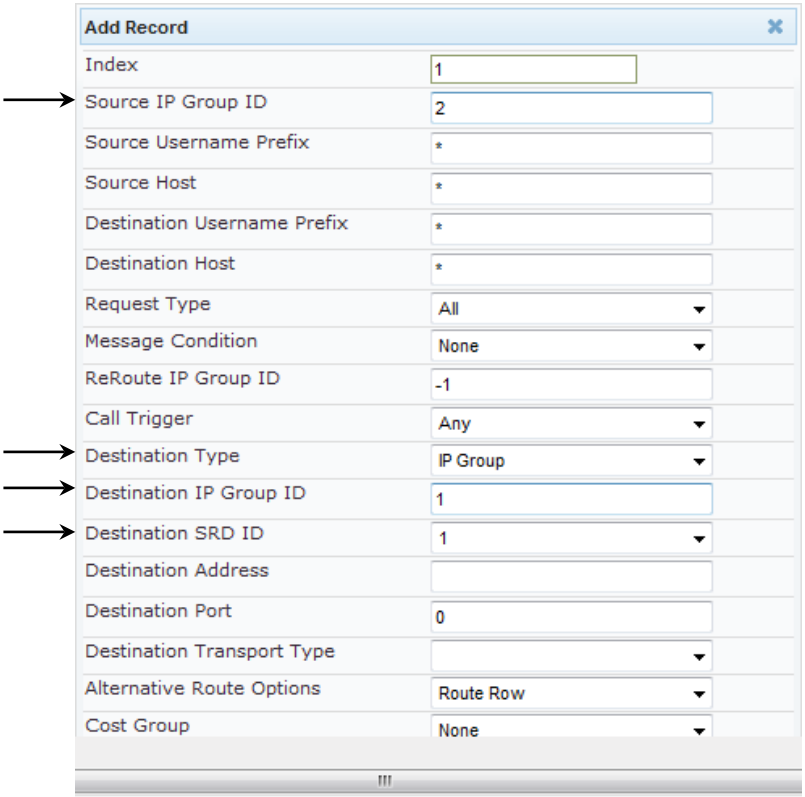


c. Click **Submit**.

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

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

Figure 4-34: Configuring IP-to-IP Routing Rules for WAN to LAN



   c. Click **Submit**.

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

Figure 4-35: Displaying Configured IP-to-IP Routing Rules

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

4.15 Step 15: Configure IP-to-IP Inbound Manipulation Rules

This step describes how to configure inbound 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. As configured in Section 4.7 on page 49, IP Group ID 1 was assigned to Lync Server 2010 and IP Group ID 2 to the Alteva SIP Trunk.

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

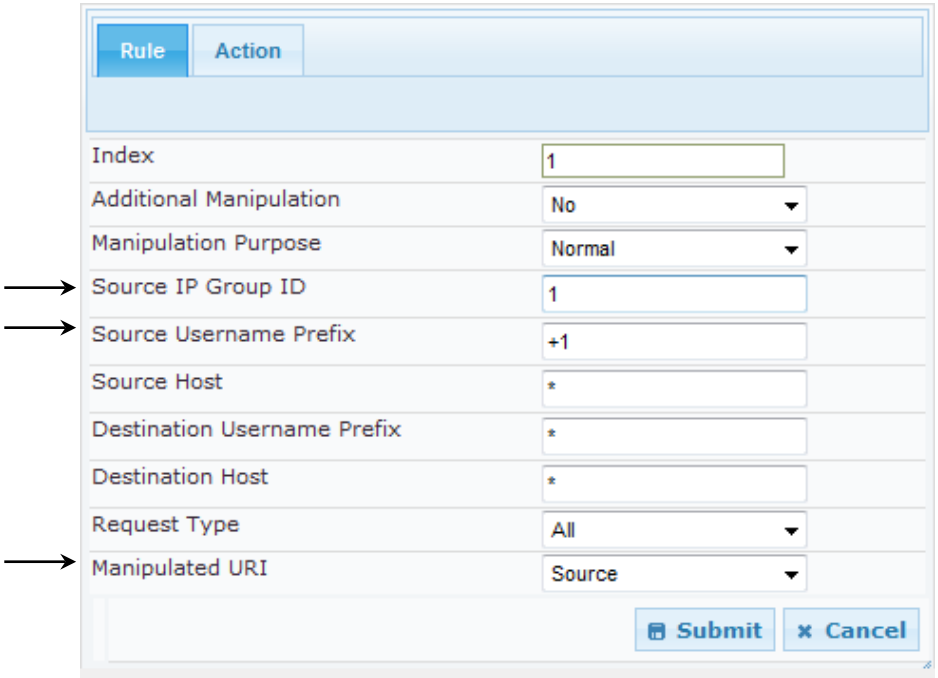
The procedure below provides an example of configuring a manipulation rule that removes the plus sign "+1" from the source number for calls to IP Group 2 (Alteva SIP Trunk) originated from IP Group 1 (i.e., Lync Server 2010), when the source number is prefixed with a ("+1").

➢ **To configure IP-to-IP Inbound Manipulation Rules:**

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

Parameter	Settings
Index	**1**
Source IP Group ID	**1**
Source Username Prefix	**+1**
Manipulated URI	**Source**

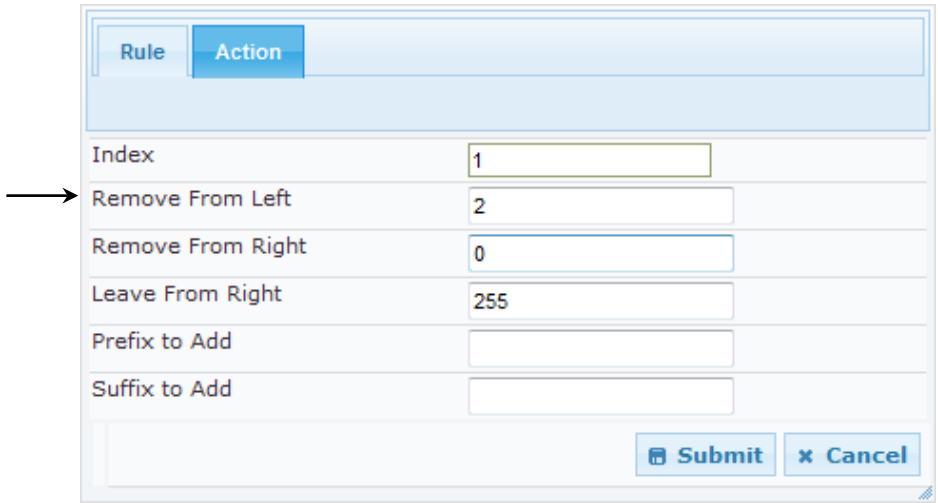
Figure 4-36: Configuring IP-to-IP Inbound Manipulation Rules – Rule Tab



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

Parameter	Settings
Remove From Left	**2**

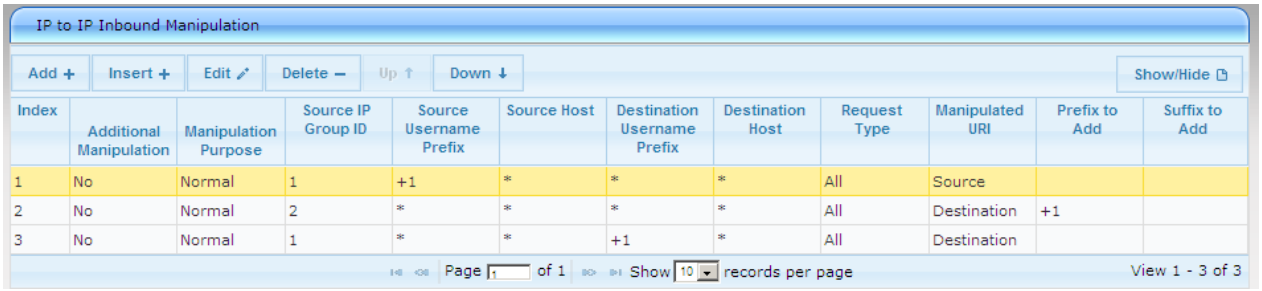
Figure 4-37: Configuring IP-to-IP Inbound Manipulation Rules - Action Tab



5. Click **Submit**.

The IP to IP Inbound table displayed below includes three manipulation rules for calls between IP Group 1 (i.e., Lync Server 2010) and IP Group 2 (i.e., Alteva SIP Trunk):

Figure 4-38: Displaying IP to IP Inbound Manipulation Rules



Rule Index	Description
1	Calls received from IP Group 1 and that have any source prefix (+1), remove 2 left digits (“+1”) from the source number.
2	Calls received from IP Group 2 add a prefix of “+1” to the destination number.
3	Calls received from IP Group 1 and that have a destination prefix (+1), remove 2 left digits (“+1”) from the destination number.

4.16 Step 16: Configure IP-to-IP Outbound Manipulation Rules

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. As configured in Section 4.7 on page 49, IP Group ID 1 was assigned to Lync Server 2010 and IP Group ID 2 to the Alteva SIP Trunk.

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

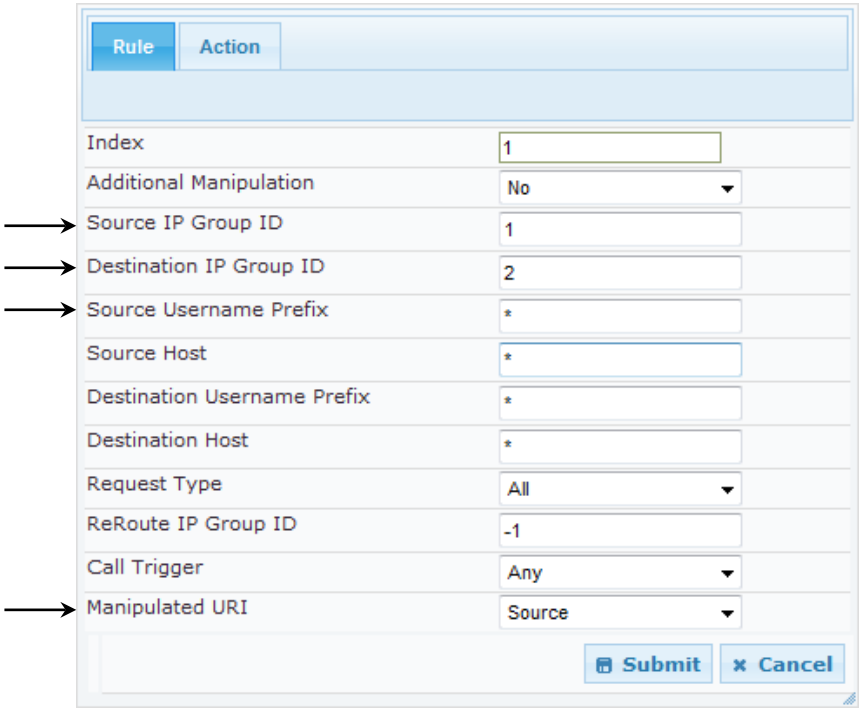
The procedure below provides an example of configuring a manipulation rule that changes the presentation of the source number to a restricted state for all calls to IP Group 2 (Alteva SIP Trunk) originated from IP Group 1 (i.e., Lync Server 2010). This rule can be further enhanced for setting a specific Source number rather than all by populating the Source Username Prefix with the appropriate source number to be manipulated.

➢ **To configure IP-to-IP Outbound Manipulation Rules:**

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	Settings
Index	**1**
Source IP Group ID	**2**
Destination IP Group ID	**1**
Source Username Prefix	***** This will manipulate all calls.
Manipulated URI	**Source**

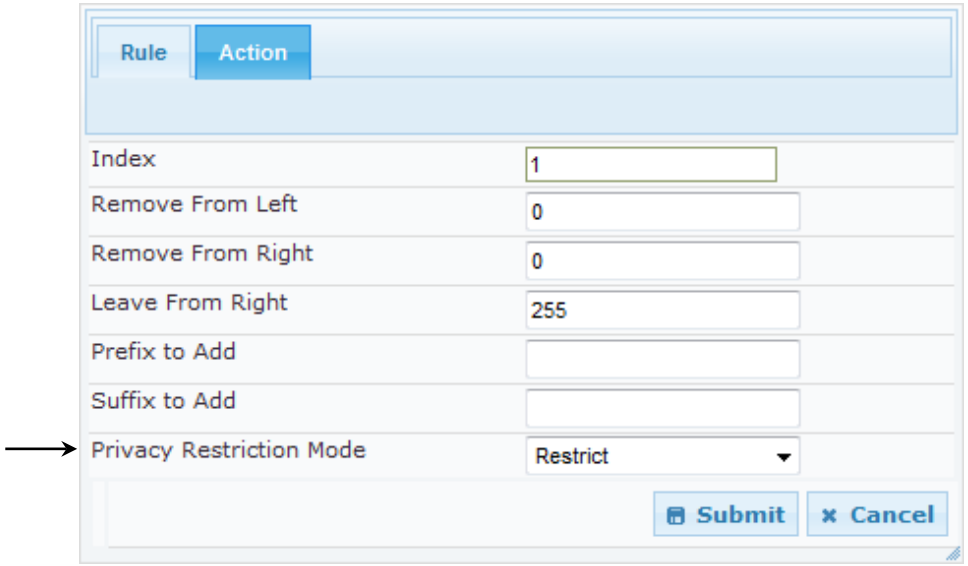
Figure 4-40: Configuring IP-to-IP Outbound Manipulation Rules – Rule Tab



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

Parameter	Settings
Privacy Restriction Mode	**Restrict**

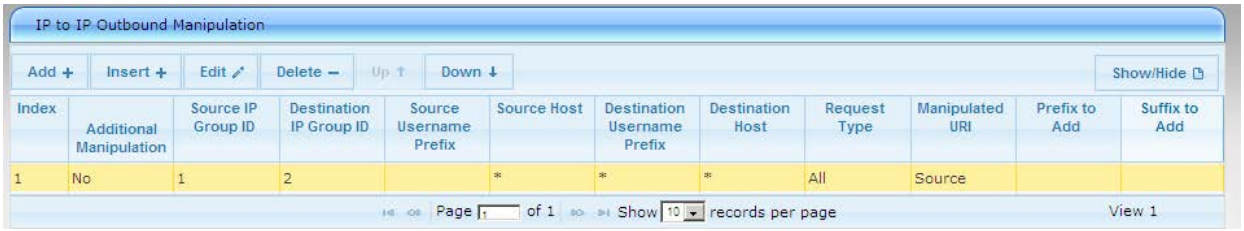
Figure 4-41: Configuring IP-to-IP Outbound Manipulation Rules - Action Tab



5. Click **Submit**.

The IP to IP Outbound table displayed below includes the manipulation rule for calls between IP Group 1 (i.e., Lync Server 2010) and IP Group 2 (i.e., Alteva SIP Trunk):

Figure 4-42: Displaying Configured IP to IP Outbound Manipulation Rules



Rule Index	Description
1	Calls received from IP Group 1 and destined to IP Group 2 will have the Privacy Restriction Mode set to Restrict.

4.17 Step 17: Configure SIP 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 and grouped together for the same SIP message by the usage of the Manipulation Set ID. 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.

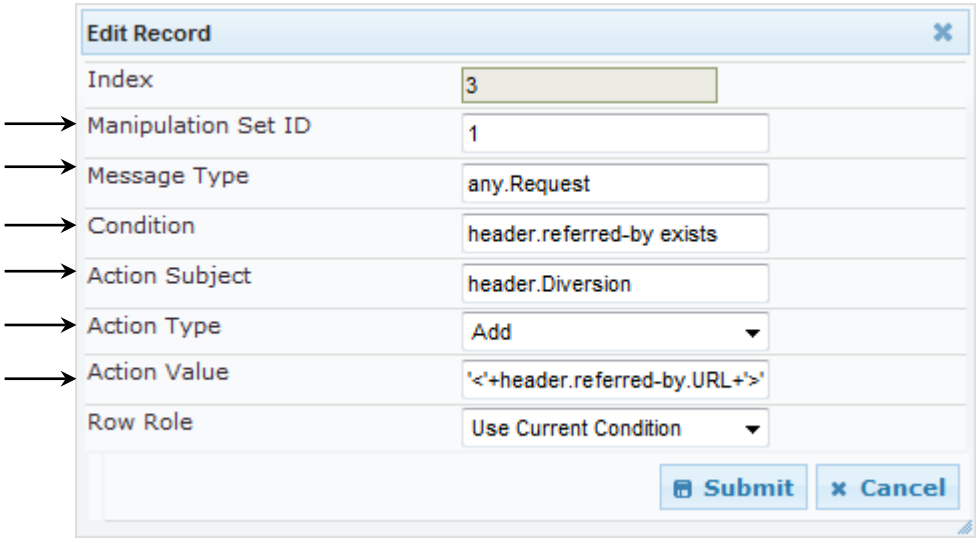
In our example scenario, SIP message manipulation is required for messages sent to the Alteva SIP Trunk (IP Group 2) for the Call Transfer / Forward feature of Lync Server 2010.

➢ **To configure SIP message manipulation rules for Index 3:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 1:

Rule Index	Setting
Index	**3**
Manipulation Set ID	**1**
Message Type	**any.Request**
Condition	**header.referred-by exists**
Action Subject	**header.Diversion**
Action Type	**Add**
Action Value	**'<'+header.referred-by.URL+'>'**

Figure 4-39: Configuring SIP Message Manipulation – Index 3

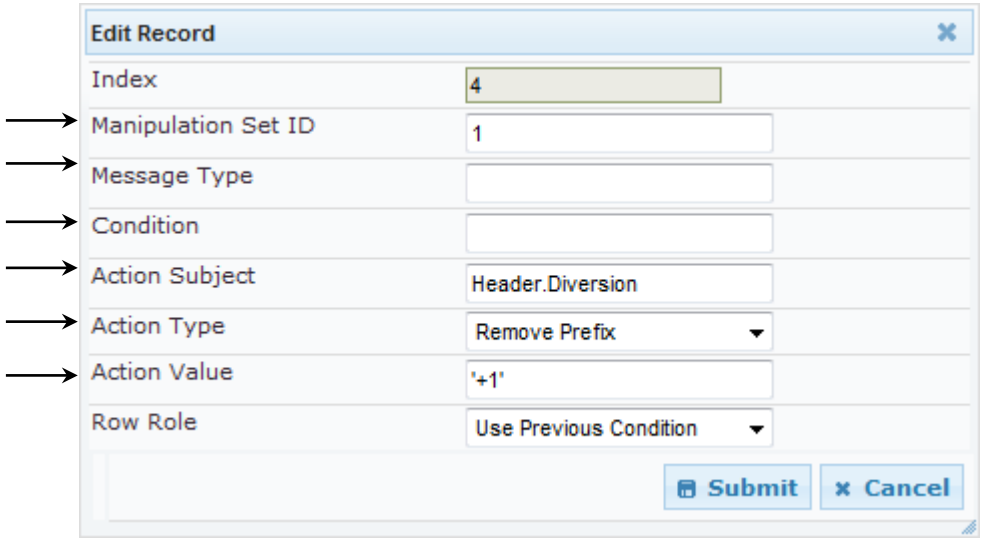


➢ **To configure SIP message manipulation rules for Index 4:**

1. Open the Message Manipulations page (**Configuration** > **VoIP** > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rules for Manipulation Set ID 1:

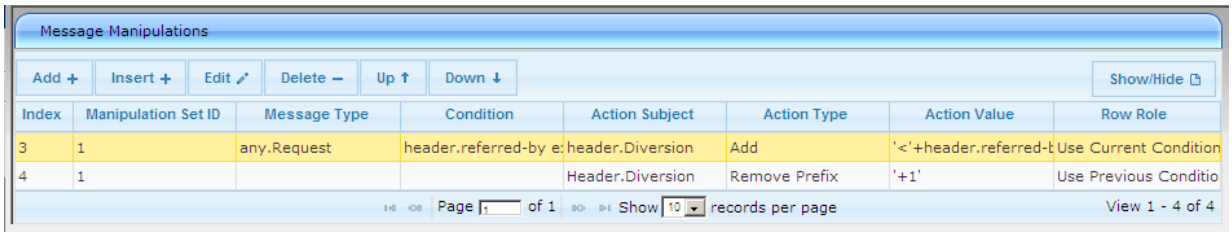
Rule Index	Setting
Index	**4**
Manipulation Set ID	**1**
Message Type	
Condition	
Action Subject	**Header.Diversion**
Action Type	**Remove Prefix**
Action Value	**'+1'**
Row Role	**Use Previous Condition**

Figure 4-40: Configuring SIP Message Manipulation – Index 4



The figure below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set ID 1) which are executed for messages received from the Lync Server 2010 (IP Group 1) prior to being sent to the Alteva SIP Trunk service (IP Group 2). Refer to the User's Manual for further details regarding the full capabilities of header manipulation. Manipulation Set IDs are indexed and utilized from within the IP Group table.

Figure 4-43: Configuring SIP Message Manipulation Rules

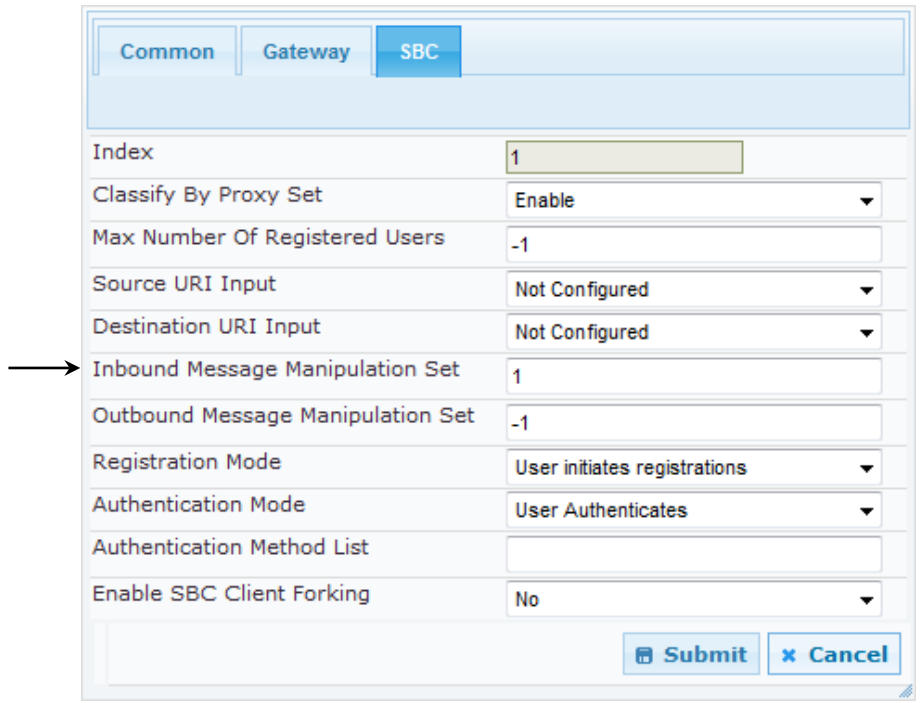


3. Review the newly created manipulation rules for Manipulation Set ID 1:

Rule Index	Description
3	SIP messages that contain a Referred-By header and are destined to the Alteva SIP Trunk are modified as follows: A Diversion header added with the user part provided from the Referred-By header.
4	If the manipulation rule Index 3(above) is executed, then the following rule is also done on the same SIP message: the prefix "+1" is removed from the user part of the Diversion header.

4. Assign the Manipulation Set ID 1 to IP Group 1:
   a. Open the IP Group Table page (**Configuration** > **VoIP** > **Control 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 4-44: Configuring SIP Message Manipulation Rules to IP Group 1



   e. Click **Submit**.

4.18 Step 18: Configure SIP Registration Accounts

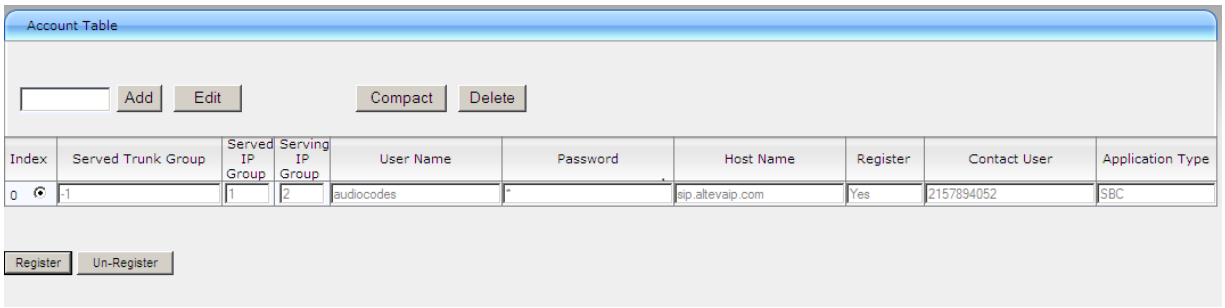
This step describes how to configure SIP registration accounts (in the Account table). This is required so that the E-SBC can register with the Alteva SIP Trunk on behalf of Lync Server 2010. The Alteva SIP Trunk requires registration and authentication to provide service.

In this example, the Served IP Group is Lync Server 2010 (IP Group 1) and the Serving IP Group is Alteva SIP Trunk (IP Group 2).

➢ **To configure SIP registration accounts:**

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

Figure 4-46: Configuring SIP Registration Accounts



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

Parameter	Settings
Served IP Group	**1** This is the Lync Server 2010.
Serving IP Group	**2** This is the Alteva SIP Trunk.
Username	Set username as provided by Alteva
Password	Set password as provided by Alteva
Host Name	**sip.altevaip.com**
Register	**Yes**
Contact User	**2157894052** Set to trunk main line.
Application Type	**SBC**

4. Click **Apply**.

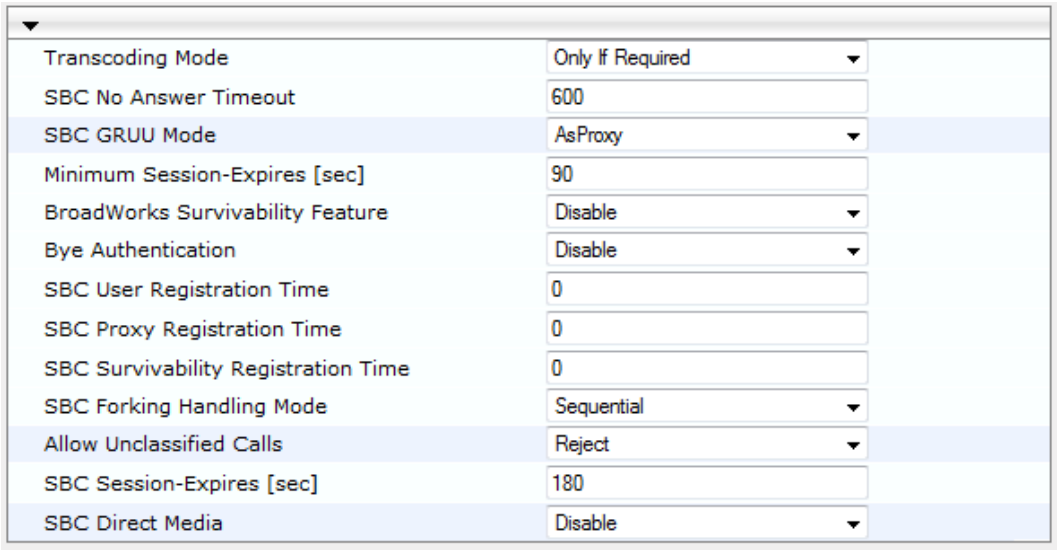
4.19 Step 19: Configure Forking Mode

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 a SIP 18x response 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 SIP 18x responses with SDP, or plays a ringback tone if a SIP 180 response without SDP is received. It's mandatory to set this field for the Lync Server 2010 environment.

➢ **To configure call forking mode:**

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

Figure 4-48: Configuring Call Forking Mode



3. Click **Submit**.

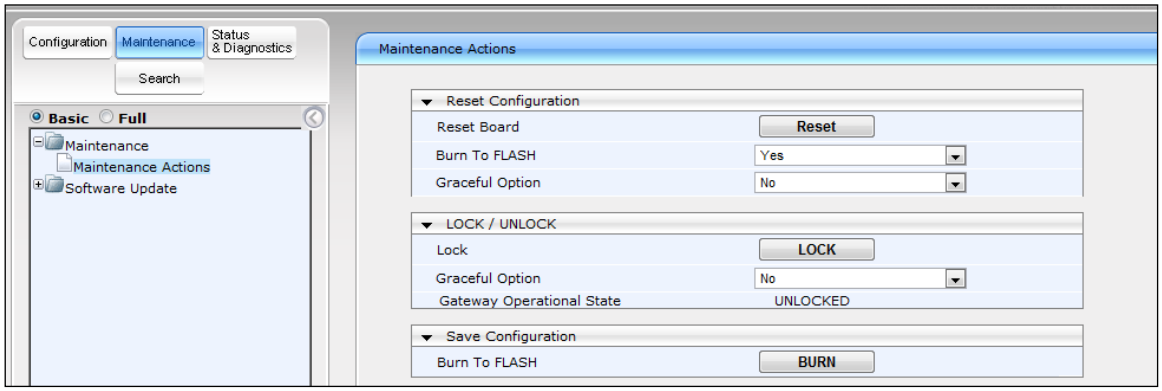
4.20 Step 20: Reset the E-SBC

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 reset the E-SBC:**

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

Figure 4-49: Resetting the E-SBC



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

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: 2967088
;Slot Number: 1
;Software Version: 6.60A.014.007
;DSP Software Version: 620AE3 => 660.03
;Board IP Address: 10.15.9.118
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.9.117
;Ram size: 512M   Flash size: 64M
;Num of DSP Cores: 8  Num DSP Channels: 40
;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
;DSP Voice features: ;E1Trunks=4 ;T1Trunks=4 ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Channel
Type: DspCh=240 IPMediaDspCh=240 ;DATA features: Eth-Port=6
;Control Protocols: MGCP SIP SBC=120 MSFT TRANSCODING=30 FEU=30
;Default features:;Coders: G711 G726;

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


[SYSTEM Params]


[BSP Params]

PCMLawSelect = 3
```

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



[SIP Params]
MEDIACHANNELS = 30
MEDIASECURITYBEHAVIOUR = 1
DNSQUERYTYPE = 1
ENABLESBCAPPLICATION = 1
ENABLESYMMETRICMKI = 1
SBCFORKINGHANDLINGMODE = 1

[SCTP Params]


[VXML 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_0_1", 1, 1, 4, "User Port #0",
"GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 1, 4, "User Port #1",
"GROUP_1", "Redundant";
PhysicalPortsTable 2 = "GE_7_1", 1, 2, 4, "User Port #2",
"GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_7_2", 1, 2, 4, "User Port #3",
"GROUP_2", "Redundant";
PhysicalPortsTable 4 = "GE_7_3", 1, 1, 4, "User Port #4",
"GROUP_3", "Active";
PhysicalPortsTable 5 = "GE_7_4", 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_0_1, GE_0_2;
EtherGroupTable 1 = "GROUP_2", 2, GE_7_1, GE_7_2;
EtherGroupTable 2 = "GROUP_3", 2, GE_7_3, GE_7_4;

[ \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, 10.15.9.118, 16, 10.15.9.117, 1,
"Voice", 10.15.9.10, 0.0.0.0, GROUP_1;
InterfaceTable 1 = 5, 10, 63.98.198.35, 16, 63.98.198.33, 2,
"Public", 198.6.1.2, 198.6.1.3, 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", Public, , 7000, 10, 7090, 0;

[ \CpMediaRealm ]


[ SRD ]
```

```
FORMAT SRD_Index = SRD_Name, SRD_MediaRealm,
SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers,
SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "LanSRD", "MRLan", 0, 0, -1, 1;
SRD 2 = "WanSRD", "MRwan", 0, 0, -1, 1;

[ \SRD ]




[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "10.15.9.11:5068", 1, 1;
ProxyIp 1 = "4.78.147.153:5060", 0, 2;
ProxyIp 2 = "4.79.132.201:5060", 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 1 = "wan users", 1, 1, 2, 10, 10, 46, 40, 0, 0, 0, 0, 2,
0, 0, 0, 1, -1, 1, 0, 2, -1, 0, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, 0,
2, 2, 0, 0, 0, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 0, 2, 1,
0, 3, 0, 1, 2, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0;
IpProfile 2 = "lan users", 1, 2, 2, 10, 10, 46, 40, 0, 0, 0, 0, 2,
0, 0, 0, 1, -1, 1, 0, 3, -1, 0, 4, -1, 1, 1, 0, 0, "", 2, 0, 1, 1,
2, 1, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 1, 1,
0, 3, 2, 1, 2, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0;

[ \IpProfile ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode;
ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;
ProxySet 1 = 1, 60, 0, 0, 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, "10.15.9.118", "", 0, -1, 0, 0, -1, 1,
"MRLan", 1, 2, -1, 1, -1, 1, 1, "", 0, -1, -1, "";
IPGroup 2 = 0, "Alteva", 2, "sip.altevaip.com", "", 0, -1, 0, 0, -
1, 2, "MRwan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "";

[ \IPGroup ]
```

```
[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroup, Account_ServingIPGroup, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, 1, 2, "audiocodes", *, "sip.altevaip.com", 1,
"2157894052", 2;

[ \Account ]


[ IP2IPRouting ]

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

[ \IP2IPRouting ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort,
SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD,
SIPInterface_MessagePolicy, SIPInterface_TLSMutualAuthentication;
SIPInterface 0 = "Voice", 2, 5060, 5068, 5067, 1, , -1;
SIPInterface 1 = "Public", 2, 5060, 5060, 5061, 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, "+1", "*", "*", "*", 0, 0, 2,
0, 255, "", "";
IPInboundManipulation 2 = 0, 0, 2, "*", "*", "*", "*", 0, 1, 0, 0,
255, "+1", "";
IPInboundManipulation 3 = 0, 0, 1, "*", "*", "+1", "*", 0, 1, 2,
0, 255, "", "";

[ \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 1 = 0, 1, 2, "", "*", "*", "*", 0, -1, 0,
0, 0, 0, 255, "", "", 2;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

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


[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0;
CodersGroup2 1 = "g711Alaw64k", 20, 0, -1, 0;

[ \CodersGroup2 ]


[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g711Ulaw64k";

[ \AllowedCodersGroup0 ]


[ AllowedCodersGroup1 ]

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

[ \AllowedCodersGroup1 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 3 = 1, "any.Request", "header.referred-by
exists", "header.Diversion", 0, "'<'+header.referred-by.URL+'>'",
0;
MessageManipulations 4 = 1, "", "", "Header.Diversion", 6, "'+1'",
1;

[ \MessageManipulations ]
```

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com