Configuration Note

AudioCodes Professional Services - Interoperability Lab

Microsoft® Skype for Business Server 2015 and M-net SIP Trunk using AudioCodes Mediant™ MSBR E-SBC

Version 6.8

Table of Contents

This page is intentionally left blank.

Notice

This document describes how to connect the Microsoft Skype for Business Server 2015 and M-net SIP Trunk using AudioCodes Mediant E-SBC product series.

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

This document is subject to change without notice.

Date Published: July-13-2016

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 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 services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Document Revision Record

LTRT	Description
13080	Initial document release for Version 6.8.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between M-net's SIP Trunk and Microsoft's Skype for Business Server 2015 environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the E-SBC based on this interoperability setup. However, it is recommended to read through this document in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including download option, visit AudioCodes Web site at http://www.audiocodes.com/sbc-wizard (login required).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and M-net Partners who are responsible for installing and configuring M-net's SIP Trunk and Microsoft's Skype for Business Server 2015 for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

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

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

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes MSBR E-SBC Version

Table 2-1: AudioCodes MSBR E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500L MSBR & E-SBC ▪ Mediant 500 MSBR & E-SBC ▪ Mediant 800 MSBR & E-SBC
Software Version	SIP_6.80A.311.003
Protocol	▪ SIP/UDP or TCP (to the M-net SIP Trunk) ▪ SIP/TCP or TLS (to the S4B FE Server)
Additional Notes	None

2.2 M-net SIP Trunking Version

Table 2-2: M-net Version

Vendor/Service Provider	Metaswitch
SSW Model/Service	CFS 9.2.10
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Skype for Business Server 2015 Version

Table 2-3: Microsoft Skype for Business Server 2015 Version

Vendor	Microsoft
Model	Skype for Business
Software Version	Release 2015 6.0.9319.0
Protocol	SIP
Additional Notes	None

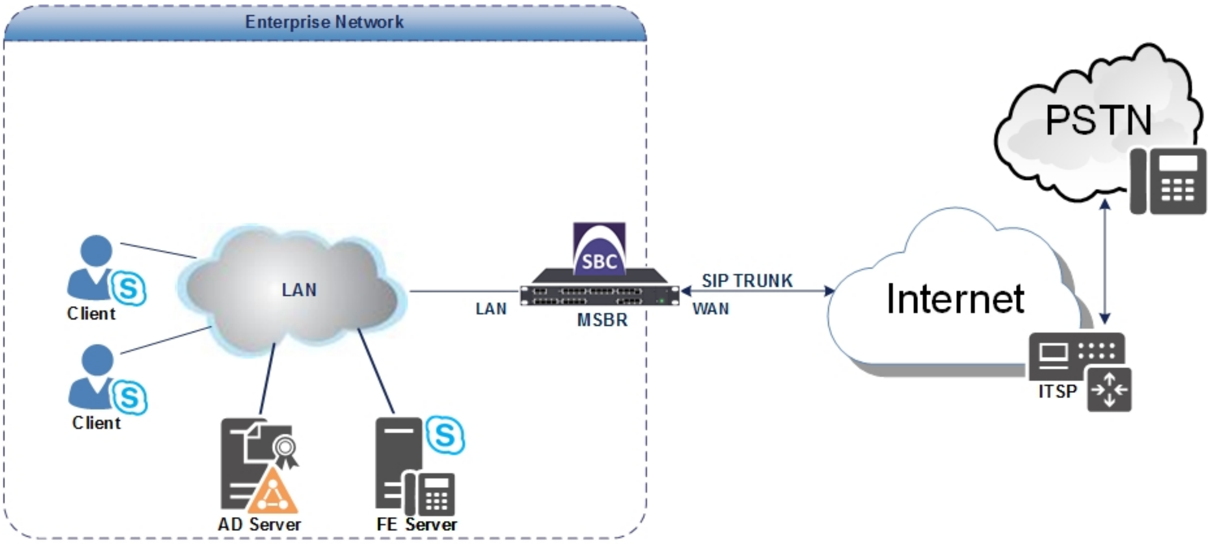
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and M-net SIP Trunk with Skype for Business 2015 was done using the following topology setup:

- Enterprise deployed with Microsoft Skype for Business Server 2015 in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using M-net's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between Skype for Business Server 2015 network in the Enterprise LAN and M-net's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and Microsoft Skype for Business with M-net SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Microsoft Skype for Business Server 2015 environment is located on the Enterprise's LAN ▪ M-net SIP Trunk is located on the WAN
Signaling Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SIP-over-TLS transport type ▪ M-net SIP Trunk operates with SIP-over-UDP or SIP-over-TCP transport type
Codecs Transcoding	▪ Microsoft Skype for Business Server 2015 supports G.711A-law and G.711U-law coders ▪ M-net SIP Trunk supports G.711A-law and G.729 coders
Media Transcoding	▪ Microsoft Skype for Business Server 2015 operates with SRTP media type ▪ M-net SIP Trunk operates with RTP media type

2.4.2 Known Limitations

The following limitations were observed during interoperability tests performed for AudioCodes' E-SBC interworking between Microsoft Skype for Business Server 2015 and M-net 's SIP Trunk:

- If the Microsoft Skype for Business Server 2015 sends one of the following error responses:
  - 503 Service Unavailable
  - 488 Not Acceptable Here

  M-net SIP Trunk still sends re-INVITEs and does not disconnect the call.

  To disconnect the call, a message manipulation rule is used to replace the above error response with the '480 Temporarily Unavailable' response (see Section 4.12 on page 69).
- In Call Forwarding scenarios, when a Skype for Business user forwards a call to a PSTN user, RTP packets need to be sent to open a pinhole in the firewall. To overcome this problem with the first incoming RTP packet in this scenario, instead of generating Ringback Tone as Call Progress Tone (CPT), which requires DSP we decided to use a Prerecorded Tones (PRT) file for ringback tones.

This page is intentionally left blank.

3 Configuring Skype for Business Server 2015

This chapter describes how to configure Microsoft Skype for Business Server 2015 to operate with AudioCodes E-SBC.

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

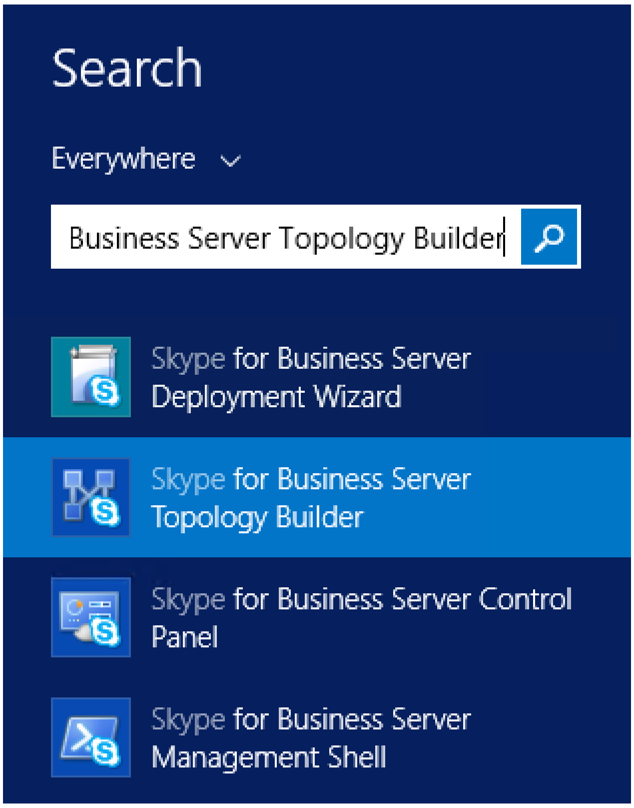
3.1 Configuring the E-SBC as an IP / PSTN Gateway

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

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

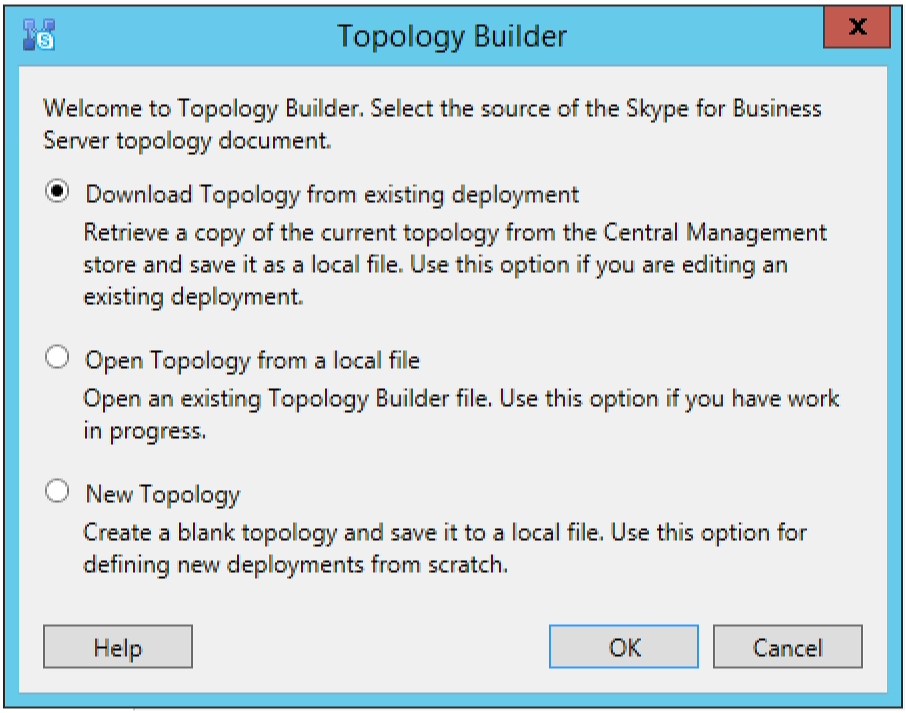
1. On the server where the Topology Builder is installed, start the Skype for Business Server 2015 Topology Builder (Windows **Start** menu > search for **Skype for Business Server Topology Builder**), as shown below:

Figure 3-1: Starting the Skype for Business Server Topology Builder



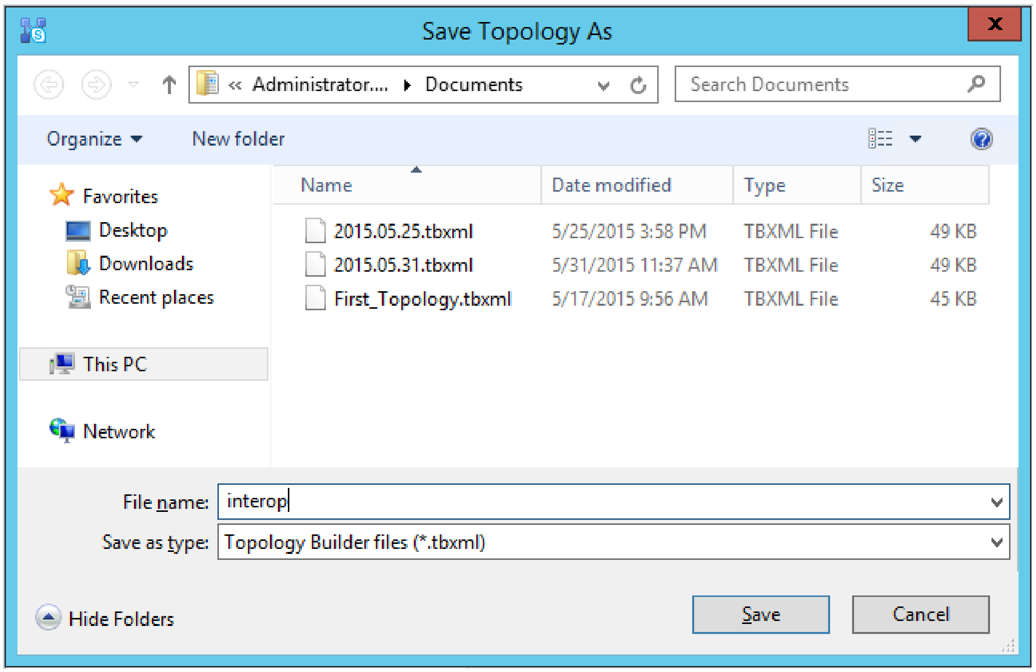
The following is displayed:

Figure 3-2: Topology Builder Dialog Box



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

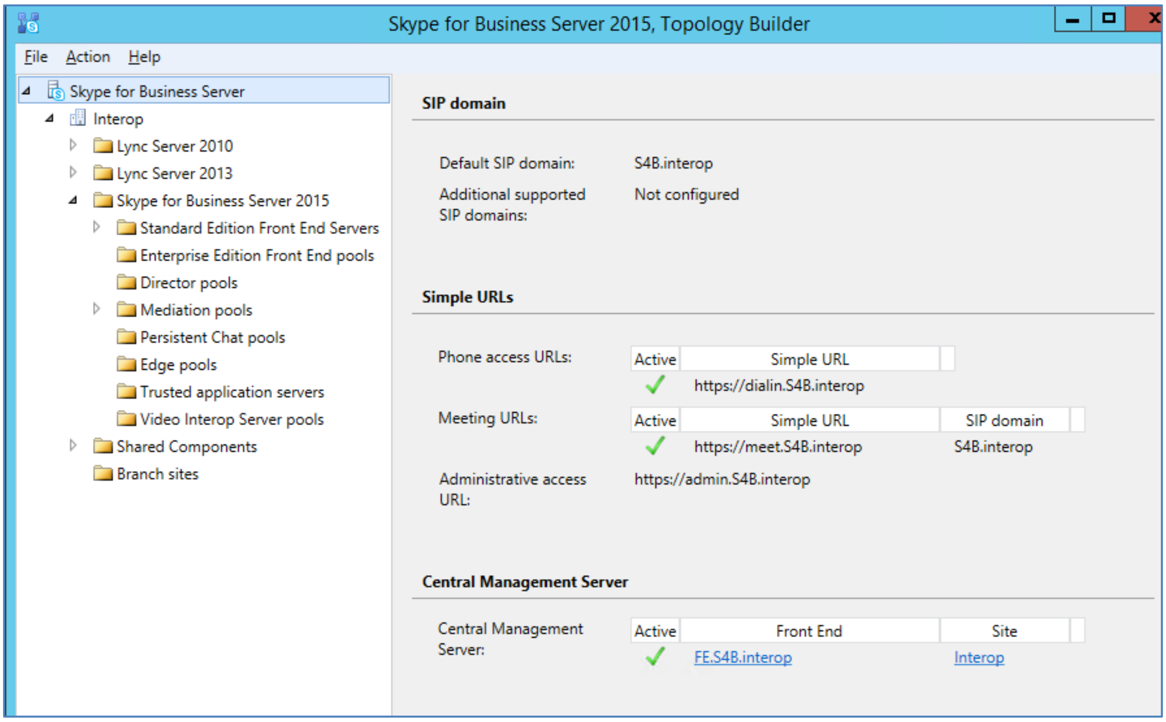
Figure 3-3: Save Topology Dialog Box



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

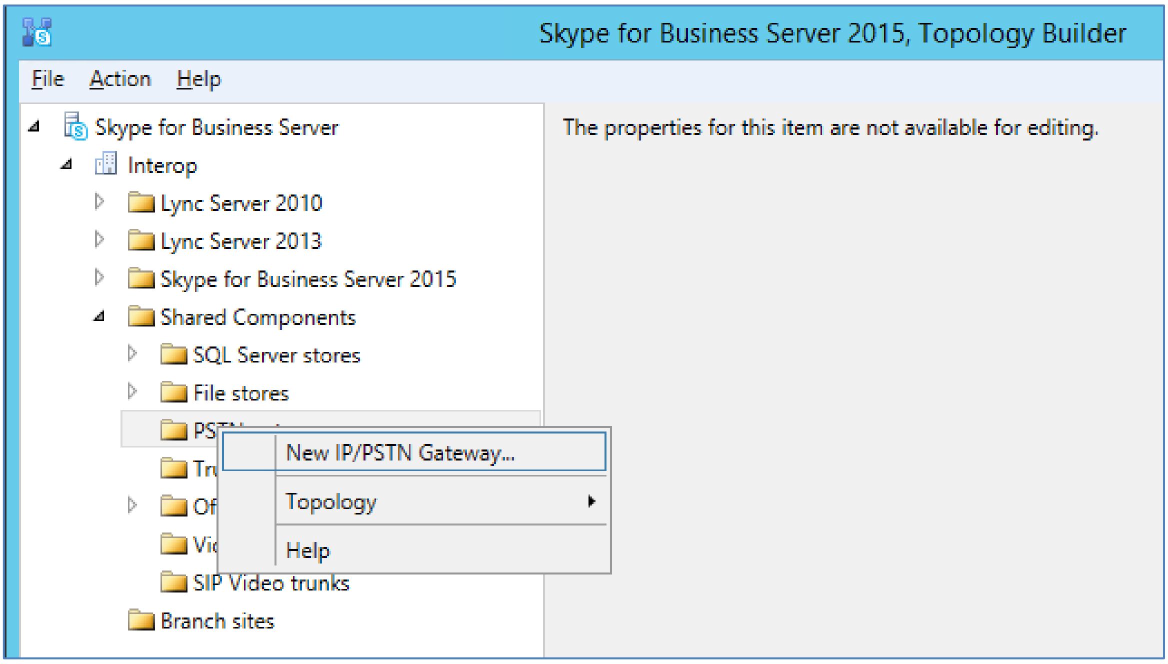
The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology



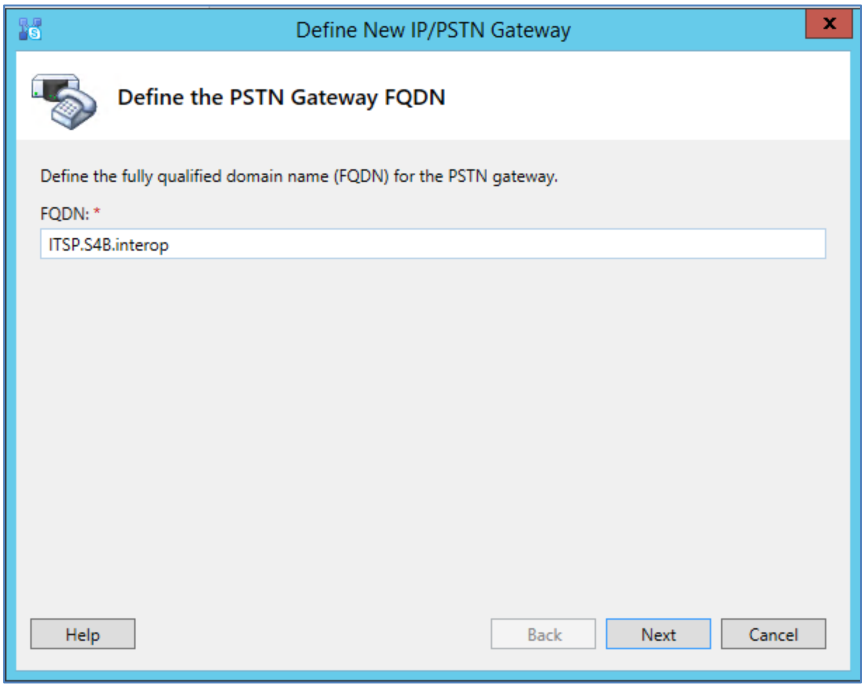
4. Under the **Shared Components** node, right-click the **PSTN gateways** node, and then from the shortcut menu, choose **New IP/PSTN Gateway**, as shown below:

Figure 3-5: Choosing New IP/PSTN Gateway



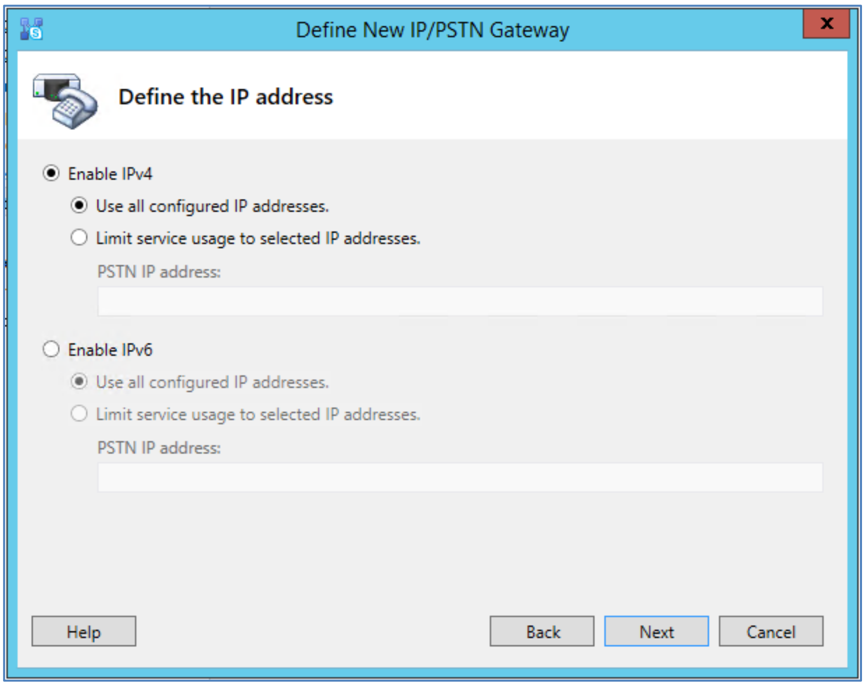
The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN



5. Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., **ITSP.S4B.interop**). This FQDN should be equivalent to the configured Subject Name (CN) in the TLS Certificate Context (see Section 4.8.3 on page 55).
6. Click **Next**; the following is displayed:

Figure 3-7: Define the IP Address



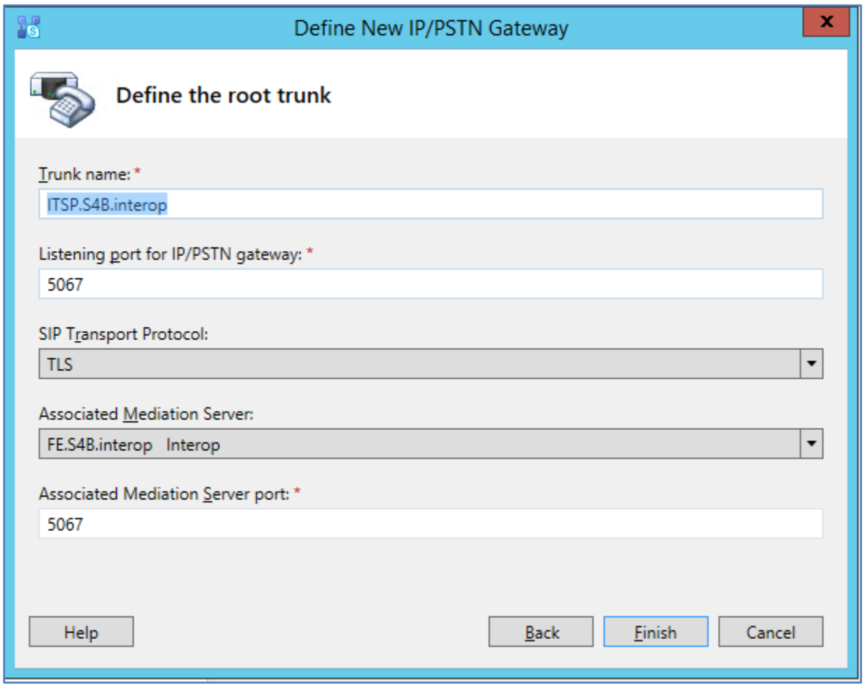
7. Define the listening mode (IPv4 or IPv6) of the IP address of your new PSTN gateway, and then click **Next**.

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

Notes:

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

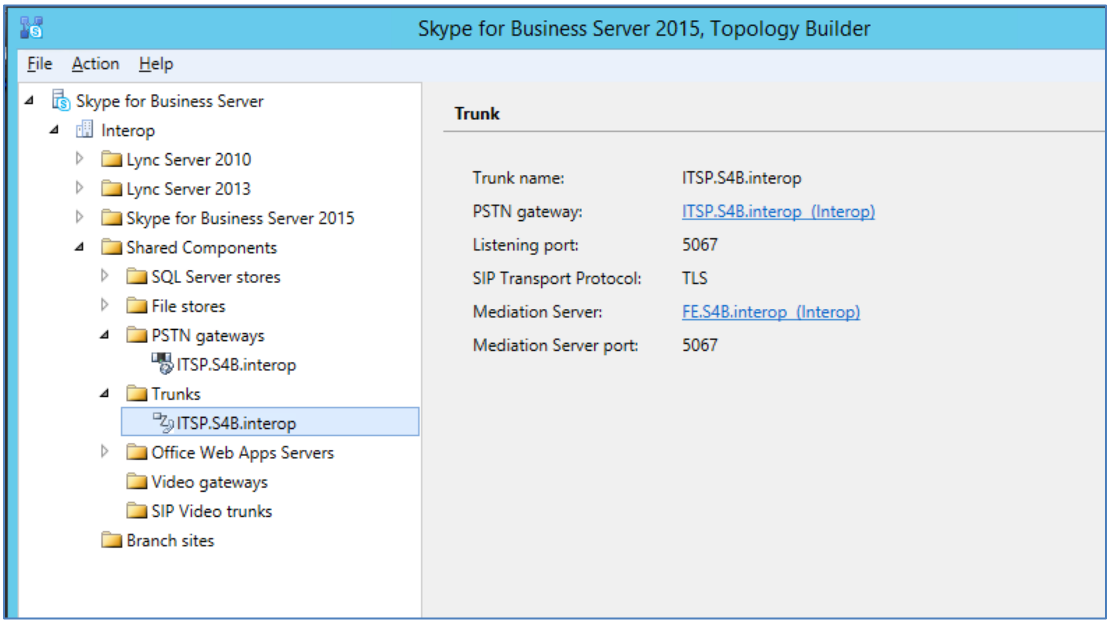
Figure 3-8: Define the Root Trunk



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

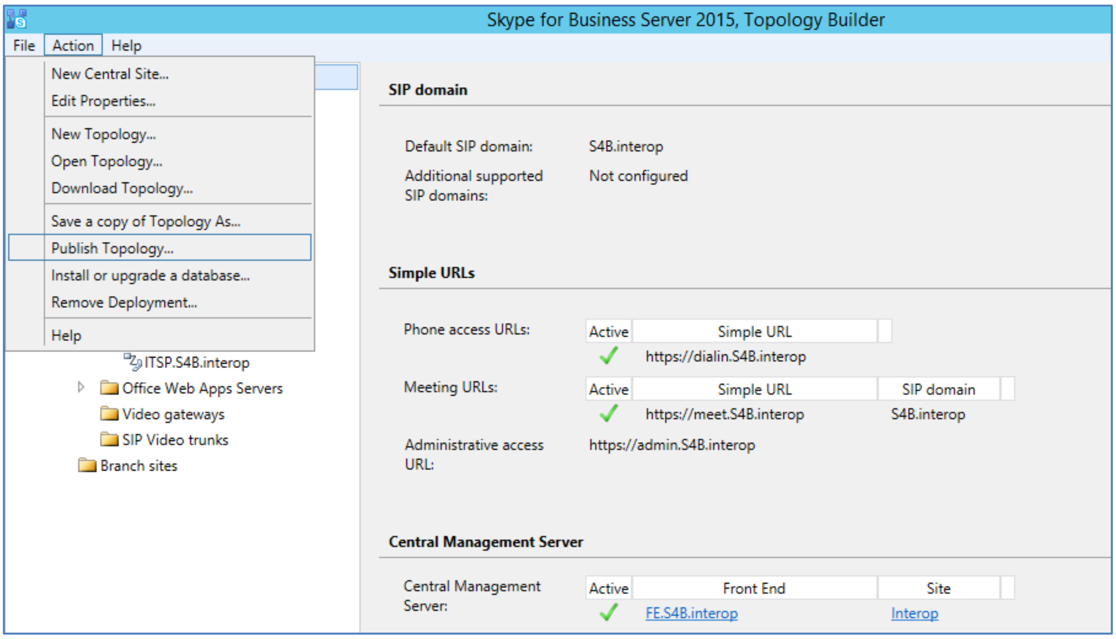
The E-SBC is added as a PSTN gateway, and a trunk is created as shown below:

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



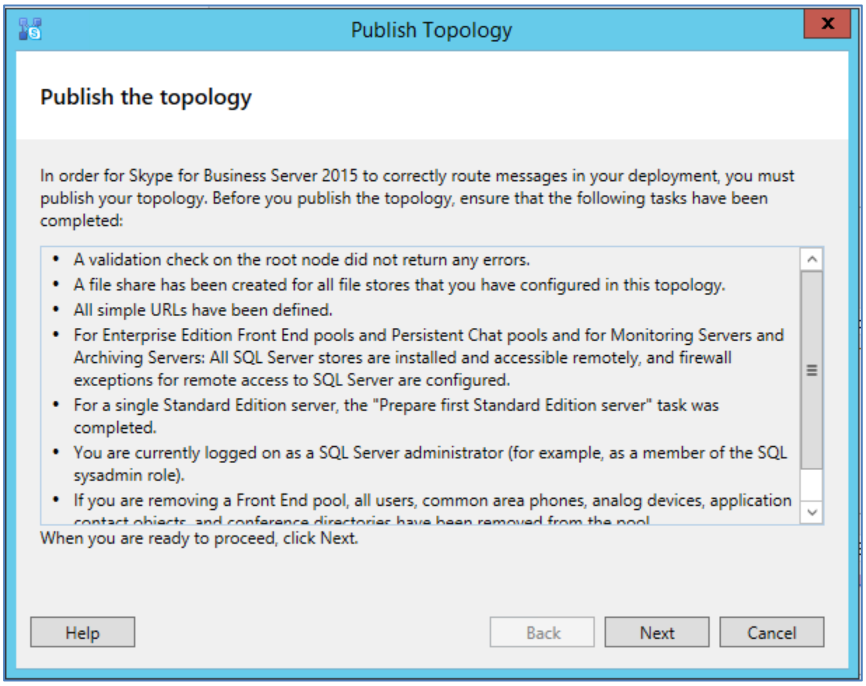
9. Publish the Topology: In the main tree, select the root node **Skype for Business Server**, and then from the **Action** menu, choose **Publish Topology**, as shown below:

Figure 3-10: Choosing Publish Topology



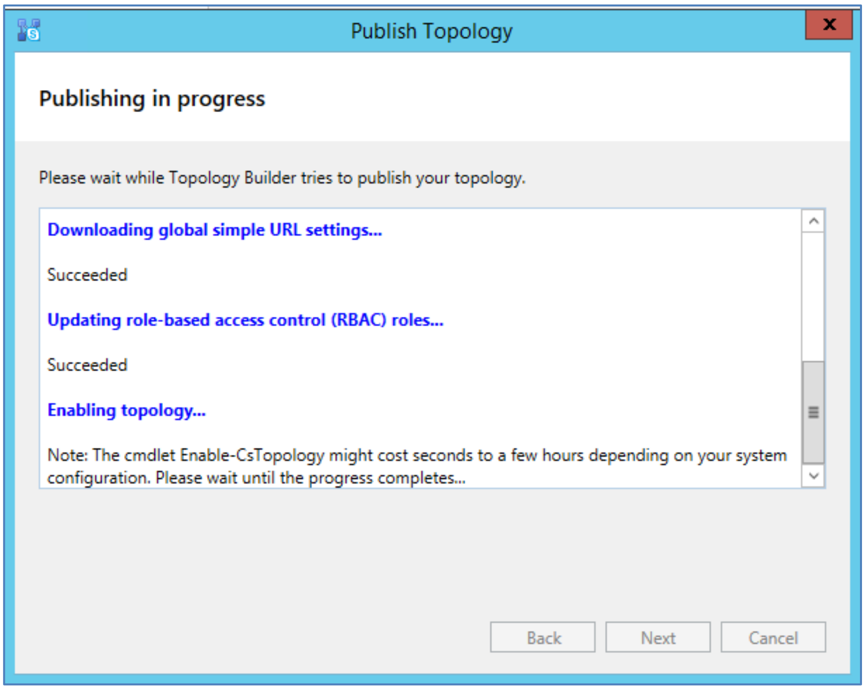
The following is displayed:

Figure 3-11: Publish the Topology



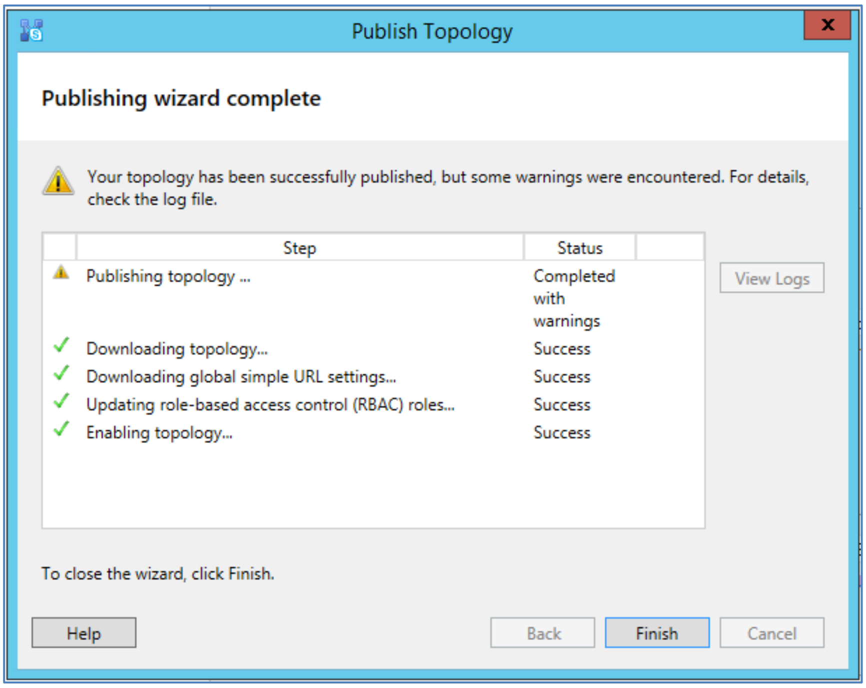
10. Click **Next**; the Topology Builder starts to publish your topology, as shown below:

Figure 3-12: Publishing in Progress



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

Figure 3-13: Publishing Wizard Complete



12. Click **Finish**.

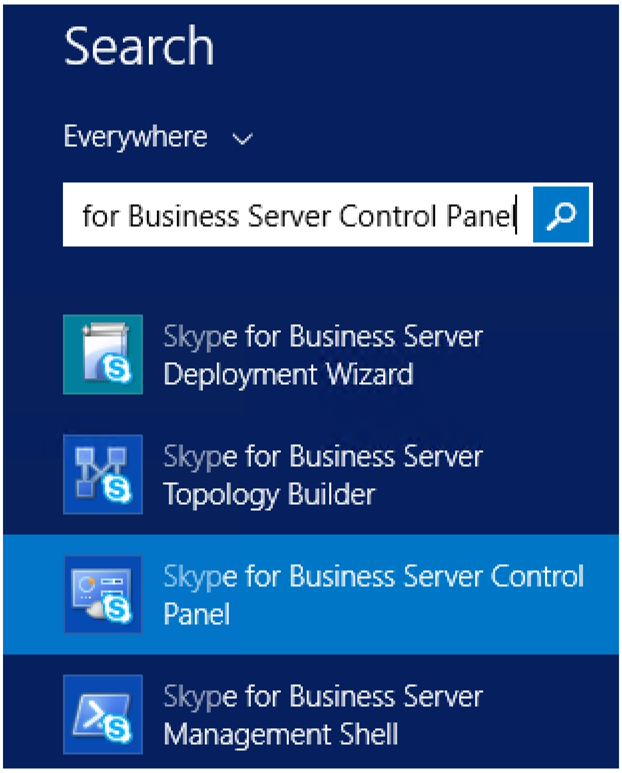
3.2 Configuring the "Route" on Skype for Business Server 2015

The procedure below describes how to configure a "Route" on the Skype for Business Server 2015 and to associate it with the E-SBC PSTN gateway.

➢ **To configure the "route" on Skype for Business Server 2015:**

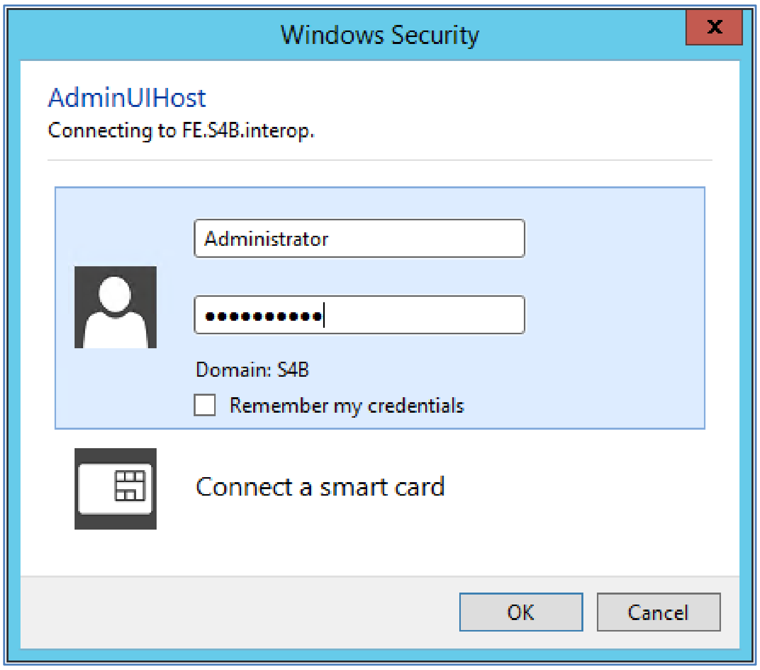
1. Start the Microsoft Skype for Business Server 2015 Control Panel (**Start** > search for **Microsoft Skype for Business Server Control Panel**), as shown below:

Figure 3-14: Opening the Skype for Business Server Control Panel



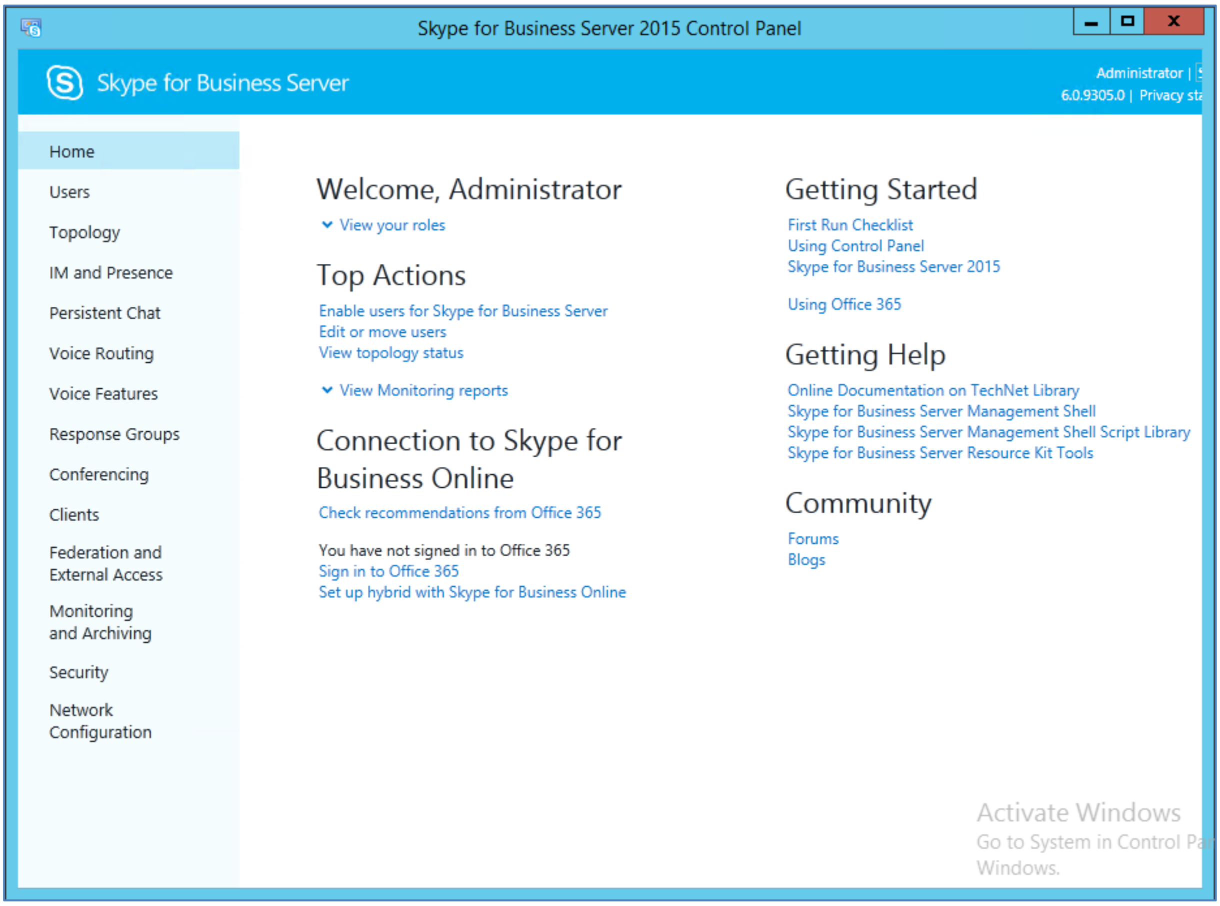
2. You are prompted to enter your login credentials.

Figure 3-15: Skype for Business Server Credentials



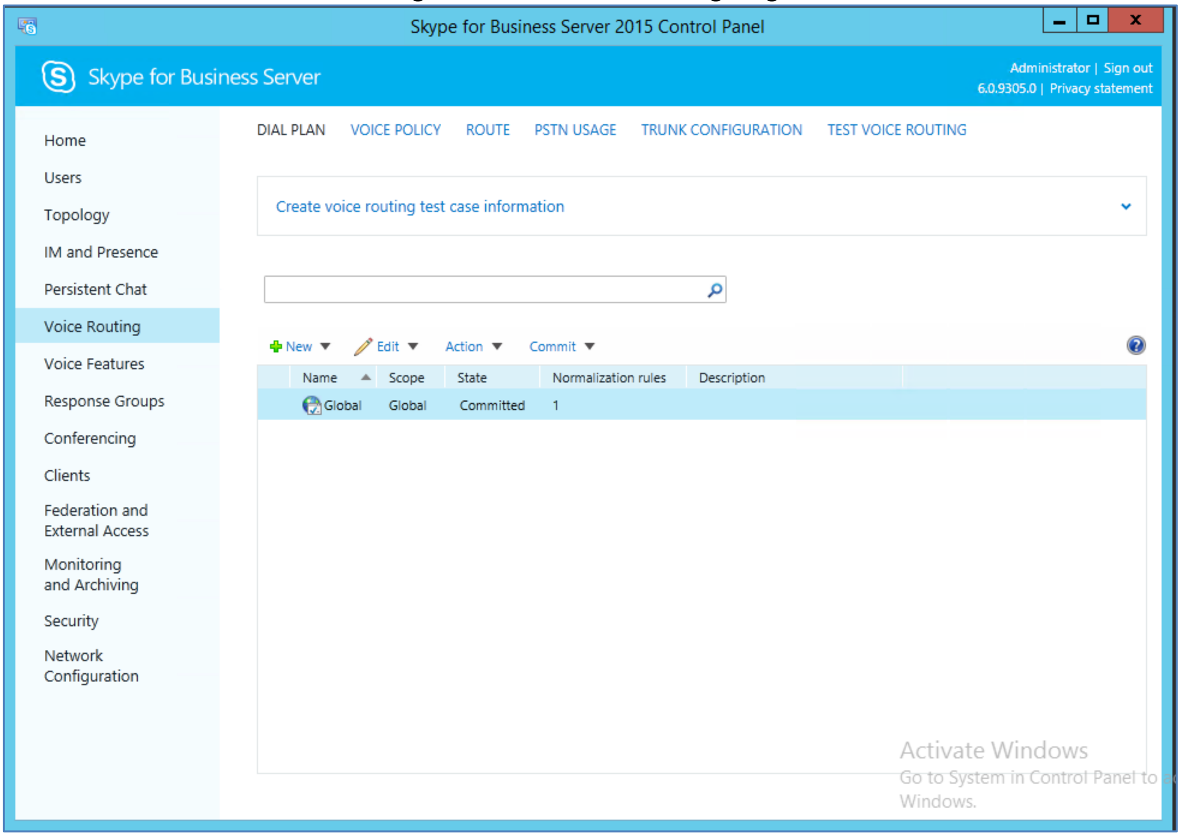
3. Enter your domain username and password, and then click **OK**; the Microsoft Skype for Business Server 2015 Control Panel is displayed.

Figure 3-16: Microsoft Skype for Business Server 2015 Control Panel



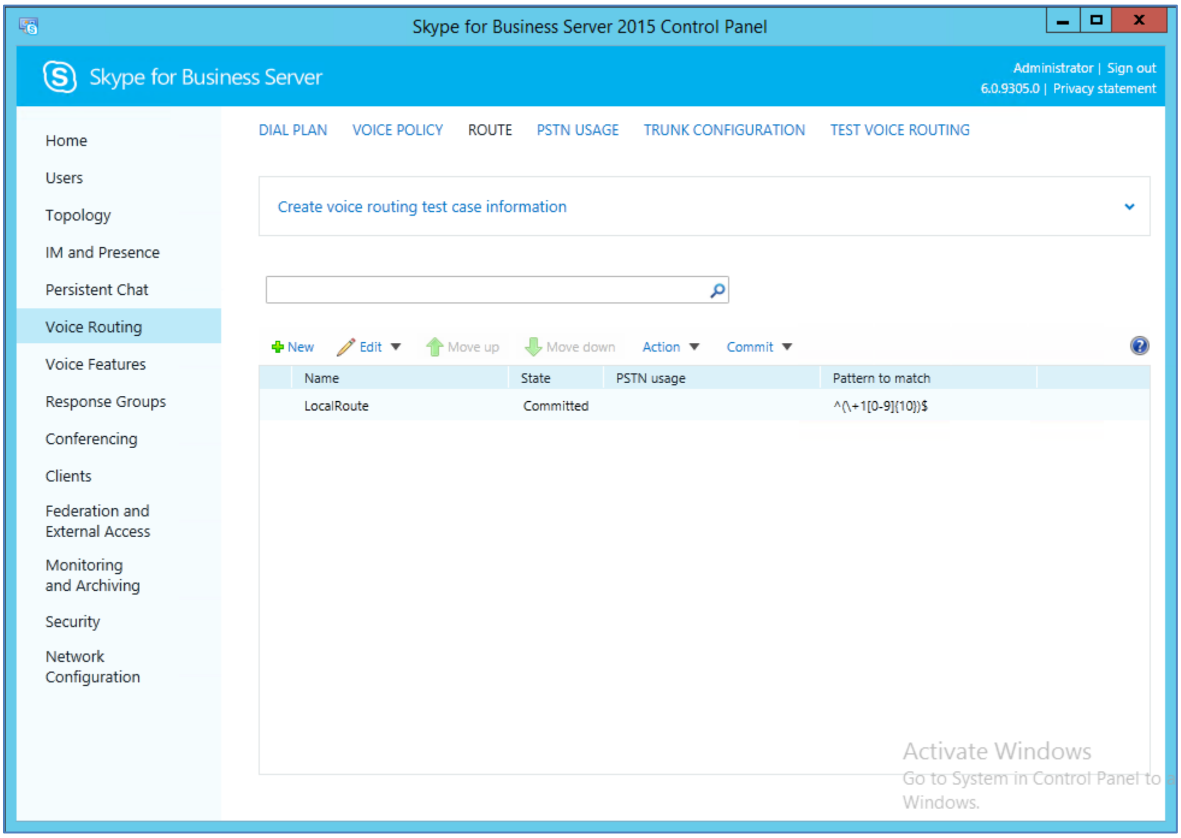
4. In the left navigation pane, select **Voice Routing**.

Figure 3-17: Voice Routing Page



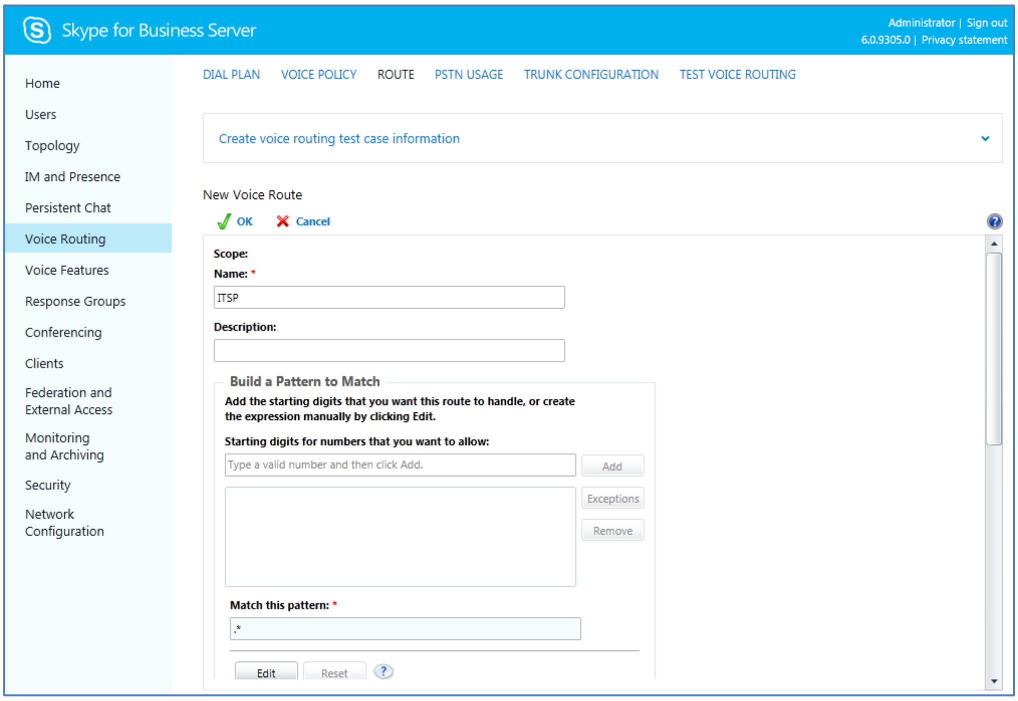
5. In the Voice Routing page, select the **Route** tab.

Figure 3-18: Route Tab



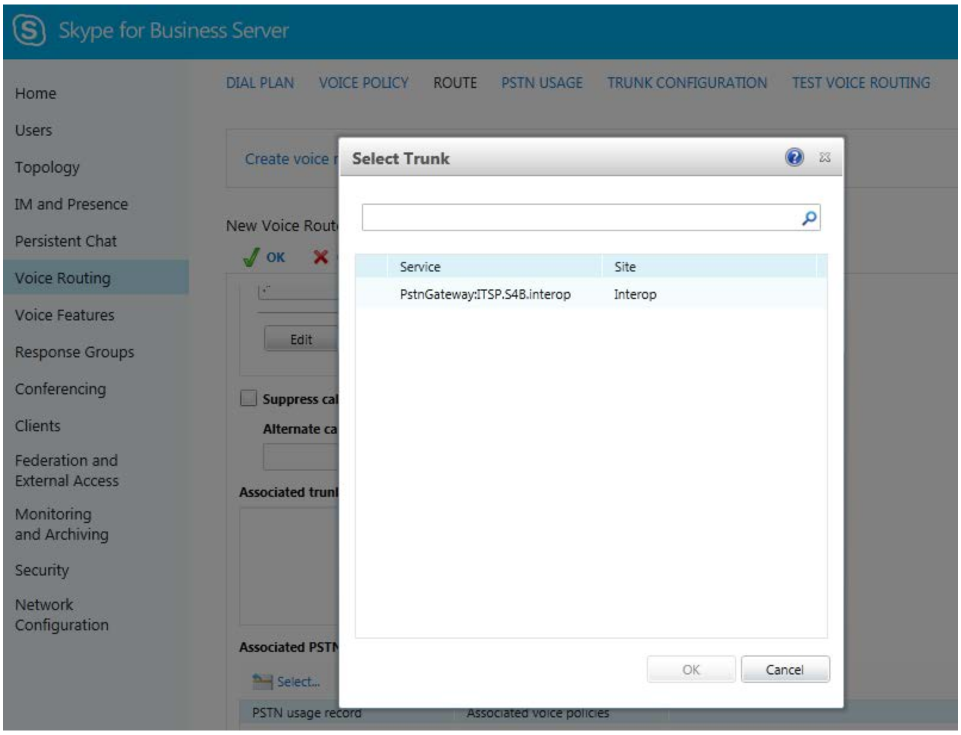
6. Click **New**; the New Voice Route page appears.

Figure 3-19: Adding New Voice Route



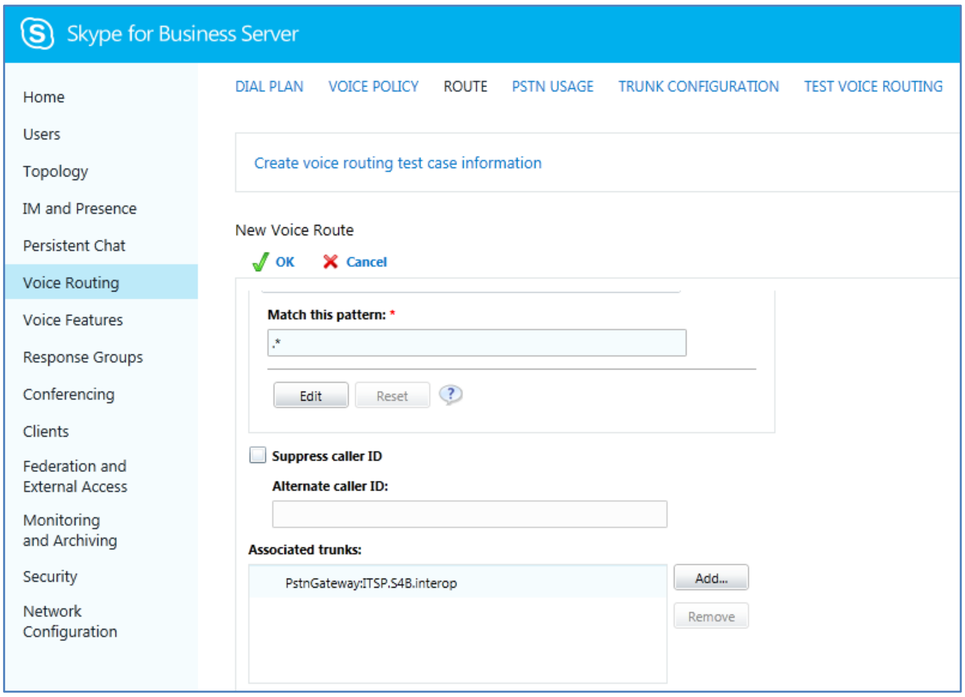
7. In the 'Name' field, enter a name for this route (e.g., **ITSP**).
8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.
9. Associate the route with the E-SBC Trunk that you created:
   a. Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Figure 3-20: List of Deployed Trunks



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

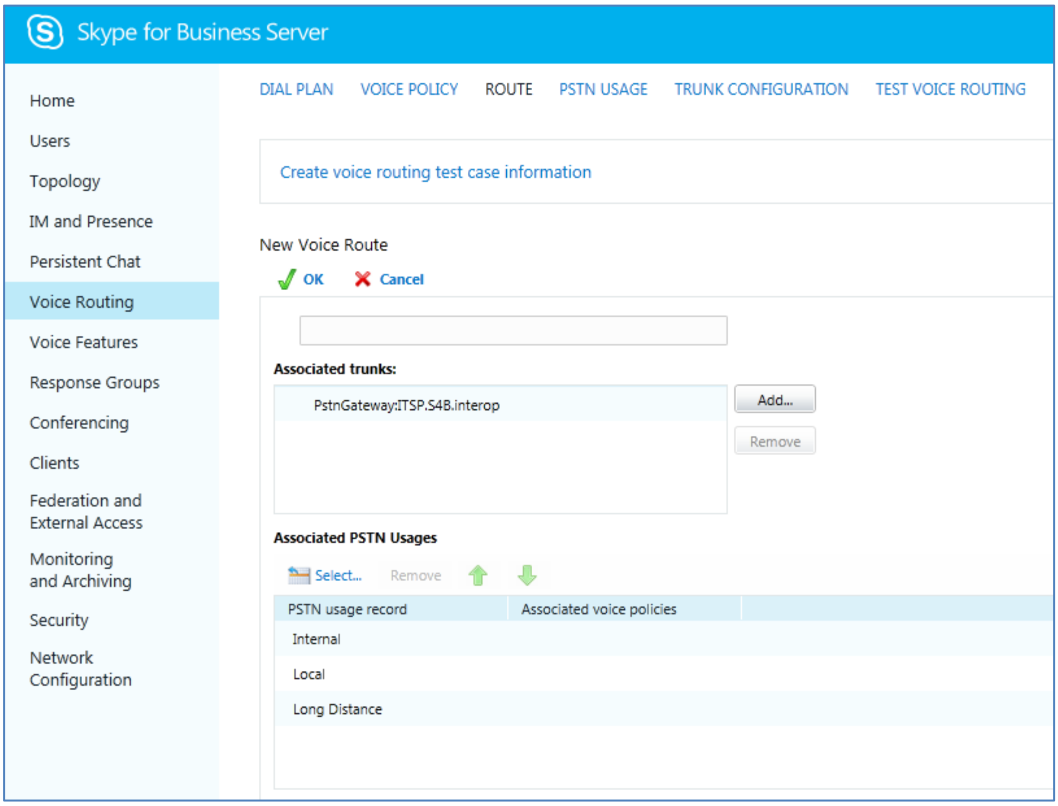
Figure 3-21: Selected E-SBC Trunk



10. Associate a PSTN Usage to this route:

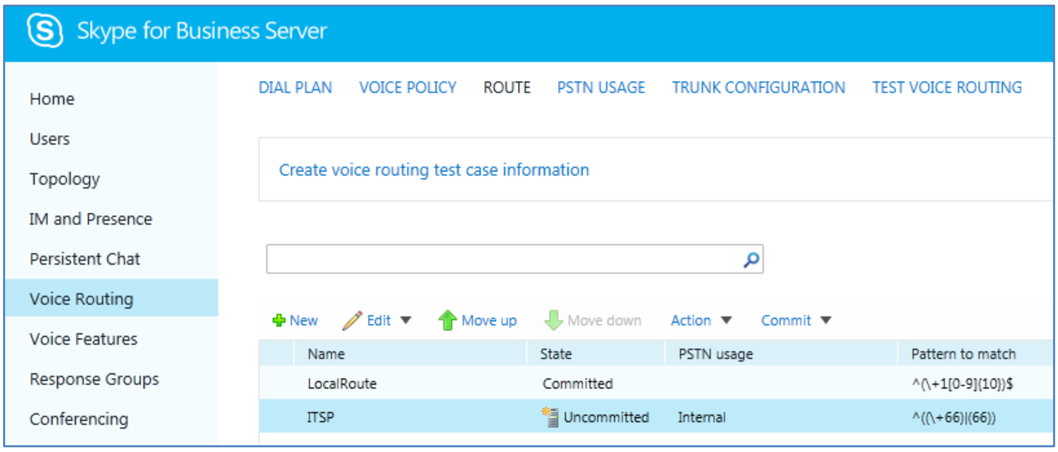
a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

Figure 3-22: Associating PSTN Usage to Route



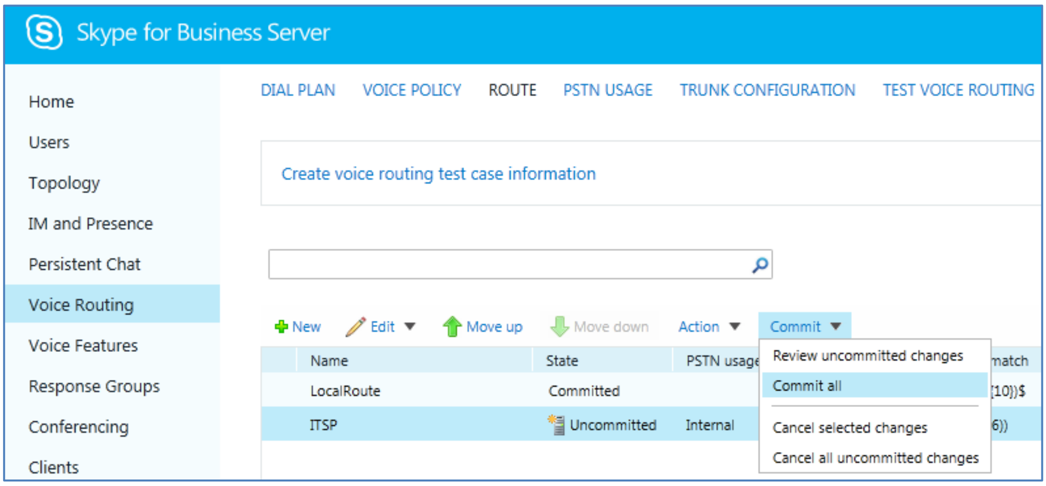
11. Click **OK** (located on the top of the New Voice Route page); the New Voice Route (Uncommitted) is displayed.

Figure 3-23: Confirmation of New Voice Route



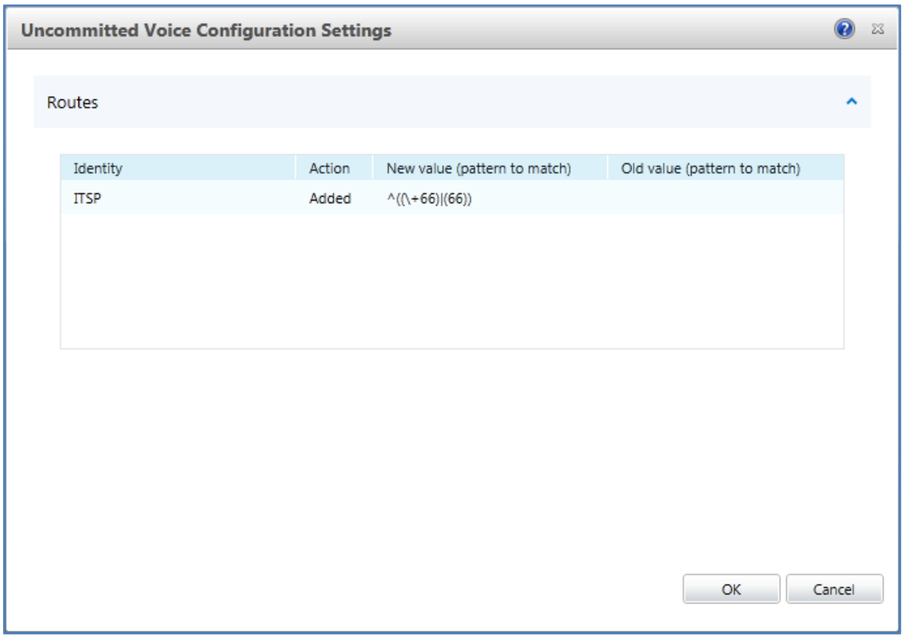
12. From the **Commit** drop-down list, choose **Commit all**, as shown below:

Figure 3-24: Committing Voice Routes



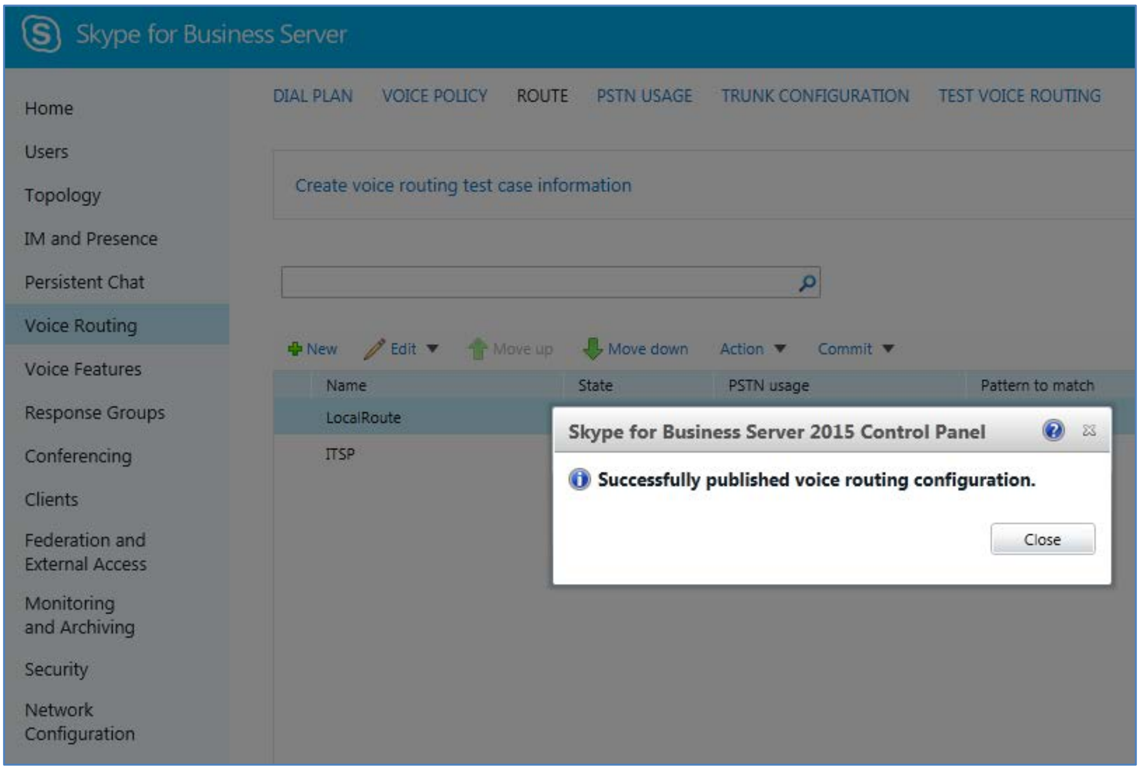
The Uncommitted Voice Configuration Settings page appears:

Figure 3-25: Uncommitted Voice Configuration Settings



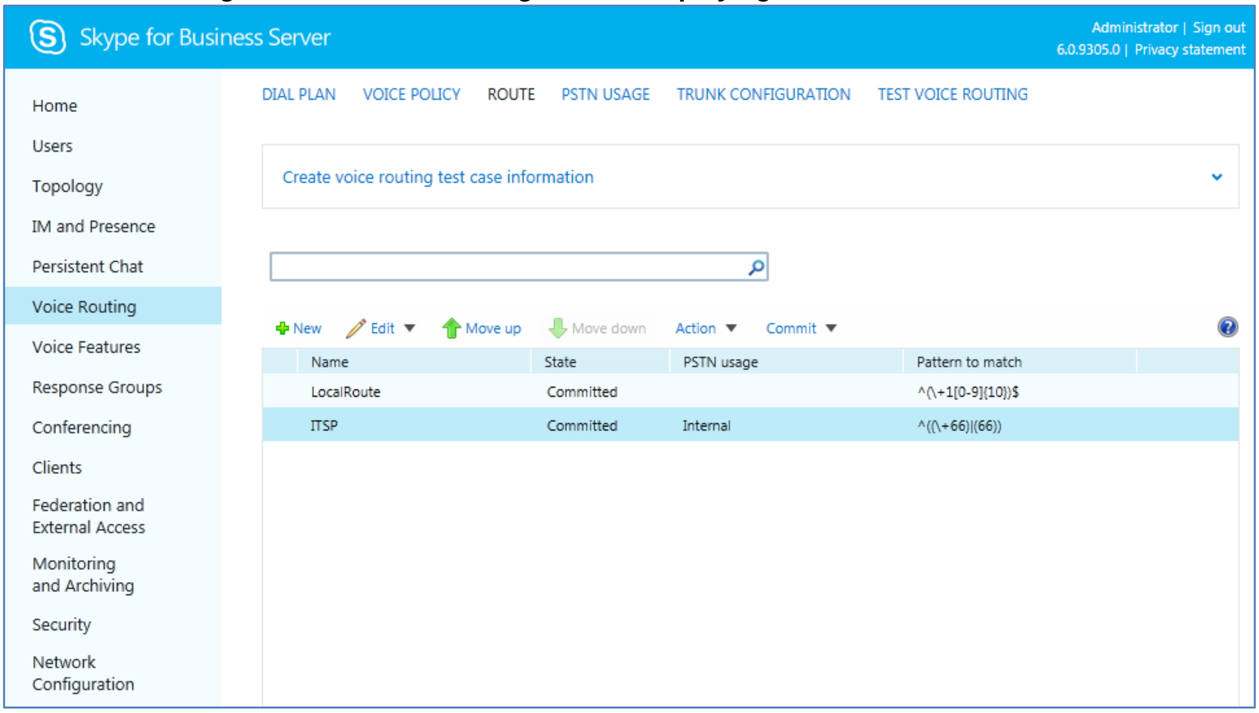
13. Click **Commit**; a message is displayed confirming a successful voice routing configuration, as shown below:

Figure 3-26: Confirmation of Successful Voice Routing Configuration



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

Figure 3-27: Voice Routing Screen Displaying Committed Routes

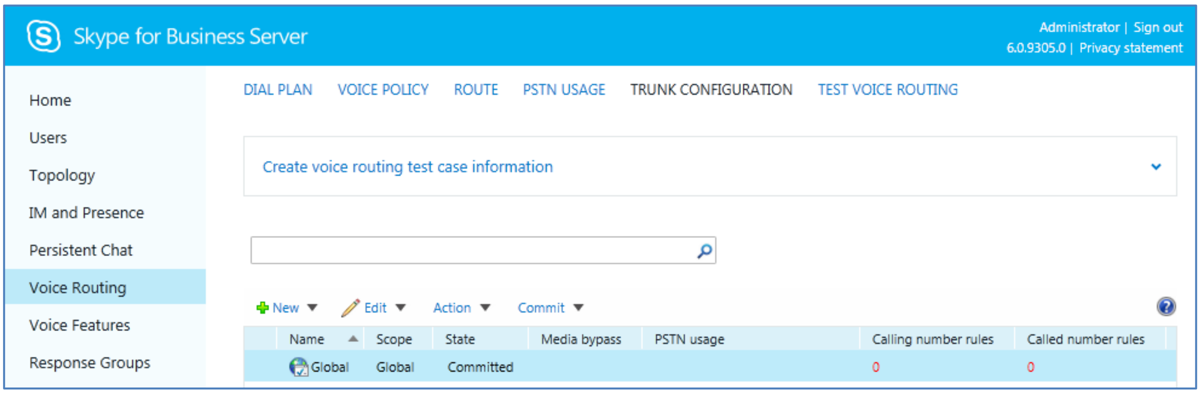


15. For ITSPs that implement a call identifier, continue with the following steps:

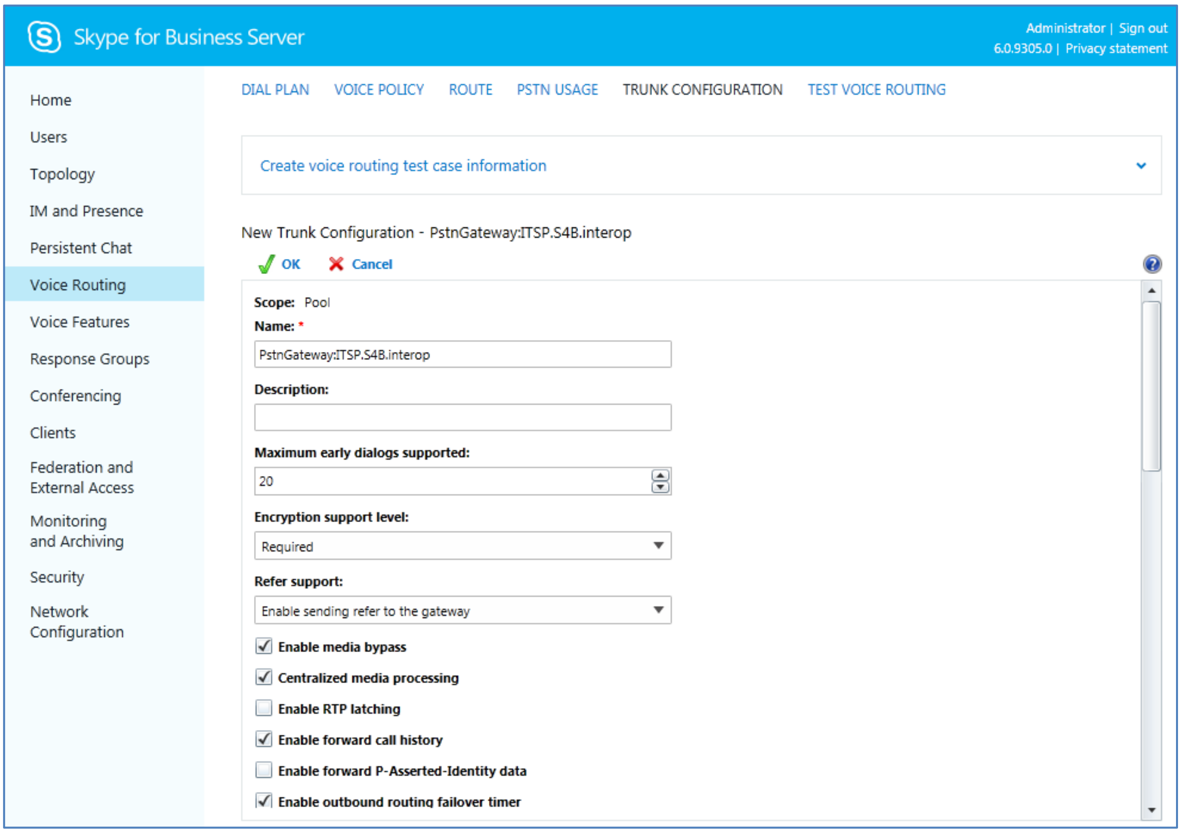
Note: The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Skype for Business user number). This ID is required by M-net SIP Trunk in the P-Asserted-Identity header. The device adds this ID to the P-Asserted-Identity header in the sent INVITE message using the IP Profile (see Section 4.5 on page 43.

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

Figure 3-28: Voice Routing Screen – Trunk Configuration Tab



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



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

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

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes MSBR E-SBC for interworking between Microsoft Skype for Business Server 2015 and the M-net SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

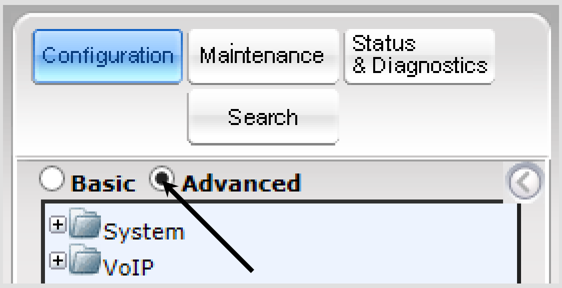
- E-SBC MSBR WAN interface - M-net SIP Trunking environment
- E-SBC LAN interface - Skype for Business Server 2015 environment

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

Notes:

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

  For more information about the Software License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Advanced-menu display mode. To do this, select the Advanced option, as shown below:



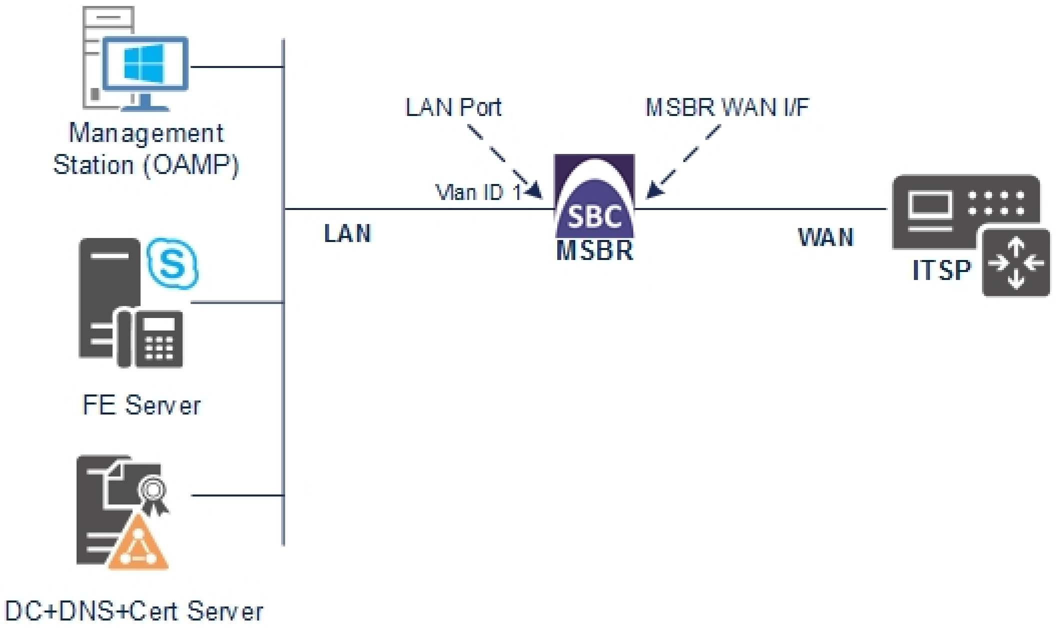
- When the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

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

- E-SBC interfaces with the following IP entities:
  - Skype for Business servers, located on the LAN
  - M-net SIP Trunk, located on the WAN
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN using dedicated LAN port and to the WAN using MSBR's VDSL WAN interface.

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure Network Interface

This step describes how to configure the IP network interface for LAN VoIP interface (assigned the name "Voice"). Configuration of WAN data interface depends on physical interface, that's why it is out of the scope of this document.

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

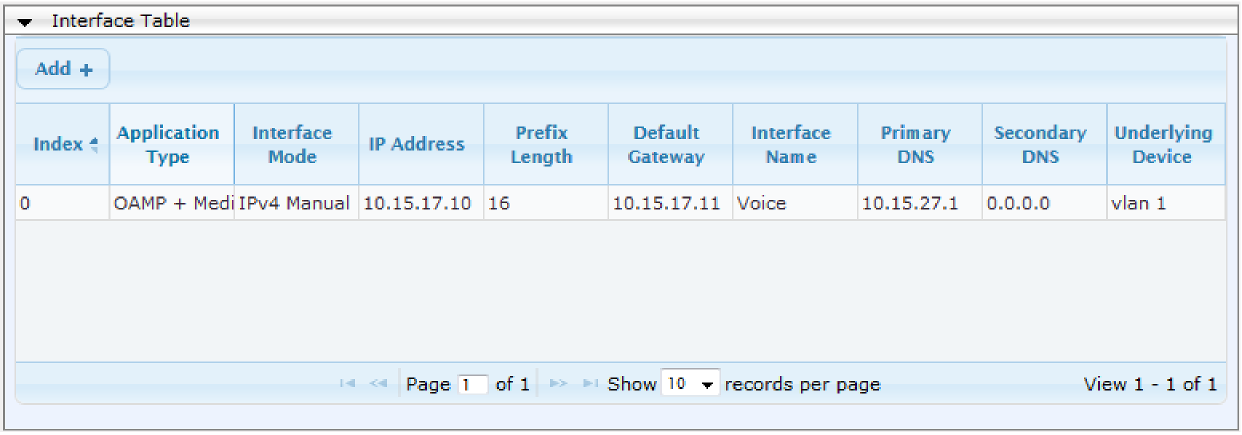
1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface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

Parameter	Value
IP Address	**10.15.17.10** (LAN IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Default Gateway	**10.15.17.11** (MSBR Data vlan 1 IP address)
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.27.1**
Underlying Device	**vlan 1**

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

The configured IP network interface is shown below:

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



Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Medi	IPv4 Manual	10.15.17.10	16	10.15.17.11	Voice	10.15.27.1	0.0.0.0	vlan 1

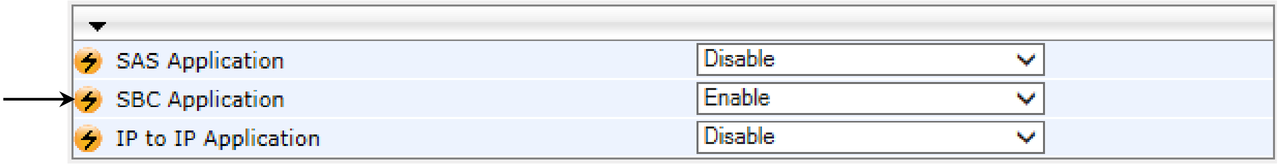
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 4-3: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.15 on page 85).

4.3 Step 3: Signaling Routing Domains Configuration

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

The SRD is composed of the following:

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

4.3.1 Step 3a: Configure Media Realms

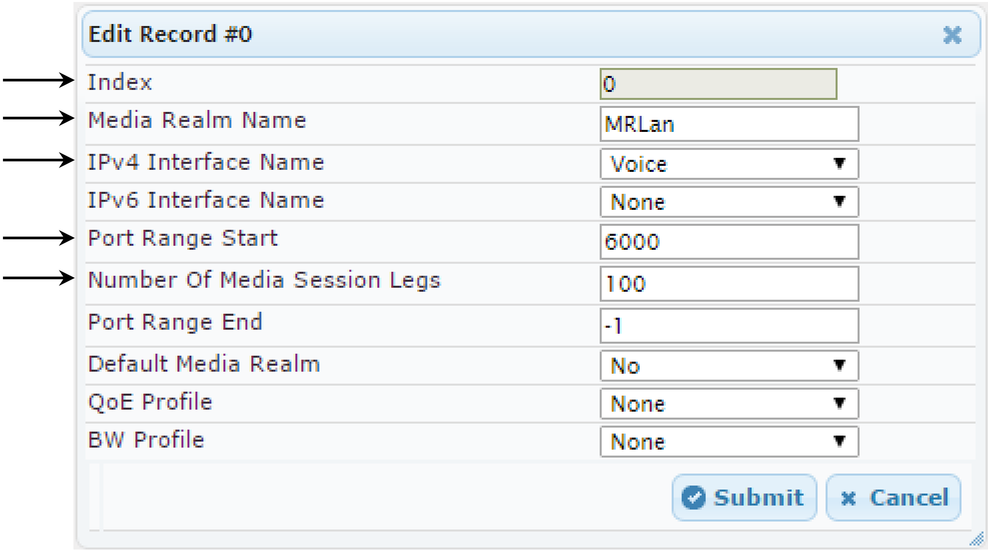
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

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

Parameter	Value
Index	**0**
Media Realm Name	**MRLan** (descriptive name)
IPv4 Interface Name	**Voice**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

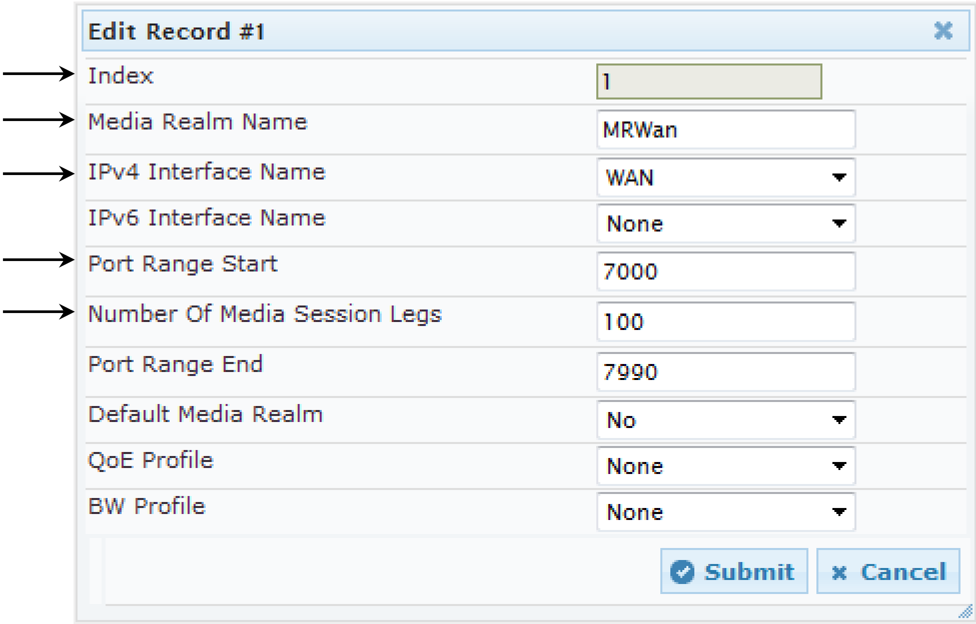
Figure 4-4: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

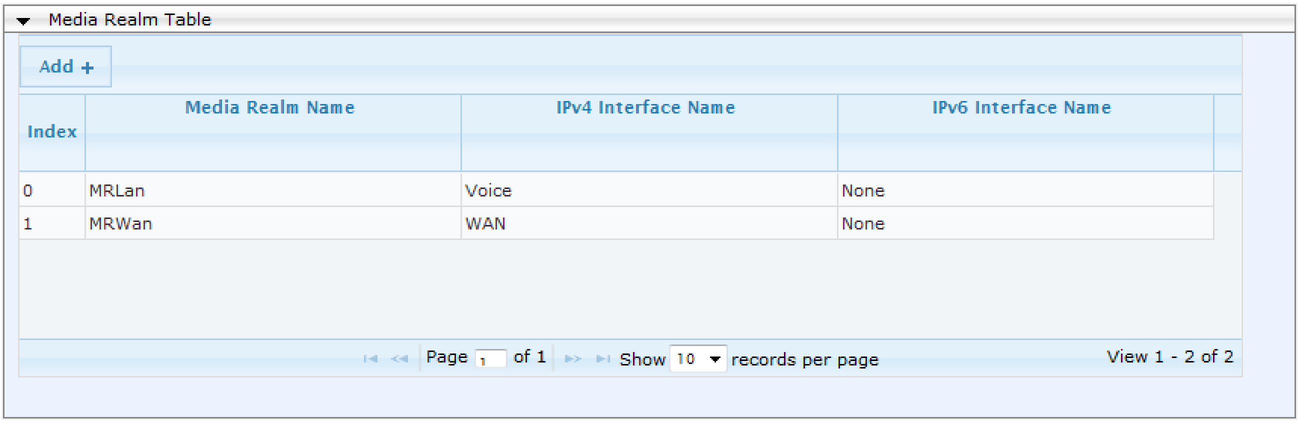
Parameter	Value
Index	**1**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**WAN** (a reserved word for MSBR WAN I/F)
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-5: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-6: Configured Media Realms in Media Realm Table



4.3.2 Step 3b: Configure SRDs

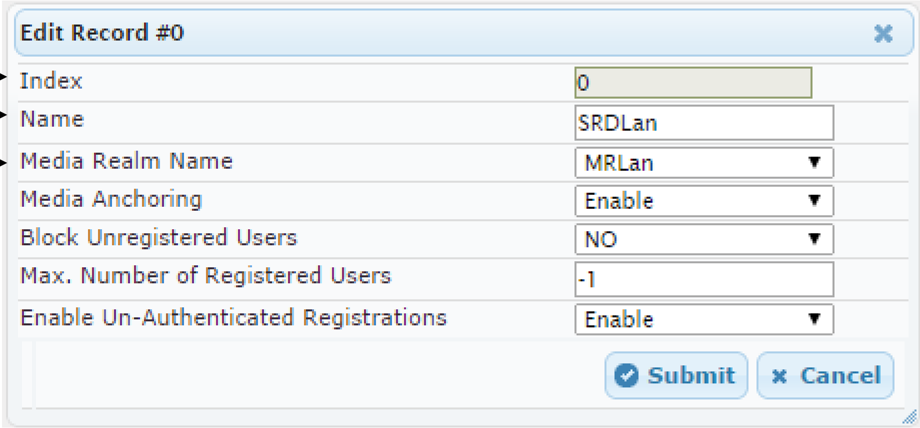
This step describes how to configure the SRDs.

➢ **To configure SRDs:**

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

Parameter	Value
Index	**0**
Name	**SRDLan** (descriptive name for SRD)
Media Realm Name	**MRLan** (associates SRD with Media Realm)

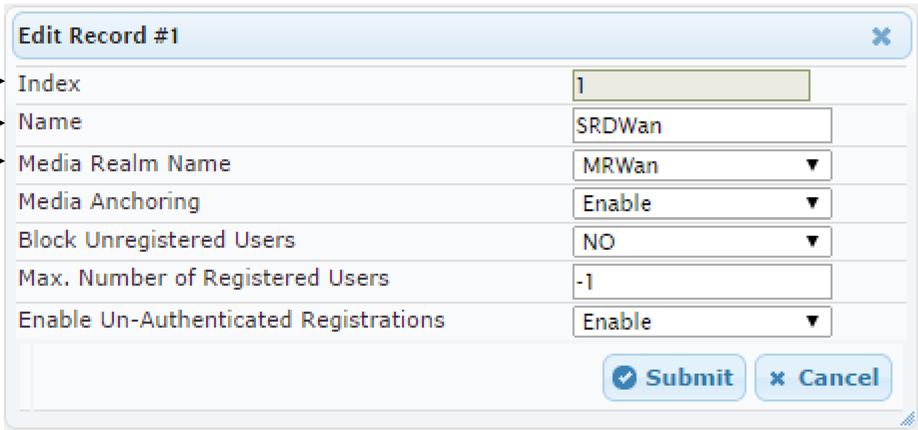
Figure 4-7: Configuring LAN SRD



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

Parameter	Value
Index	**1**
Name	**SRDWan**
Media Realm Name	**MRWan**

Figure 4-8: Configuring WAN SRD



The configured SRDs are shown in the figure below:

Figure 4-9: Configured SRDs in SRD Table

4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

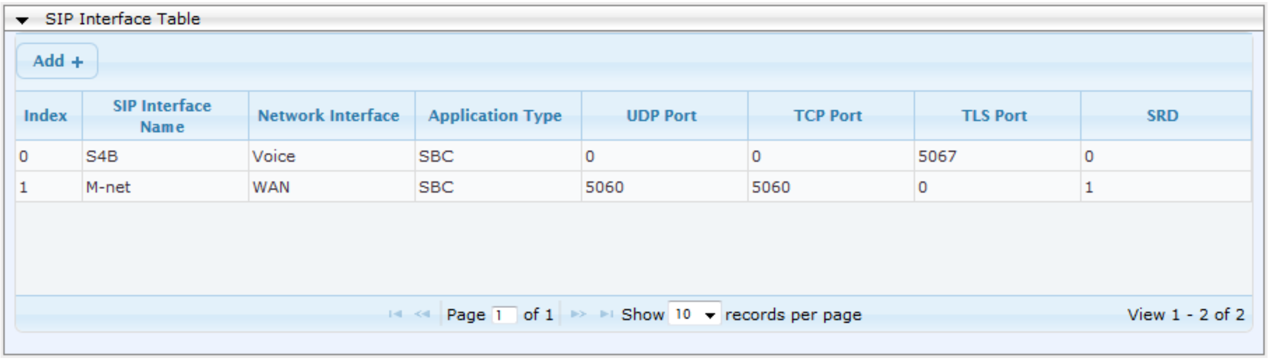
Parameter	Value
Index	**0**
Interface Name	**S4B** (arbitrary descriptive name)
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**0**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**1**
Interface Name	**M-net** (arbitrary descriptive name)
Network Interface	**WAN**
Application Type	**SBC**
UDP Port	**5060**
TCP Port	**5060**
TLS Port	**0**
SRD	**1**

The configured SIP Interfaces are shown in the figure below:

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



Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
0	S4B	Voice	SBC	0	0	5067	0
1	M-net	WAN	SBC	5060	5060	0	1

Note: The TLS port parameter (for S4B SIP Interface) must be identically configured in the Skype for Business Topology Builder (see Section 3.1 on page13).

4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Skype for Business Server 2015
- M-net SIP Trunk

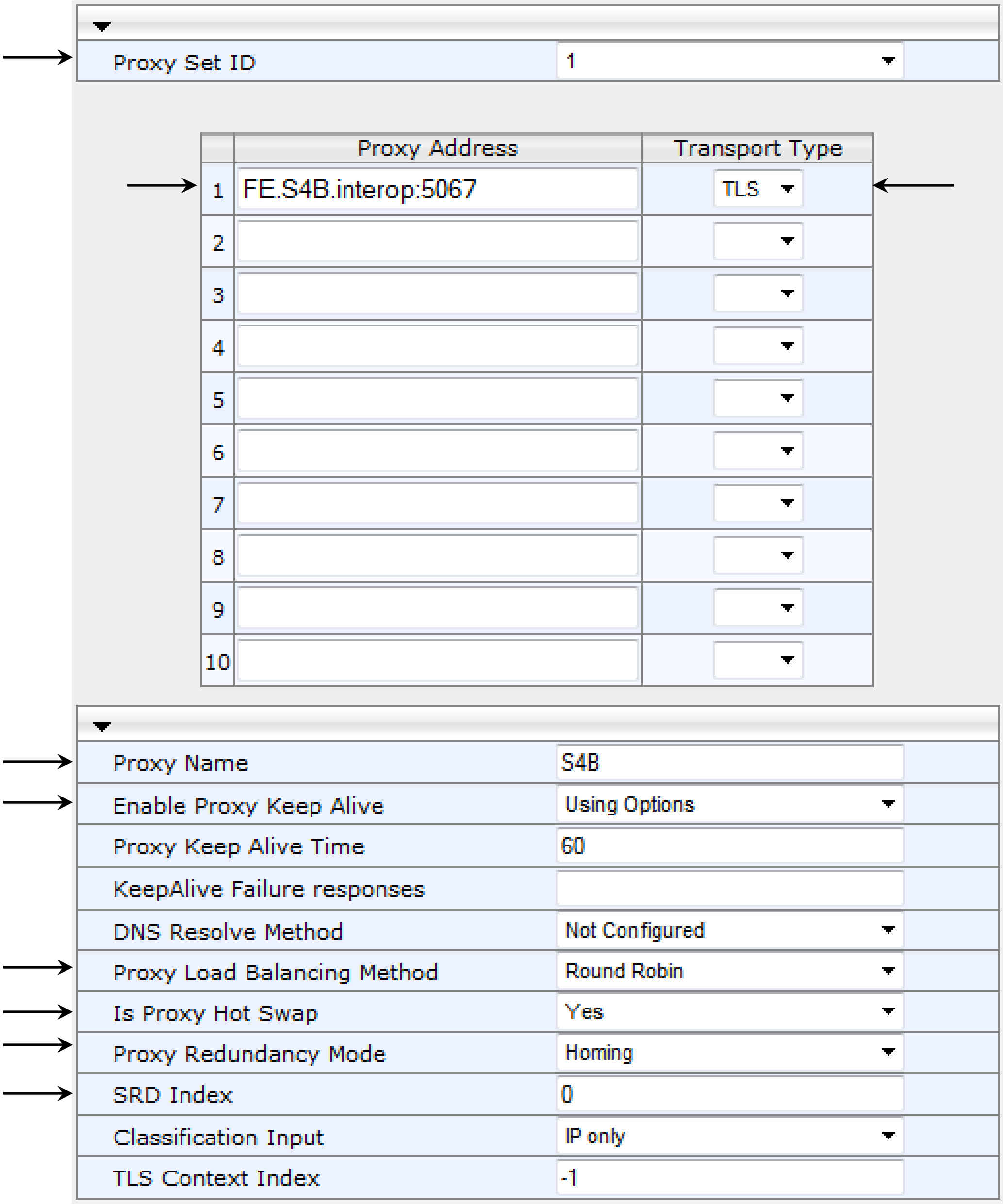
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➤ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the Skype for Business Server 2015 as shown below:

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**FE.S4B.interop:5067** (Skype for Business Server 2015 IP address / FQDN and destination port)
Transport Type	**TLS**
Proxy Name	**S4B** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
Proxy Redundancy Mode	**Homing**
SRD Index	**0**

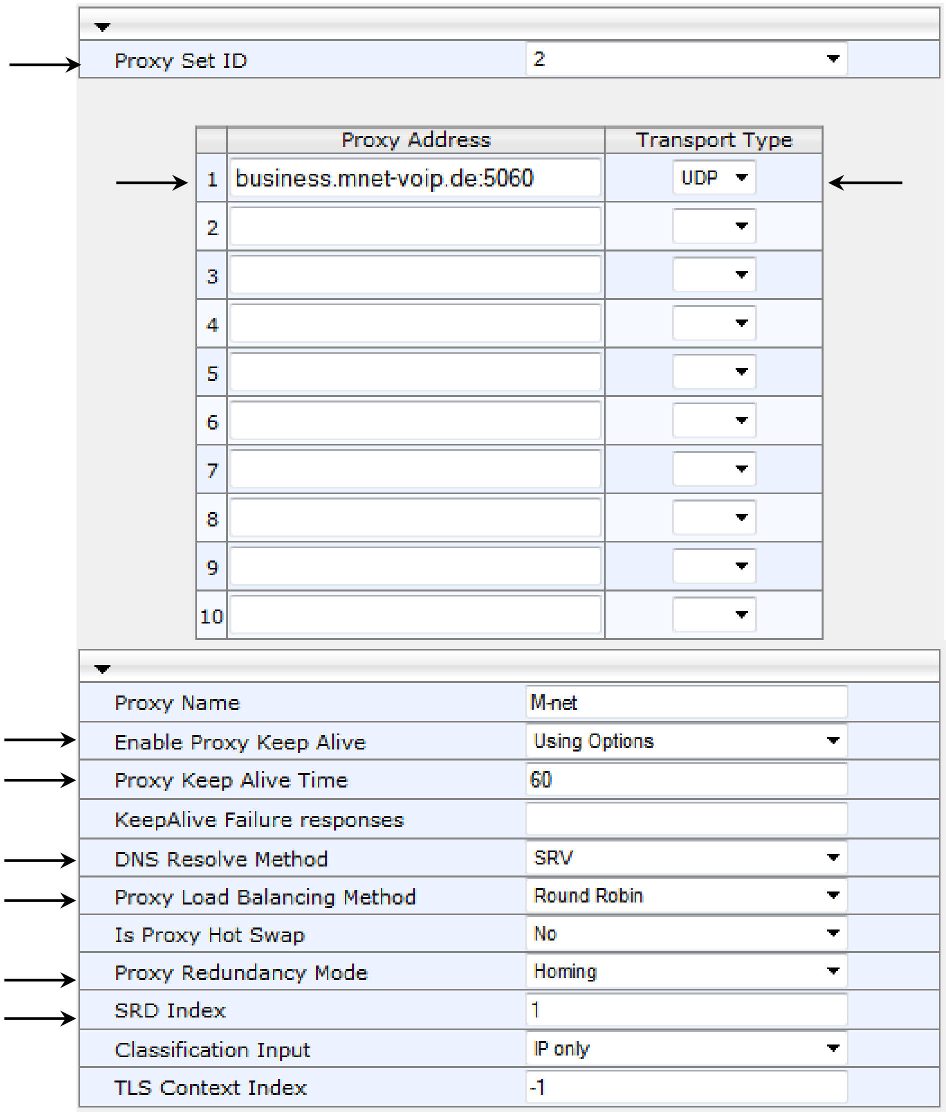
Figure 4-11: Configuring Proxy Set for Microsoft Skype for Business Server 2015



3. Configure a Proxy Set for the M-net SIP Trunk:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**business.mnet-voip.de** (M-net FQDN)
Transport Type	**UDP or TCP**
Proxy Name	**M-net** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
DNS Resolve Method	**SRV**
Proxy Load Balancing Method	**Round Robin**
Proxy Redundancy Mode	**Homing**
SRD Index	**1**

Figure 4-12: Configuring Proxy Set for M-net SIP Trunk



4.5 Step 5: Configure IP Groups

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

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

- Skype for Business Server 2015 (Mediation Server)
- M-net SIP Trunk

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the Skype for Business Server 2015 as shown below:

Parameter	Value
Index	**1**
Type	**Server**
Description	**S4B** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**business.mnet-voip.de** (according to ITSP requirement)
SRD	**0**
Media Realm Name	**MRLan**
IP Profile ID	**1**

3. Configure an IP Group for the M-net SIP Trunk:

Parameter	Value
Index	**2**
Type	**Server**
Description	**M-net** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**business.mnet-voip.de** (according to ITSP requirement)
SRD	**1**
Media Realm Name	**MRWan**
IP Profile ID	**2**

The configured IP Groups are shown in the figure below:

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

IP Group Table

Add +

Index	Type	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
1	Server	S4B	1	business.mnet-voip.de			No	0
2	Server	M-net	2	business.mnet-voip.de			No	1

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

4.6 Step 6: Configure IP Profiles

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

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

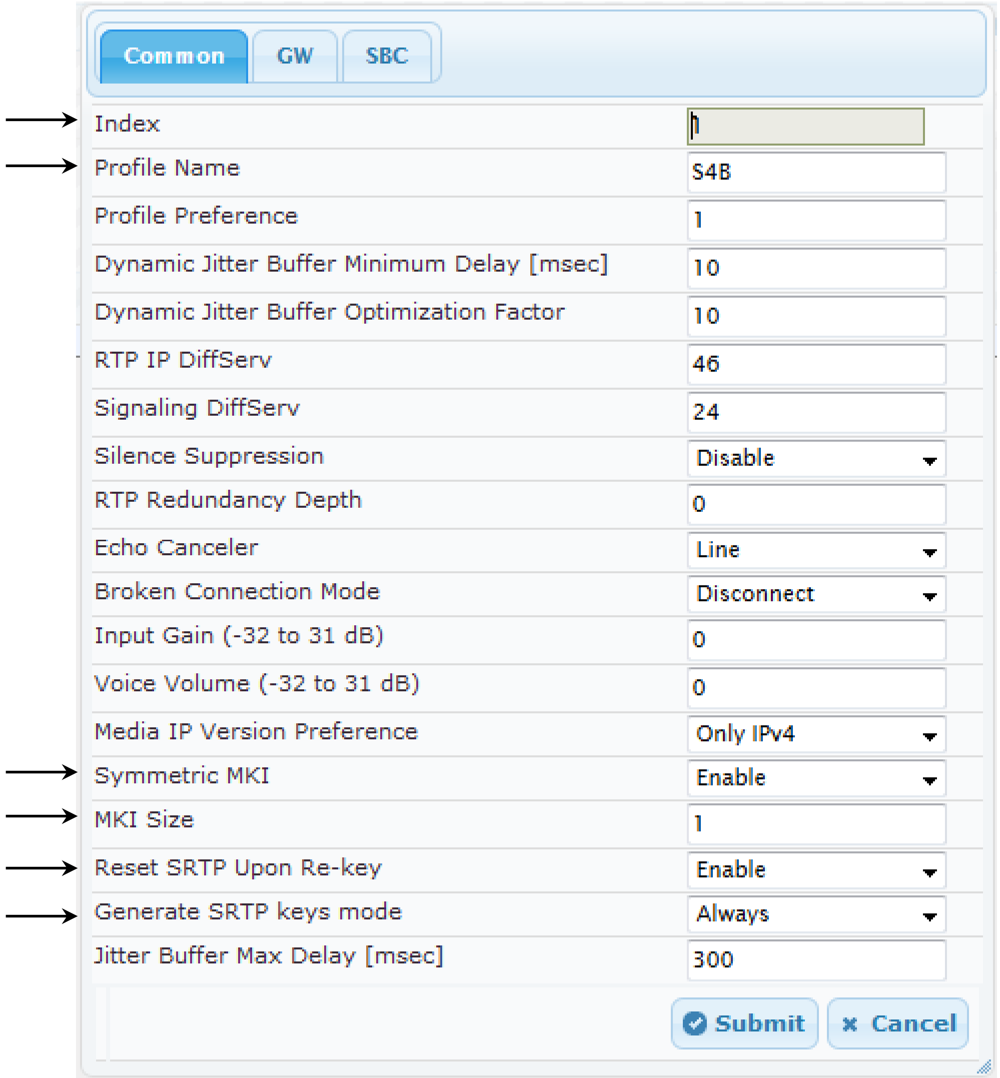
- Microsoft Skype for Business Server 2015 - to operate in secure mode using SRTP and TLS
- M-net SIP trunk - to operate in non-secure mode using RTP and UDP

➢ **To configure IP Profile for the Skype for Business Server 2015:**

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

Parameter	Value
Index	**1**
Profile Name	**S4B**
Symmetric MKI	**Enable**
MKI Size	**1**
Reset SRTP State Upon Re-key	**Enable**
Generate SRTP keys mode	**Always**

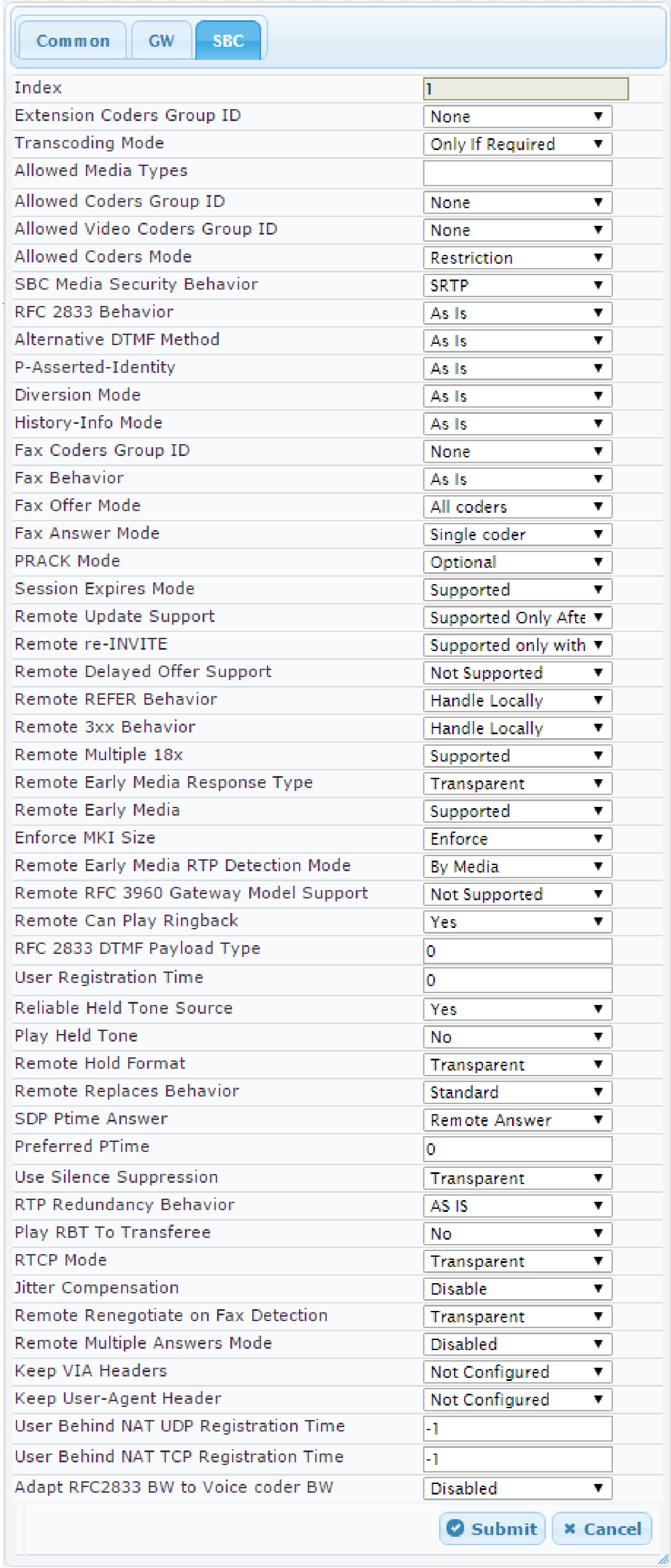
Figure 4-14: Configuring IP Profile for Skype for Business Server 2015 – Common Tab



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

Parameter	Value
SBC Media Security Behavior	**SRTP**
PRACK Mode	**Optional** (required, as M-net SIP Trunk does not generate PRACK)
Session Expires Mode	**Supported** (required, as M-net SIP Trunk does not support Session Timer)
Remote Update Support	**Supported Only After Connect**
Remote re-INVITE	**Supported Only with SDP**
Remote Delayed Offer Support	**Not Supported**
Remote REFER Behavior	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP REFER)
Remote 3xx Behavior	**Handle Locally** (required, as Skype for Business Server 2015 does not support receipt of SIP 3xx responses)
Enforce MKI Size	**Enforce**
Remote Early Media RTP Detection Mode	**By Media** (required, as Skype for Business Server 2015 does not send RTP immediately to remote side when it sends a SIP 18x response)

Figure 4-15: Configuring IP Profile for Skype for Business Server 2015 – SBC Tab



Common | GW | SBC

Index	1
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
Allowed Coders Group ID	None
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
SBC Media Security Behavior	SRTP
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Optional
Session Expires Mode	Supported
Remote Update Support	Supported Only Afte
Remote re-INVITE	Supported only with
Remote Delayed Offer Support	Not Supported
Remote REFER Behavior	Handle Locally
Remote 3xx Behavior	Handle Locally
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
Enforce MKI Size	Enforce
Remote Early Media RTP Detection Mode	By Media
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Transparent
Remote Replaces Behavior	Standard
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Transparent
Remote Multiple Answers Mode	Disabled
Keep VIA Headers	Not Configured
Keep User-Agent Header	Not Configured
User Behind NAT UDP Registration Time	-1
User Behind NAT TCP Registration Time	-1
Adapt RFC2833 BW to Voice coder BW	Disabled

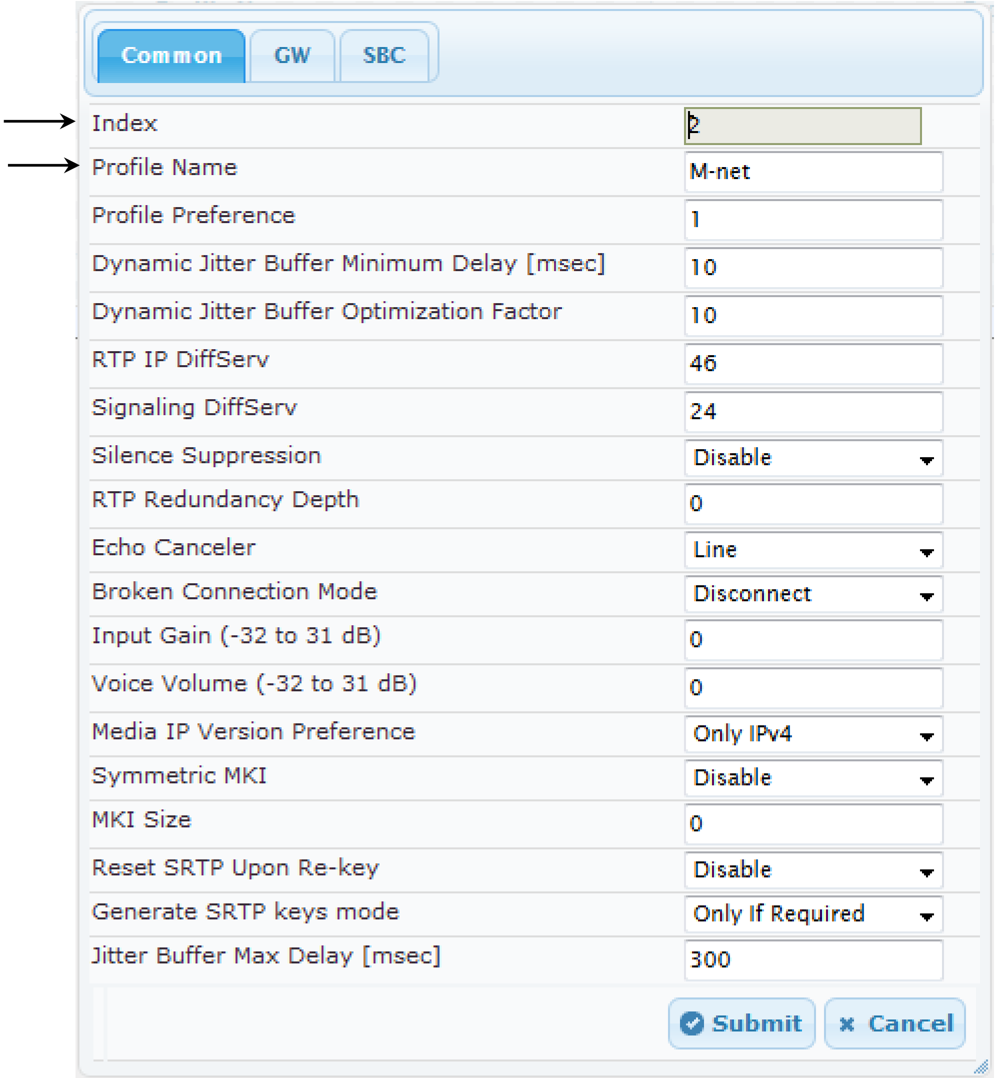
Submit | Cancel

➢ To configure an IP Profile for the M-net SIP Trunk:

1. Click **Add**.
2. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Profile Name	**M-net**

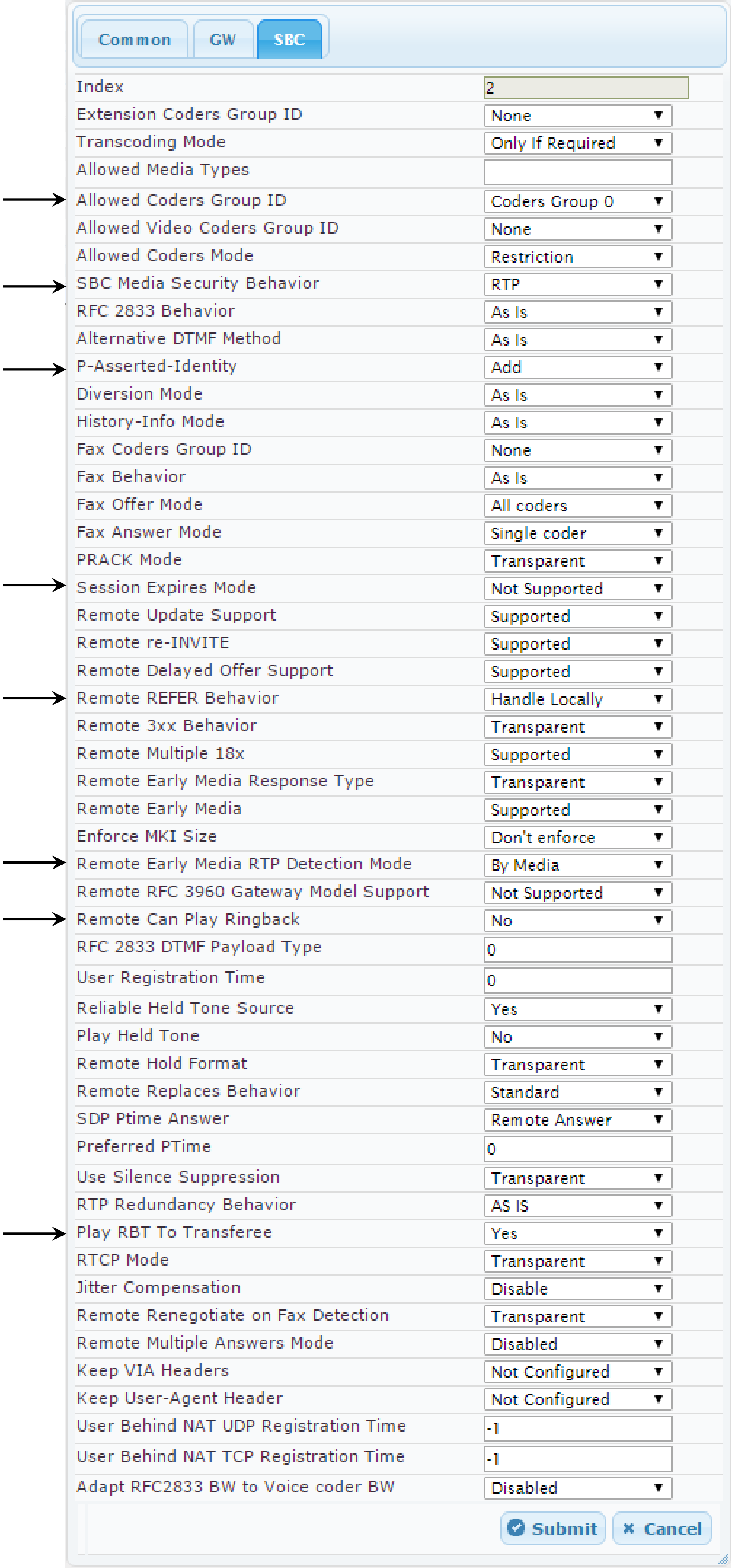
Figure 4-16: Configuring IP Profile for M-net SIP Trunk – Common Tab



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

Parameter	Value
Allowed Coders Group ID	**Coders Group 0**
SBC Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** (required for anonymous calls)
Session Expires Mode	**Not Supported** (required, as M-net SIP Trunk does not support Session Timer)
Remote REFER Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Remote Early Media RTP Detection Mode	**By Media** (required, in order to send pre-recorded ringback tone)
Remote Can Play Ringback	**No**
Play RBT To Transferee	**Yes**

Figure 4-17: Configuring IP Profile for M-net SIP Trunk – SBC Tab



4.7 Step 7: Configure Coders

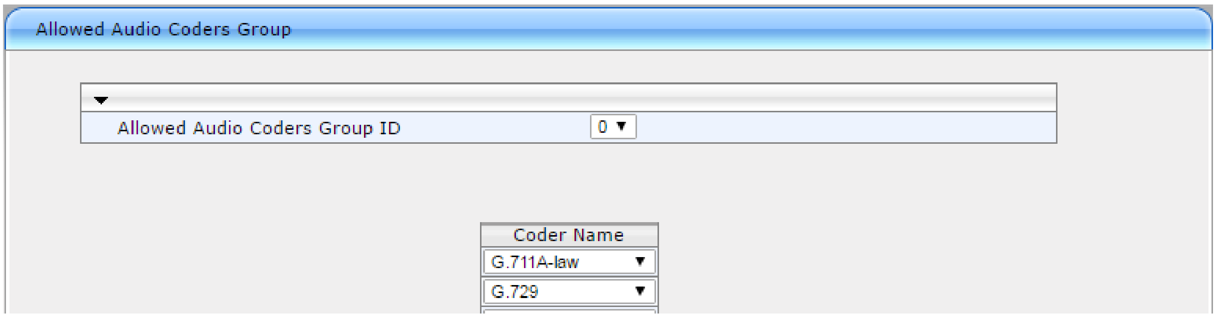
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the M-net SIP Trunk uses the G.711A-law and G.729 coders only. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the M-net SIP Trunk (see Section 4.5 on page 43).

➢ **To set a preferred coders for the M-net SIP Trunk:**

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

Parameter	Value
Allowed Audio Coders Group ID	**0**
Coder Name	**G.711A-law**
Coder Name	**G.729**

Figure 4-18: Configuring Allowed Coders Group for M-net SIP Trunk



4.8 Step 8: SIP TLS Connection Configuration

This section describes how to configure the E-SBC for using a TLS connection with the Skype for Business Server 2015 Mediation Server. This is essential for a secure SIP TLS connection.

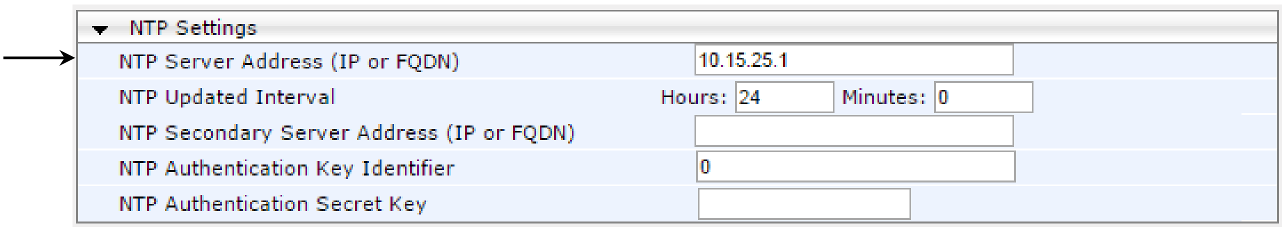
4.8.1 Step 8a: Configure the NTP Server Address

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

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

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

Figure 4-19: Configuring NTP Server Address



3. Click **Submit**.

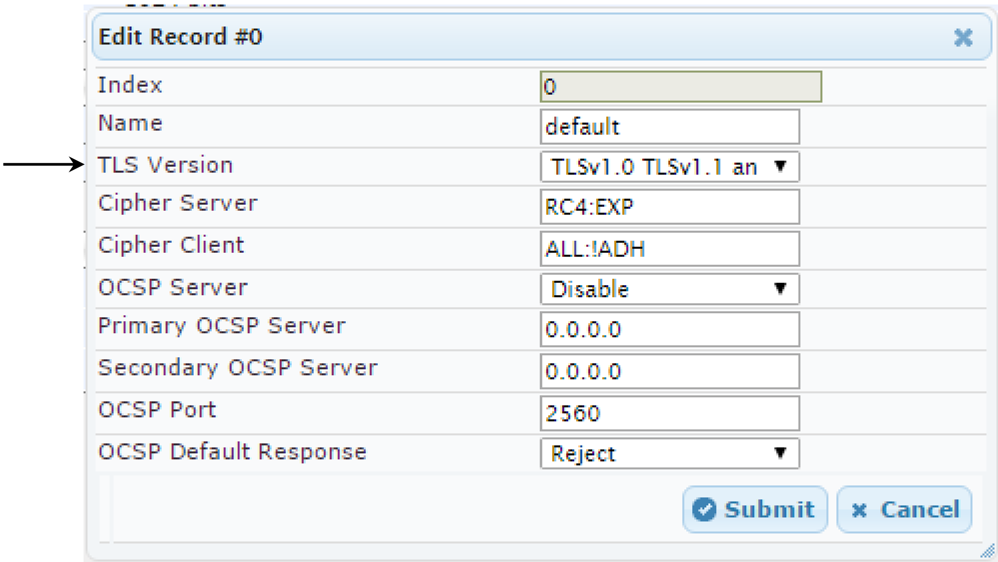
4.8.2 Step 8b: Configure the TLS version

This step describes how to configure the E-SBC to use TLS only. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ **To configure the TLS version:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click 'Edit'.
3. From the '**TLS Version**' drop-down list, select '**TLSv1.0 TLSv1.1 and TLSv1.2**'.

Figure 4-20: Configuring TLS version



4. Click **Submit**.

4.8.3 Step 8c: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA). The certificate is used by the E-SBC to authenticate the connection with Skype for Business Server 2015.

The procedure involves the following main steps:

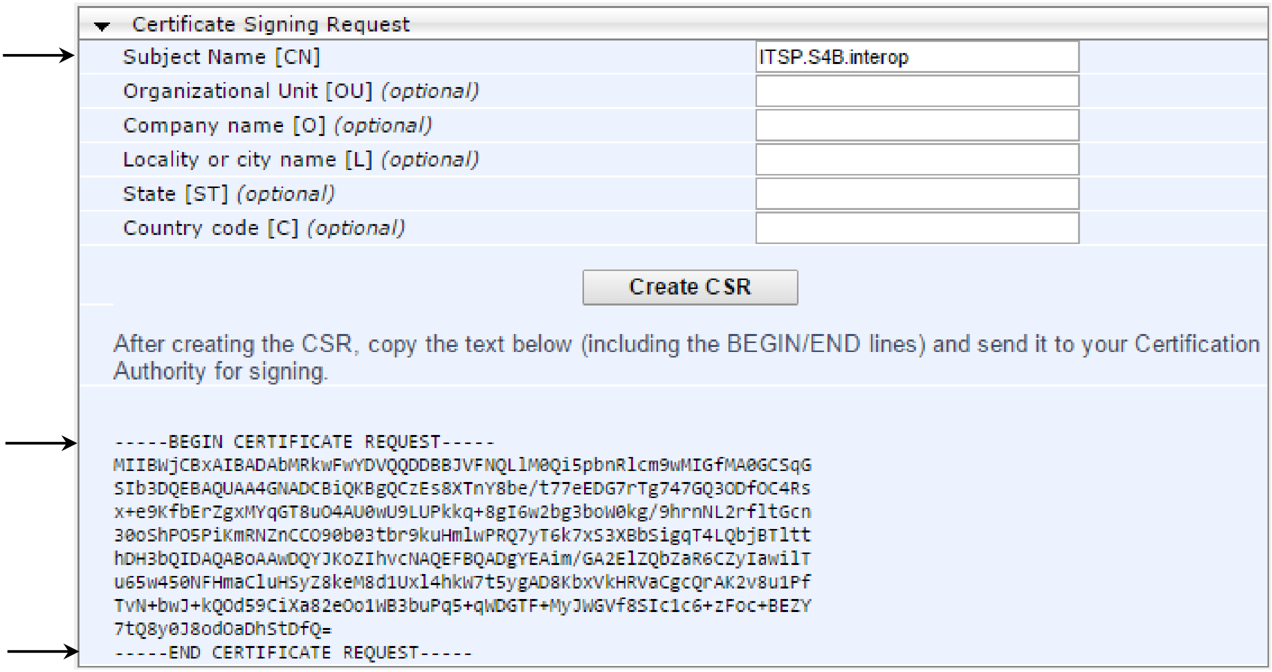
a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root Certificate from CA.
d. Deploying Device and Trusted Root Certificates on E-SBC.

Note: The Subject Name (CN) field parameter should be identically configured in the DNS Active Directory and Topology Builder (see Section 3.1 on page 13).

➢ **To configure a certificate:**

1. Open the TLS Contexts page (**Configuration** tab > **System** menu > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
   a. In the 'Subject Name [CN]' field, enter the E-SBC FQDN name (e.g., **ITSP.S4B.interop**).
   b. Fill in the rest of the request fields according to your security provider's instructions.
4. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

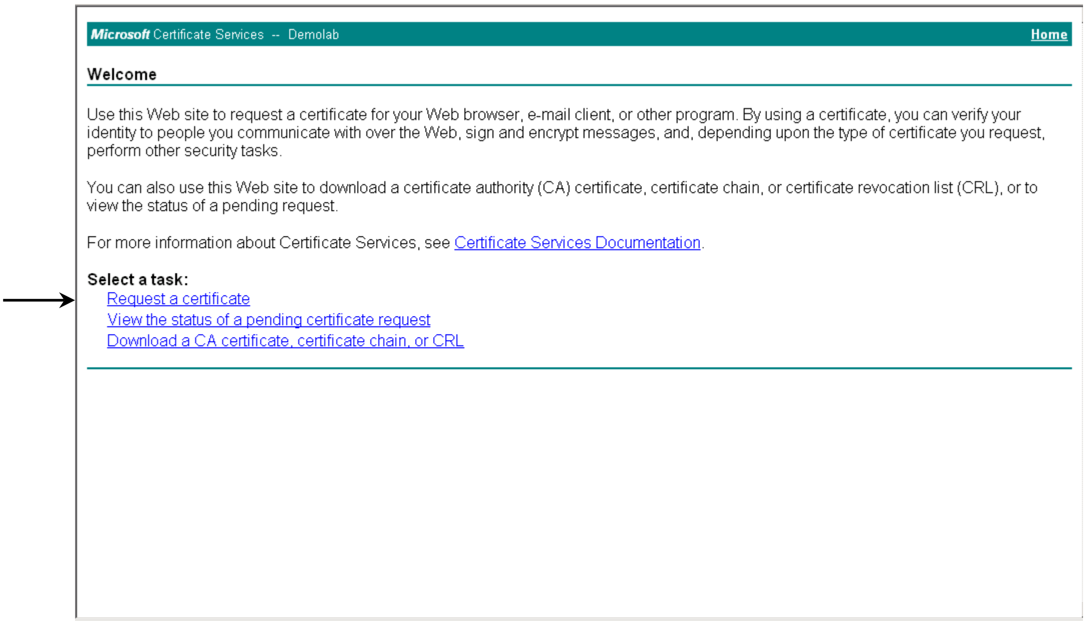
Figure 4-21: Certificate Signing Request – Creating CSR



> **Note:** The value entered in this field must be identical to the gateway name configured in the Topology Builder for Skype for Business Server 2015 (see Section 3.1 on page 13).

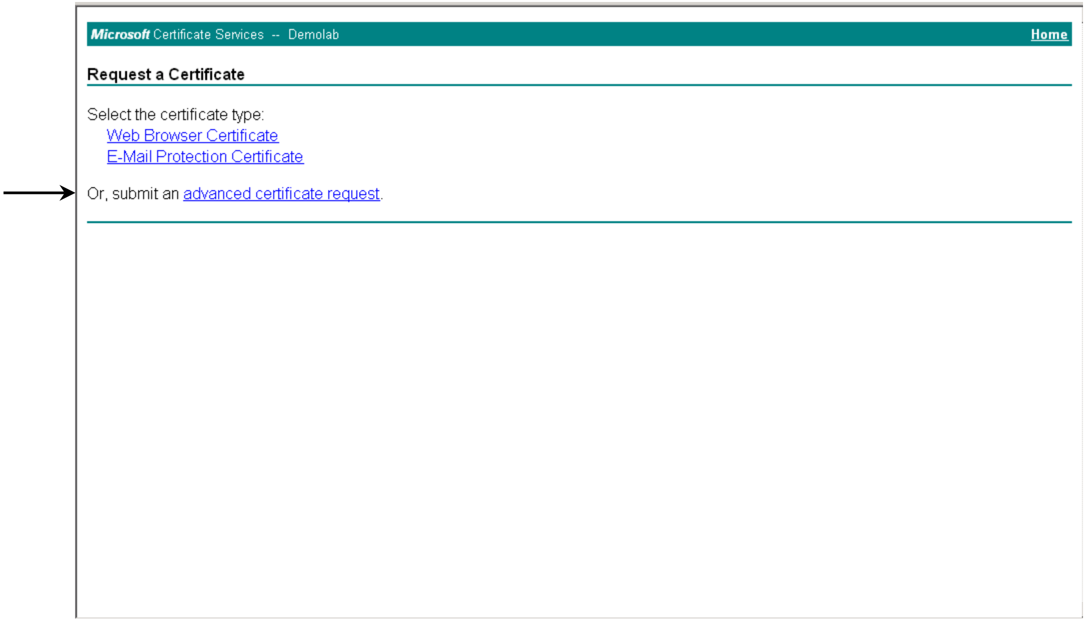
5. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----"** to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.
7. Click **Request a certificate**.

Figure 4-22: Microsoft Certificate Services Web Page



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

Figure 4-23: Request a Certificate Page



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

Figure 4-24: Advanced Certificate Request Page

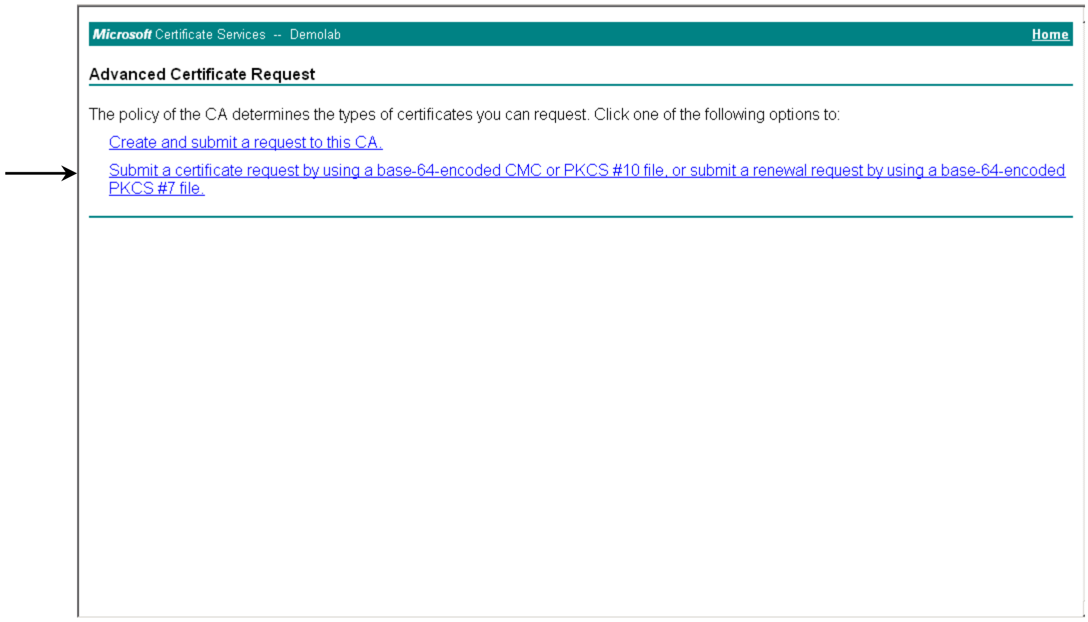
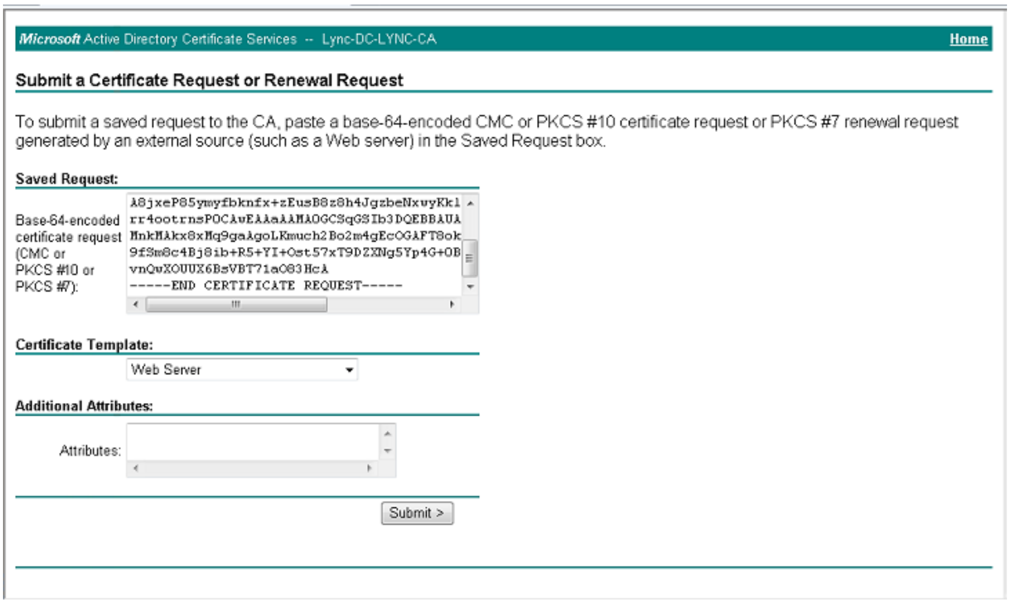
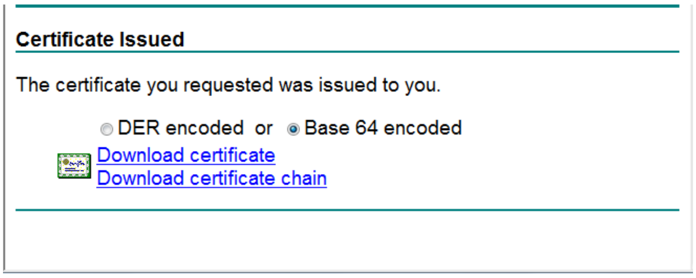


Figure 4-25: Submit a Certificate Request or Renewal Request Page



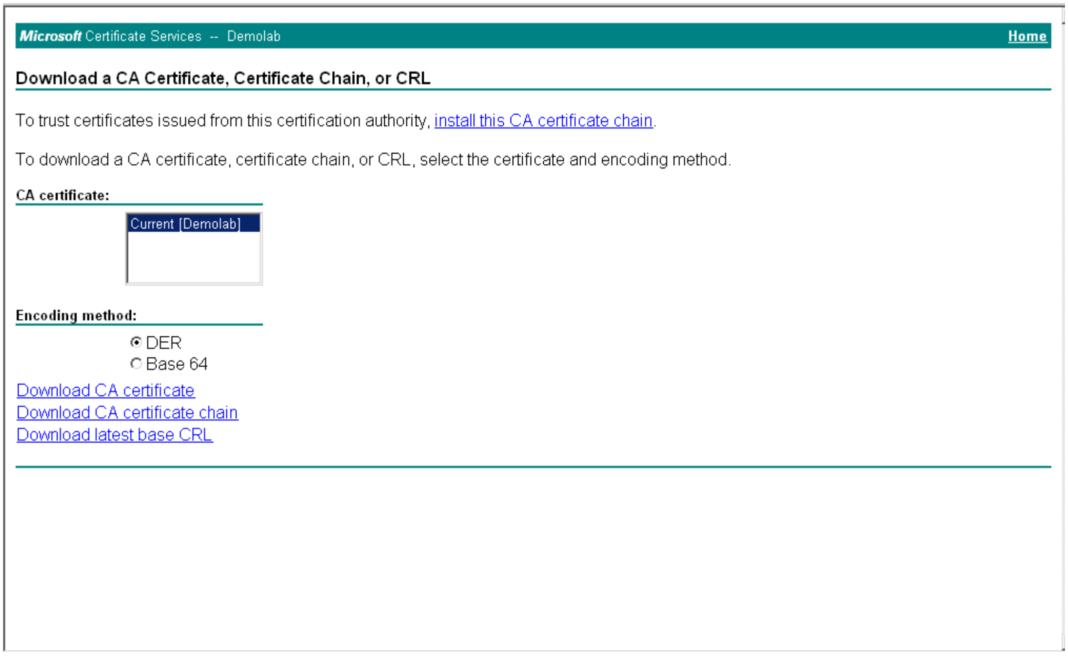
10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.
11. From the 'Certificate Template' drop-down list, select **Web Server**.
12. Click **Submit**.

Figure 4-26: Certificate Issued Page



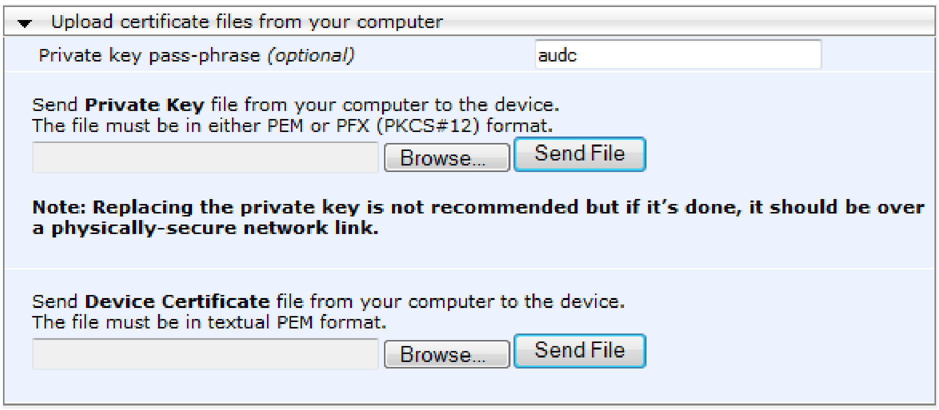
13. Select the **Base 64 encoded** option for encoding, and then click **Download certificate**.
14. Save the file as *gateway.cer* to a folder on your computer.
15. Click the **Home** button or navigate to the certificate server at http://<Certificate Server>/CertSrv.
16. Click **Download a CA certificate**,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

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



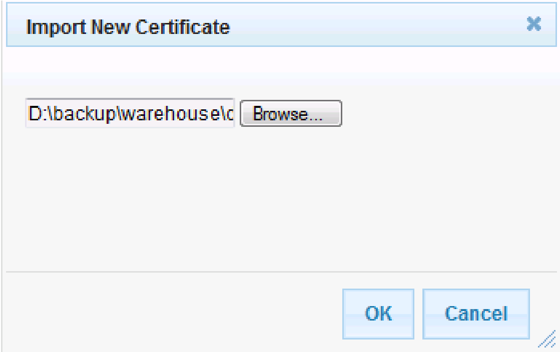
17. Under the 'Encoding method' group, select the **Base 64** option for encoding.
18. Click **Download CA certificate**.
19. Save the file as *certroot.cer* to a folder on your computer.
20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
    a. In the TLS Contexts table, select the required TLS Context index row (typically, the default TLS Context at Index 0 is used), and then click the **TLS Context Certificates** button, located at the bottom of the TLS Contexts page; the Context Certificates page appears.
    b. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate file that you saved on your computer in Step 14, and then click **Send File** to upload the certificate to the E-SBC.

Figure 4-28: Upload Device Certificate Files from your Computer Group



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

Figure 4-29: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 85).

4.9 Step 9: Configure SRTP

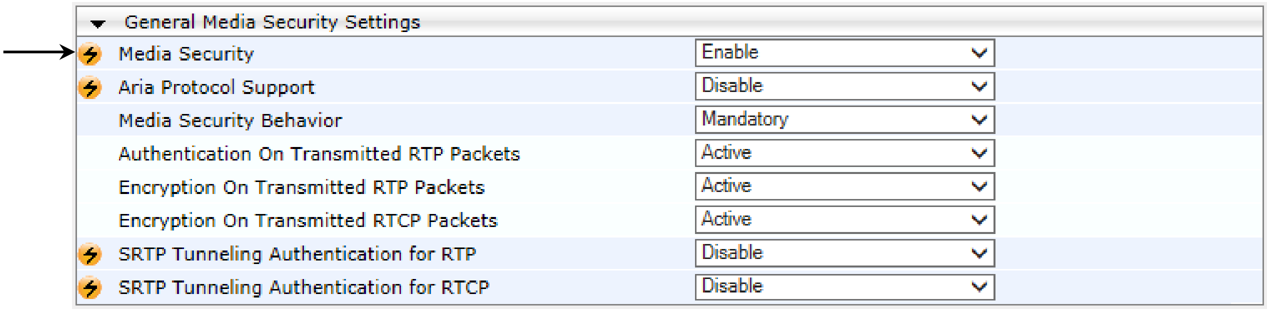
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Skype for Business Server 2015 when you configured an IP Profile for Skype for Business Server 2015 (see Section 4.5 on page 43).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**

Figure 4-30: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.15 on page 85).

4.10 Step 10: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 43, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents M-net SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business Server 2015 (LAN) and M-net SIP Trunk (WAN):

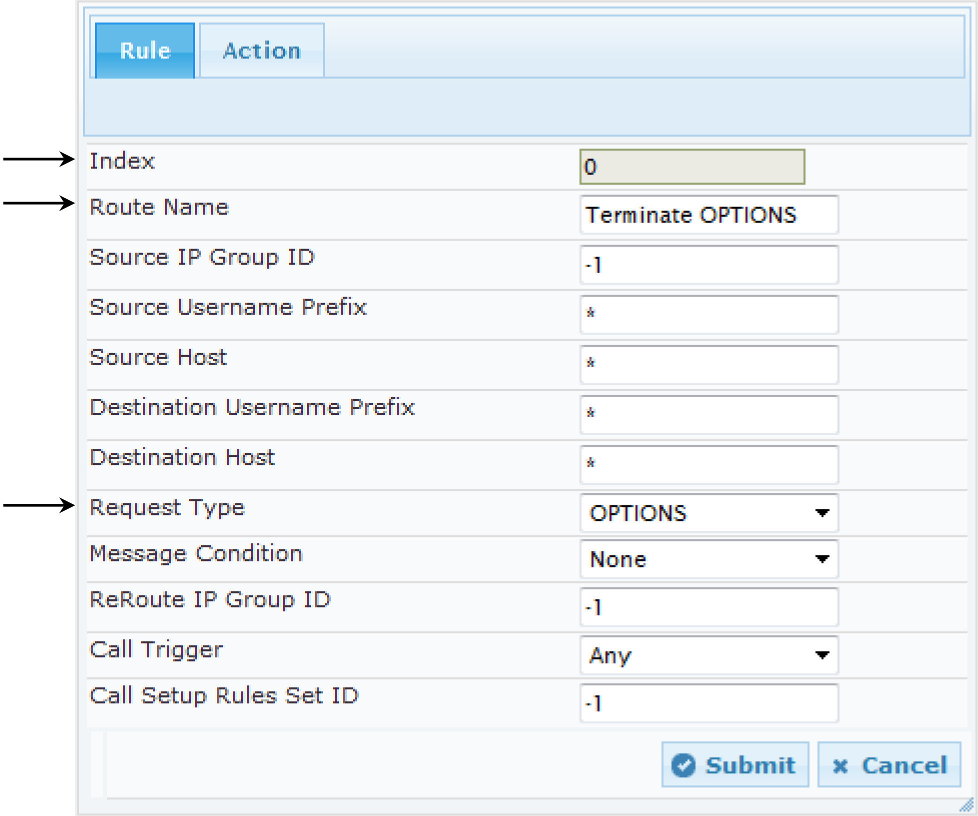
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Skype for Business Server 2015 to M-net SIP Trunk
- Calls from M-net SIP Trunk to Skype for Business Server 2015

➢ To configure IP-to-IP routing rules:

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

Parameter	Value
Index	**0**
Route Name	**Terminate OPTIONS** (arbitrary descriptive name)
Request Type	**OPTIONS**

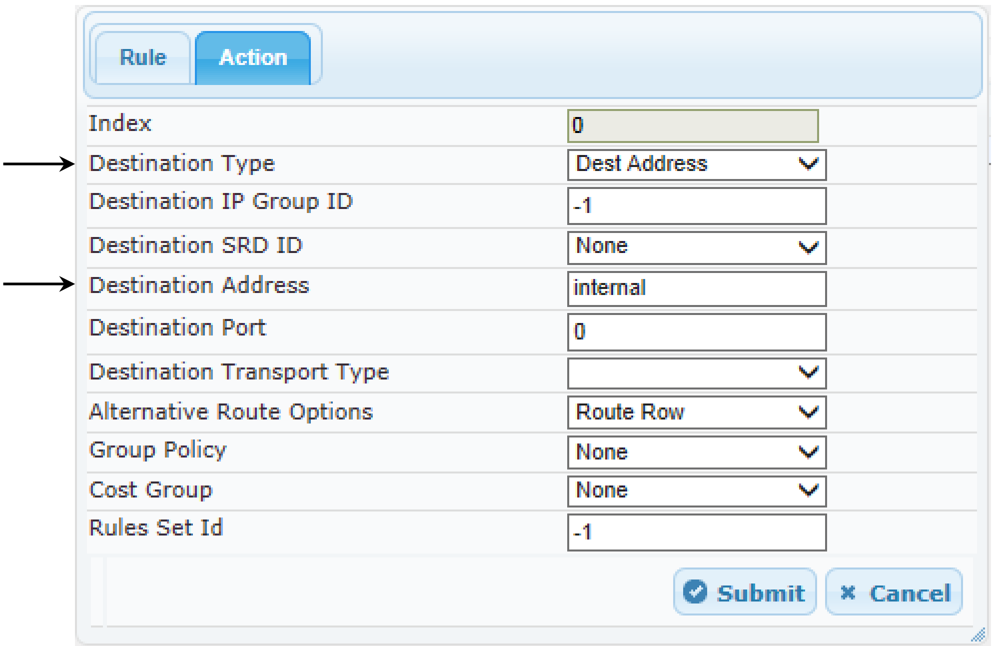
Figure 4-31: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS – Rule Tab



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

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

Figure 4-32: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS – Action Tab



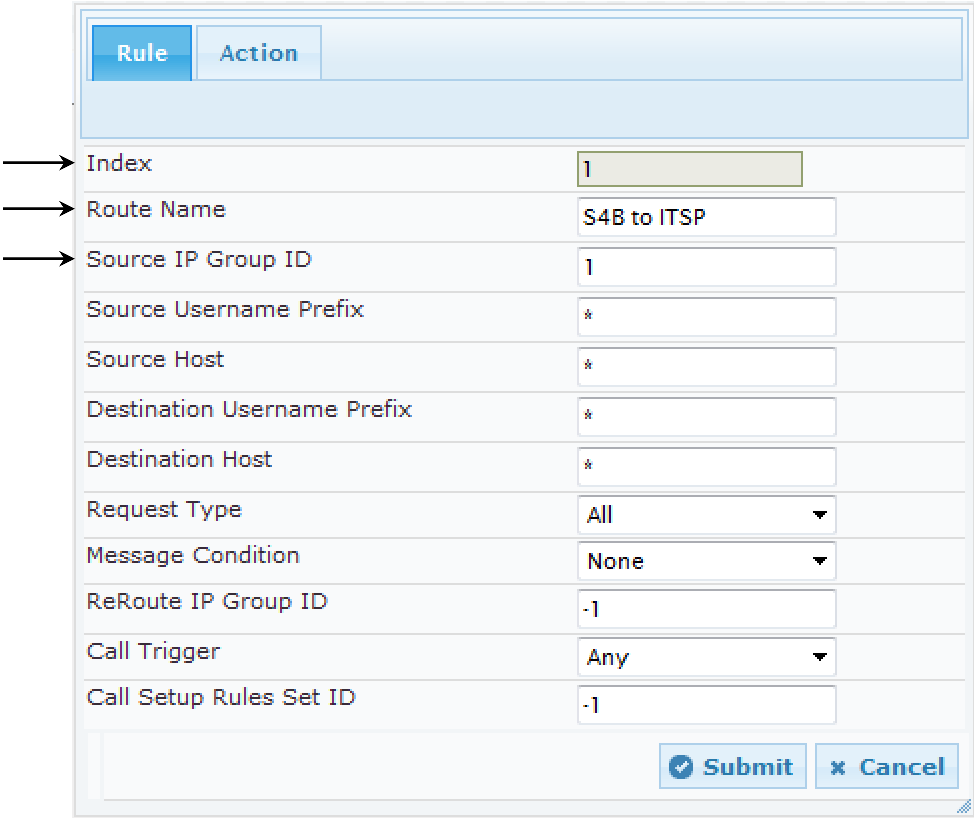
3. Configure a rule to route calls from Skype for Business Server 2015 to M-net SIP Trunk:

   a. Click **Add**.

   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Route Name	**S4B to ITSP** (arbitrary descriptive name)
Source IP Group ID	**1**

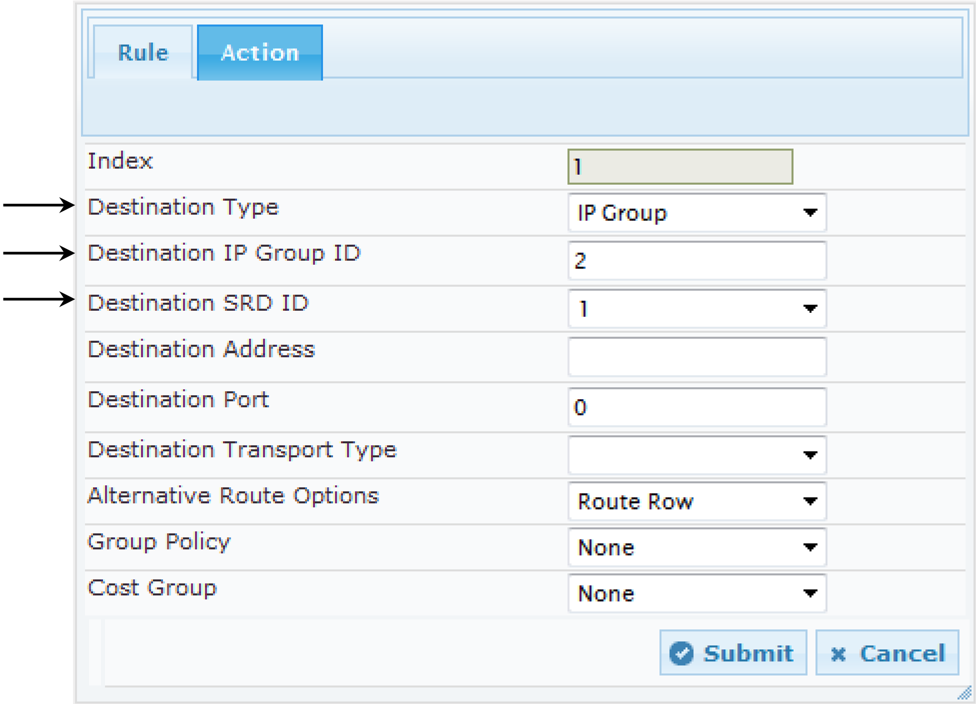
Figure 4-33: Configuring IP-to-IP Routing Rule for S4B to ITSP – Rule tab



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

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

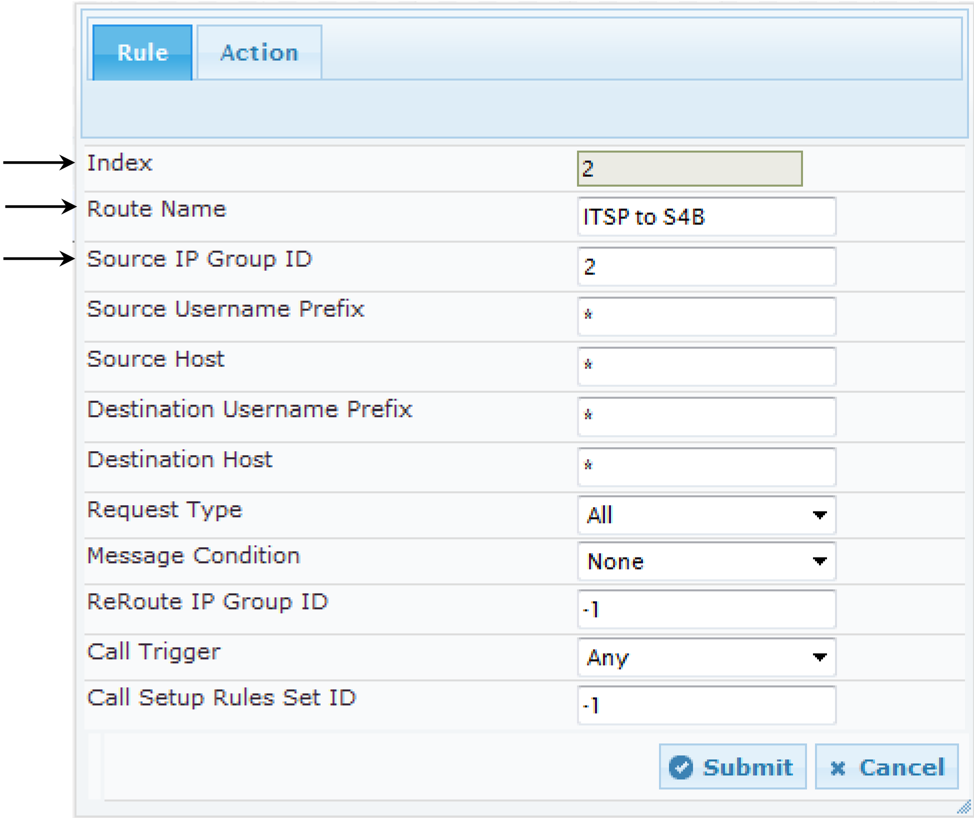
Figure 4-34: Configuring IP-to-IP Routing Rule for S4B to ITSP – Action tab



5. To configure rule to route calls from M-net SIP Trunk to Skype for Business Server 2015:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Route Name	**ITSP to S4B** (arbitrary descriptive name)
Source IP Group ID	**2**

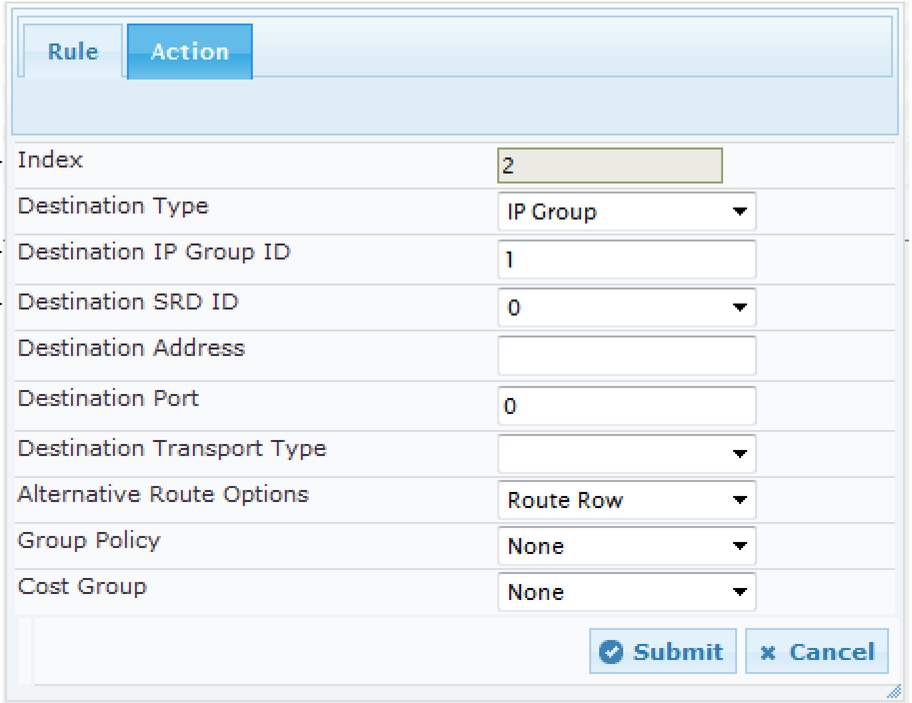
Figure 4-35: Configuring IP-to-IP Routing Rule for ITSP to S4B – Rule tab



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

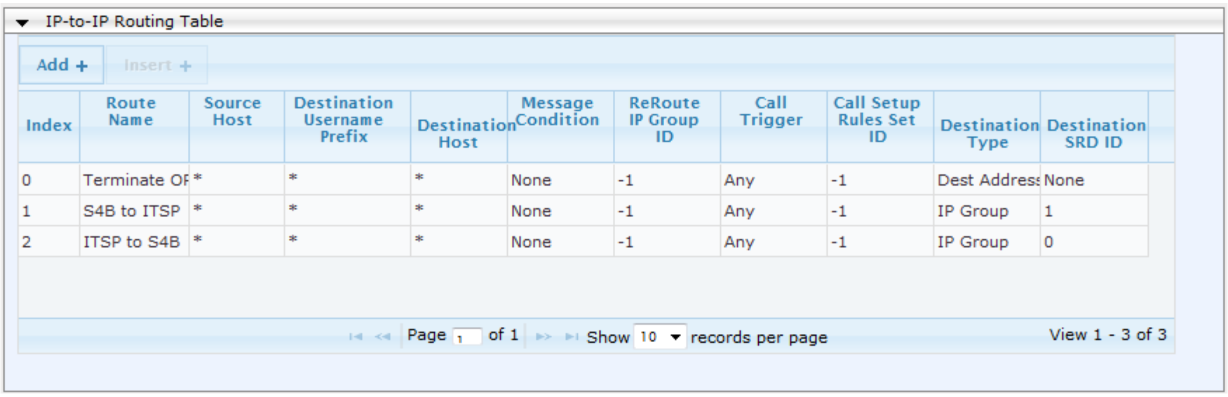
Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**0**

Figure 4-36: Configuring IP-to-IP Routing Rule for ITSP to S4B – Action tab



The configured routing rules are shown in the figure below:

Figure 4-37: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



IP-to-IP Routing Table

Add + Insert +

Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination SRD ID
0	Terminate OF	*	*	*	None	-1	Any	-1	Dest Address	None
1	S4B to ITSP	*	*	*	None	-1	Any	-1	IP Group	1
2	ITSP to S4B	*	*	*	None	-1	Any	-1	IP Group	0

Page 1 of 1 Show 10 records per page View 1 - 3 of 3

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

4.11 Step 11: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 43, IP Group 1 represents Skype for Business Server 2015, and IP Group 2 represents M-net SIP Trunk.

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

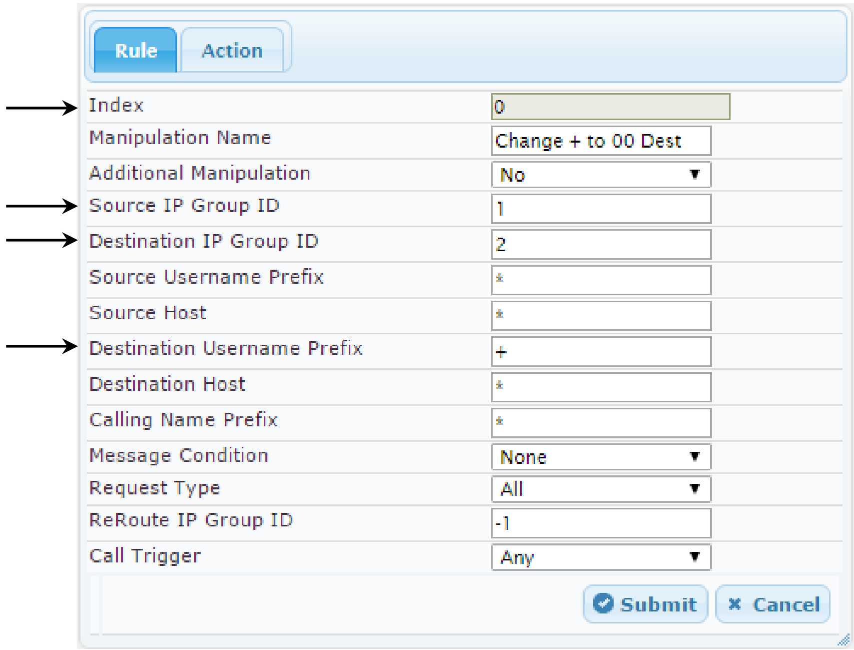
For this interoperability test topology, a manipulation is configured to replace the "+" (plus sign) by “00” in the destination number for calls from the Skype for Business Server 2015 IP Group to the M-net SIP Trunk IP Group for the destination username prefix "+".

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

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

Parameter	Value
Index	**0**
Source IP Group	**1**
Destination IP Group	**2**
Destination Username Prefix	**+** (plus sign)

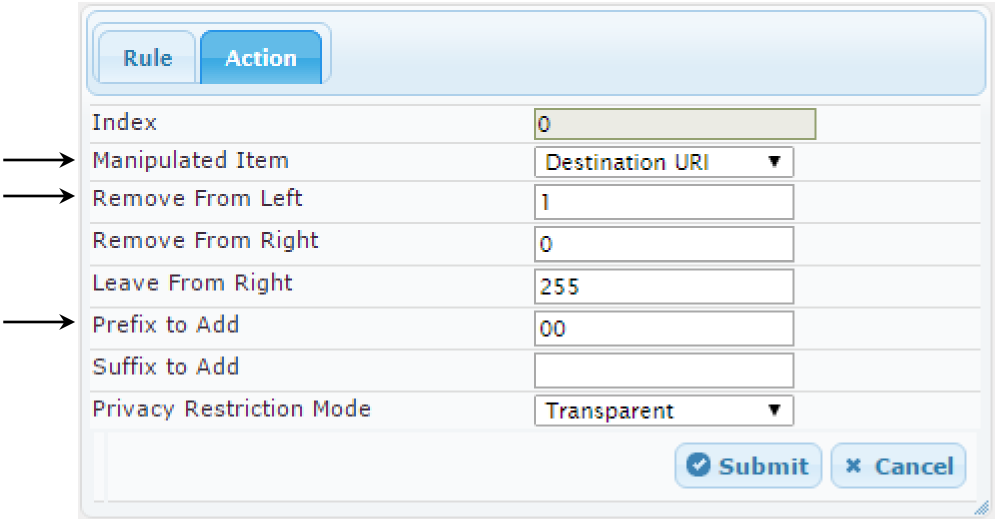
Figure 4-38: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Value
Manipulated Item	**Destination URI**
Remove From Left	**1**
Prefix to Add	**00**

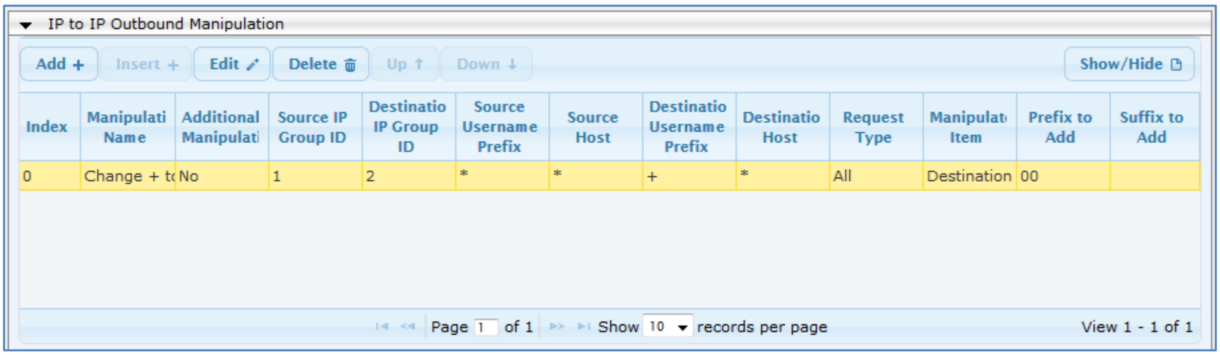
Figure 4-39: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP Group 1 (i.e., Skype for Business Server 2015) and IP Group 2 (i.e., M-net SIP Trunk):

Figure 4-40: Example of Configured IP-to-IP Outbound Manipulation Rules



4.12 Step 12: Configure Message Manipulation Rules

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

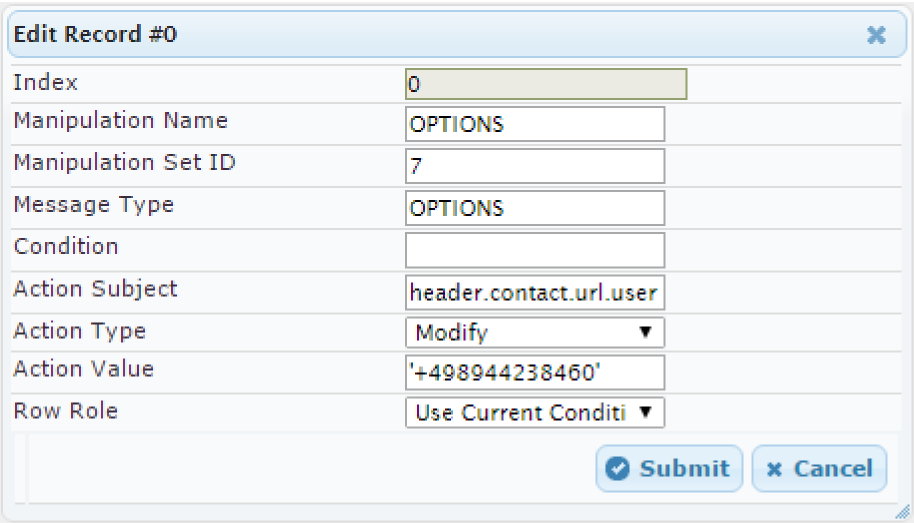
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 7). This rule applies to SIP OPTIONS messages sent from E-SBC toward M-net SIP Trunk. This replaces the user part of the SIP Contact Header with the value of 'pilot user'.

Parameter	Value
Index	**0**
Manipulation Name	**OPTIONS**
Manipulation Set ID	**7**
Message Type	**OPTIONS**
Condition	
Action Subject	**header.contact.url.user**
Action Type	**Modify**
Action Value	**'+498944238460'**

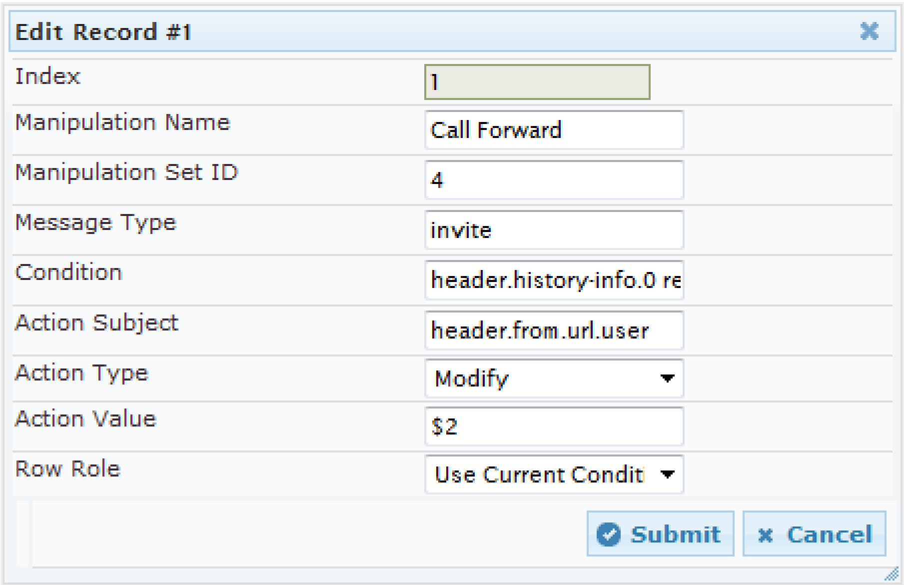
Figure 4-41: Configuring SIP Message Manipulation Rule 0 (for OPTIONS)



3. Configure another manipulation rule (Manipulation Set 4) for M-net SIP Trunk. This rule is applied to messages sent to the M-net SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This replaces the user part of the SIP From Header with the value from the SIP History-Info Header.

Parameter	Value
Index	**1**
Manipulation Name	**Call Forward**
Manipulation Set ID	**4**
Message Type	**invite**
Condition	**header.history-info.0 regex (<sip:)(.*)(@)(.*)**
Action Subject	**header.from.url.user**
Action Type	**Modify**
Action Value	**$2**

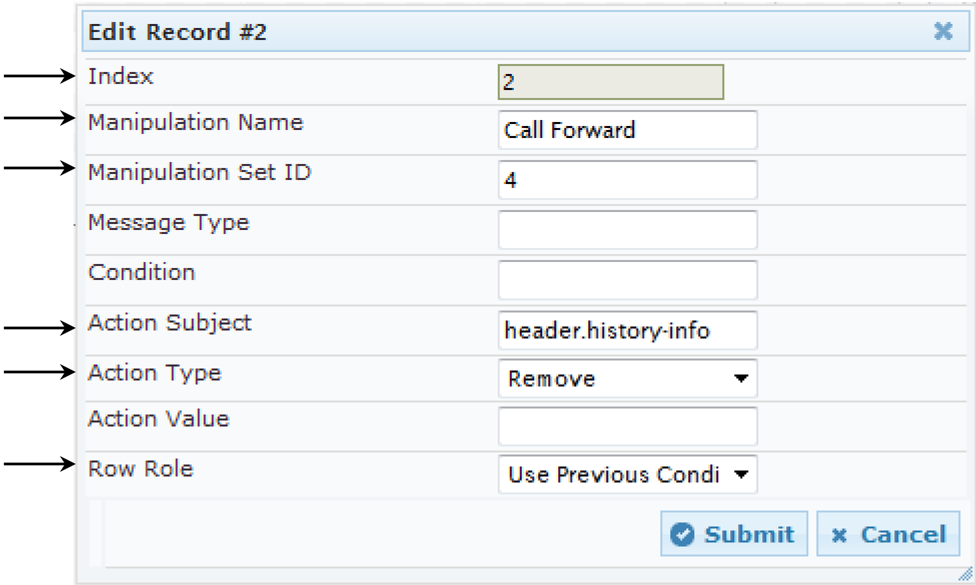
Figure 4-42: Configuring SIP Message Manipulation Rule 1 (for M-net SIP Trunk)



4. If the manipulation rule Index 1 (above) is executed, then the following rule is also executed. This rule is applied to messages sent to the M-net SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This removes the SIP History-Info Header.

Parameter	Value
Index	**2**
Manipulation Name	**Call Forward**
Manipulation Set ID	**4**
Action Subject	**header.history-info**
Action Type	**Remove**
Row Role	**Use Previous Condition**

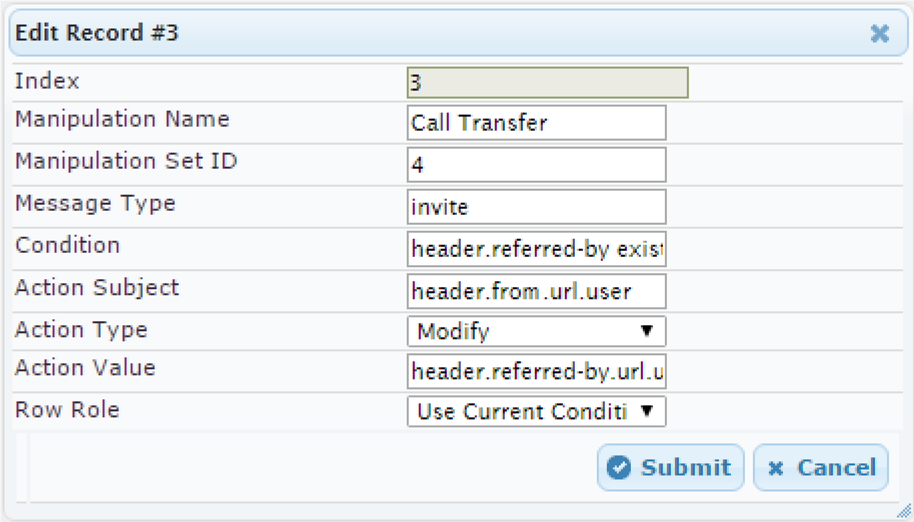
Figure 4-43: Configuring SIP Message Manipulation Rule 2 (for M-net SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 4) for M-net SIP Trunk. This rule is applied to messages sent to the M-net SIP Trunk IP Group during Call Transfer initiated by the Skype for Business Server 2015 IP Group. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	**3**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Message Type	**invite**
Condition	**header.referred-by exists**
Action Subject	**header.from.url.user**
Action Type	**Modify**
Action Value	**header.referred-by.url.user**

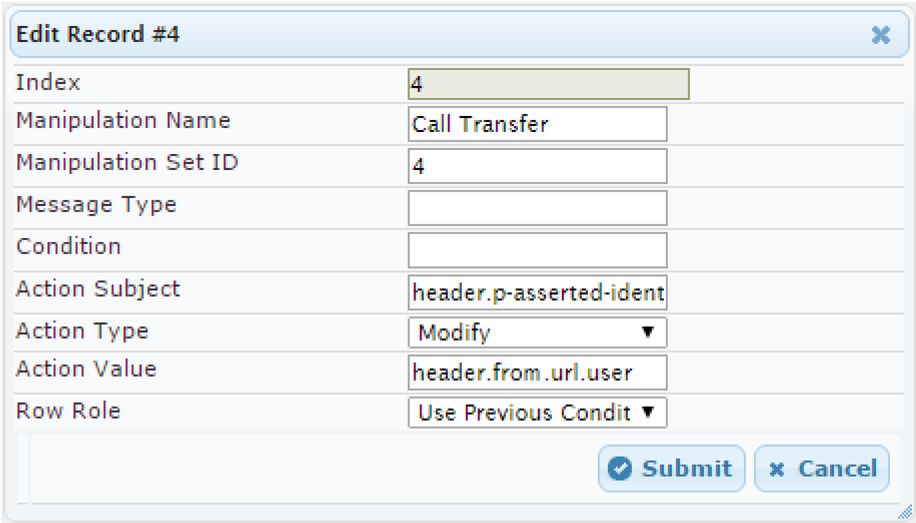
Figure 4-44: Configuring SIP Message Manipulation Rule 3 (for M-net SIP Trunk)



6. If manipulation rule Index 4 (above) is executed, then the following rule is also executed. This rule is applied to messages sent to the M-net SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP From Header.

Parameter	Value
Index	**4**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Action Subject	**header.p-asserted-identity.url.user**
Action Type	**Modify**
Action Value	**header.from.url.user**
Row Role	**Use Previous Condition**

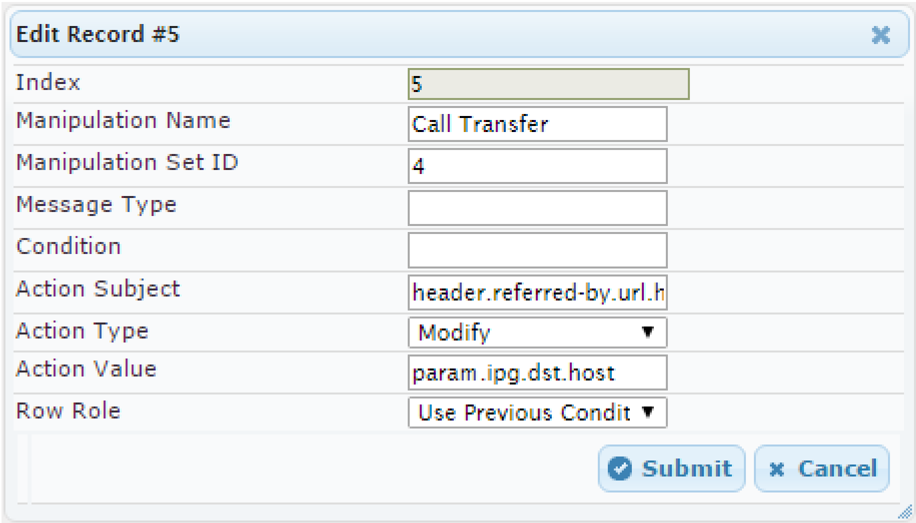
Figure 4-45: Configuring SIP Message Manipulation Rule 4 (for M-net SIP Trunk)



7. If manipulation rule Index 4 (above) is executed, then the following rule is also executed. This rule is applied to messages sent to the M-net SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This replaces the host part of the SIP Referred-By Header with the value “SIP Group Name”, configured for the M-net SIP Trunk IP Group.

Parameter	Value
Index	**5**
Manipulation Name	**Call Transfer**
Manipulation Set ID	**4**
Action Subject	**header.referred-by.url.host**
Action Type	**Modify**
Action Value	**param.ipg.dst.host**
Row Role	**Use Previous Condition**

Figure 4-46: Configuring SIP Message Manipulation Rule 5 (for M-net SIP Trunk)



8. Configure another manipulation rule (Manipulation Set 4) for M-net SIP Trunk. This rule is applied to response messages sent to the M-net SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type ‘503’ or ‘603’ with the value ‘486’, because M-net SIP Trunk not recognizes ‘503’ or ‘603’ method types.

Parameter	Value
Index	**6**
Manipulation Name	**Reject Causes**
Manipulation Set ID	**4**
Message Type	**any.response**
Condition	**header.request-uri.methodtype=='503' OR header.request-uri.methodtype=='488'**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'480'**

Figure 4-47: Configuring SIP Message Manipulation Rule 6 (for M-net SIP Trunk)

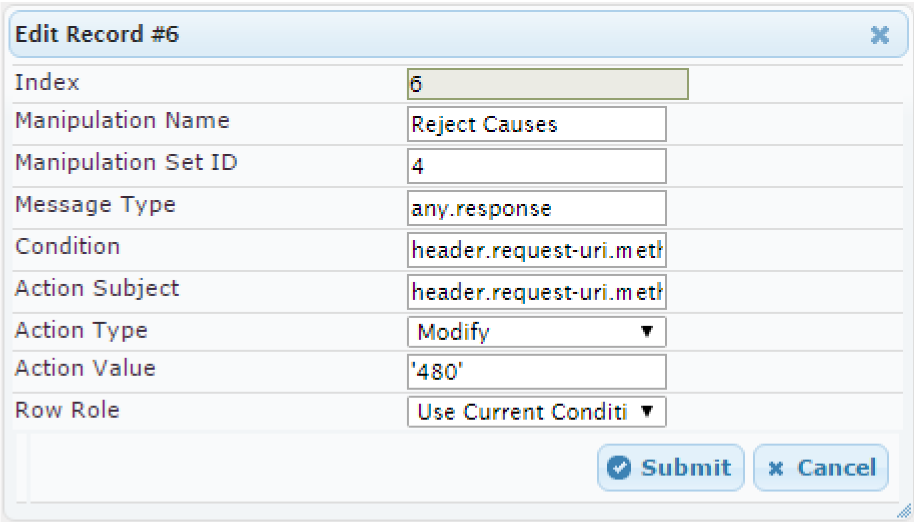


Figure 4-48: Configured SIP Message Manipulation Rules

Message Manipulations

Add + Insert +

Index	Manipulation Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	OPTIONS	7	OPTIONS		header.contact.url.use	Modify	'+498944238460'
1	Call Forward	4	invite	header.history-info.0 re	header.from.url.user	Modify	$2
2	Call Forward	4			header.history-info	Remove	
3	Call Transfer	4	invite	header.referred-by exi	header.from.url.user	Modify	header.referred-by.u
4	Call Transfer	4			header.p-asserted-ide	Modify	header.from.url.user
5	Call Transfer	4			header.referred-by.url	Modify	param.ipg.dst.host
6	Reject Causes	4	any.response	header.request-uri.met	header.request-uri.me	Modify	'480'

Page 1 of 1 Show 10 records per page View 1 - 7 of 7

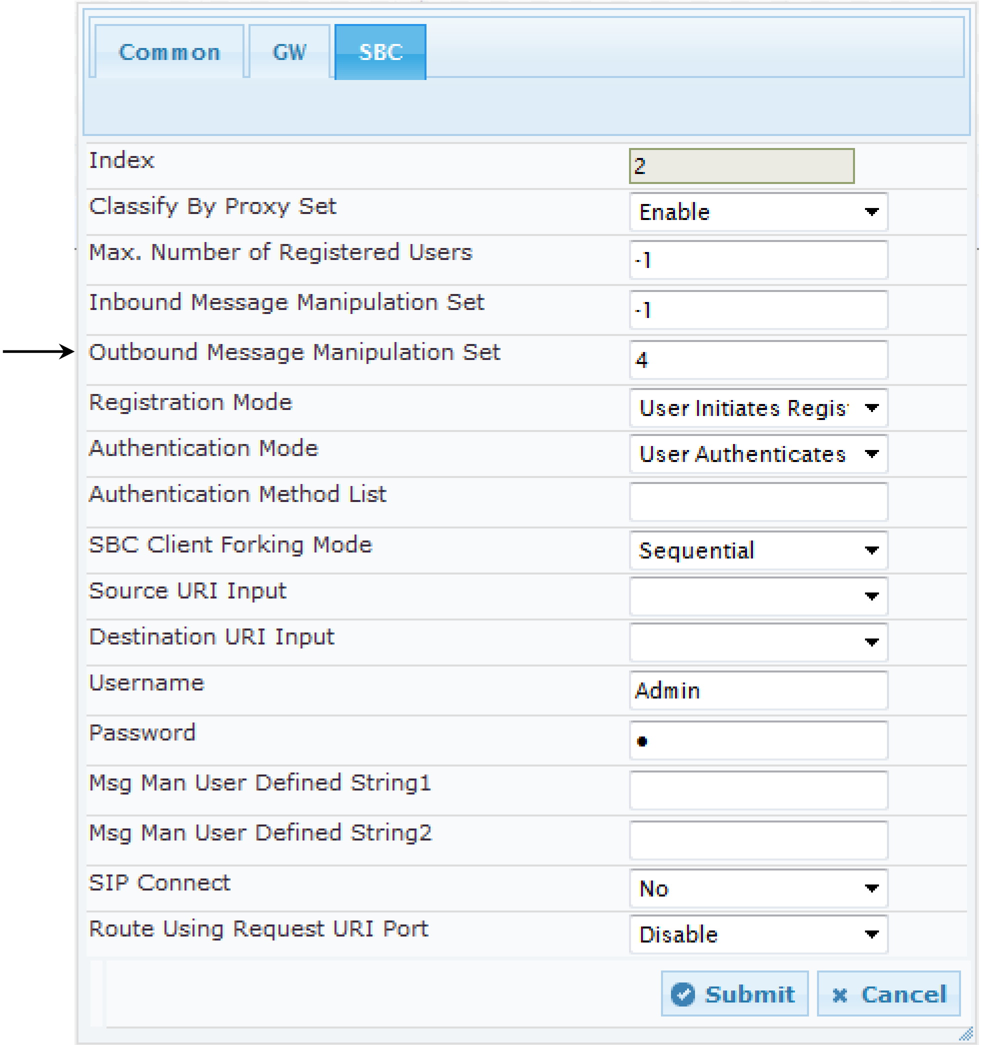
The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set ID 4 and which are executed for messages sent to the M-net SIP Trunk IP Group. These rules are specifically required to enable proper interworking between M-net SIP Trunk and Skype for Business Server 2015. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to SIP OPTIONS messages sent from the E-SBC toward M-net SIP Trunk. This replaces the user part of the SIP Contact Header with the value of 'pilot user'.	Specific format of SIP OPTIONS message, requested by M-net SIP Trunk.
1	This rule is applied to messages sent to the M-net SIP Trunk IP Group for Call Forward initiated by the Skype for Business Server 2015 IP Group. This replaces the user part of the SIP From Header with the value from the SIP History-Info Header.	For **Call Forward** scenarios, M-net SIP Trunk needs that User part in SIP From Header will be defined number. In order to do this, User part of the SIP From Header replaced with the value from History-Info Header.
2	If manipulation rule Index 1 (above) is executed, then the following rule is also executed. This removes the SIP History-Info Header.	
3	This rule is applied to messages sent to the M-net SIP Trunk IP Group during Call Transfer initiated by the Skype for Business Server 2015 IP Group. This replaces the user part of the SIP From Header with the value from the SIP Referred-By Header.	For **Call Transfer** initiated by Skype for Business Server 2015, M-net SIP Trunk needs to replace the Host part of the SIP Referred-By Header with the value from the SIP From Header and user part of the From Header with the value from Referred-By Header.
4	If manipulation rule Index 4 (above) is executed, then the following rule is also executed. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP From Header.	
5	If manipulation rule Index 4 (above) is executed, then the following rule is also executed. This replaces the host part of the SIP Referred-By Header with the value "SIP Group Name", configured for the M-net SIP Trunk IP Group.	

Rule Index	Rule Description	Reason for Introducing Rule
6	This rule is applied to response messages sent to the M-net SIP Trunk IP Group for Rejected Calls initiated by the Skype for Business Server 2015 IP Group. This replaces the method type ‘503’ or ‘488’ with the value ‘480’.	M-net SIP Trunk not recognizes ‘503’ or ‘488’ method types.

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

Figure 4-49: Assigning Manipulation Set 4 to the M-net SIP Trunk IP Group



   e. Click **Submit**.

4.13 Step 13: Configure Registration Account

This step describes how to configure the SIP registration account. This is required so that the E-SBC can register with the M-net SIP Trunk on behalf of Skype for Business Server 2015. The M-net SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Skype for Business Server 2015 (IP Group 1) and the Serving IP Group is M-net SIP Trunk (IP Group 2).

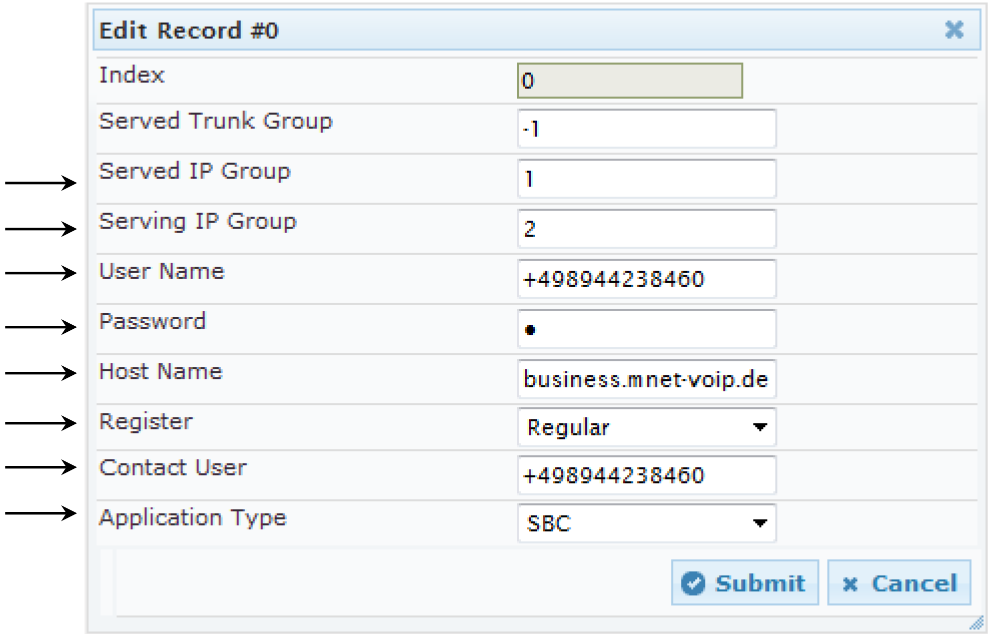
➢ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Click **Add**.
3. Configure the account according to the provided information from M-net, for example:

Parameter	Value
Served IP Group	**1** (Skype for Business Server 2015)
Serving IP Group	**2** (M-net SIP Trunk)
User Name	As provided by M-net
Password	As provided by M-net
Host Name	**business.mnet-voip.de**
Register	**Regular**
Contact User	**+498944238460** (trunk main line)
Application Type	**SBC**

4. Click **Add**.

Figure 4-50: Configuring a SIP Registration Account



➢ **To configure a registration time:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).
2. Configure 'Registration Time' parameter with appropriated value (e.g., **1200**).

Figure 4-51: Configuring a SIP Registration Time

3. Click **Submit**.

4.14 Step 14: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

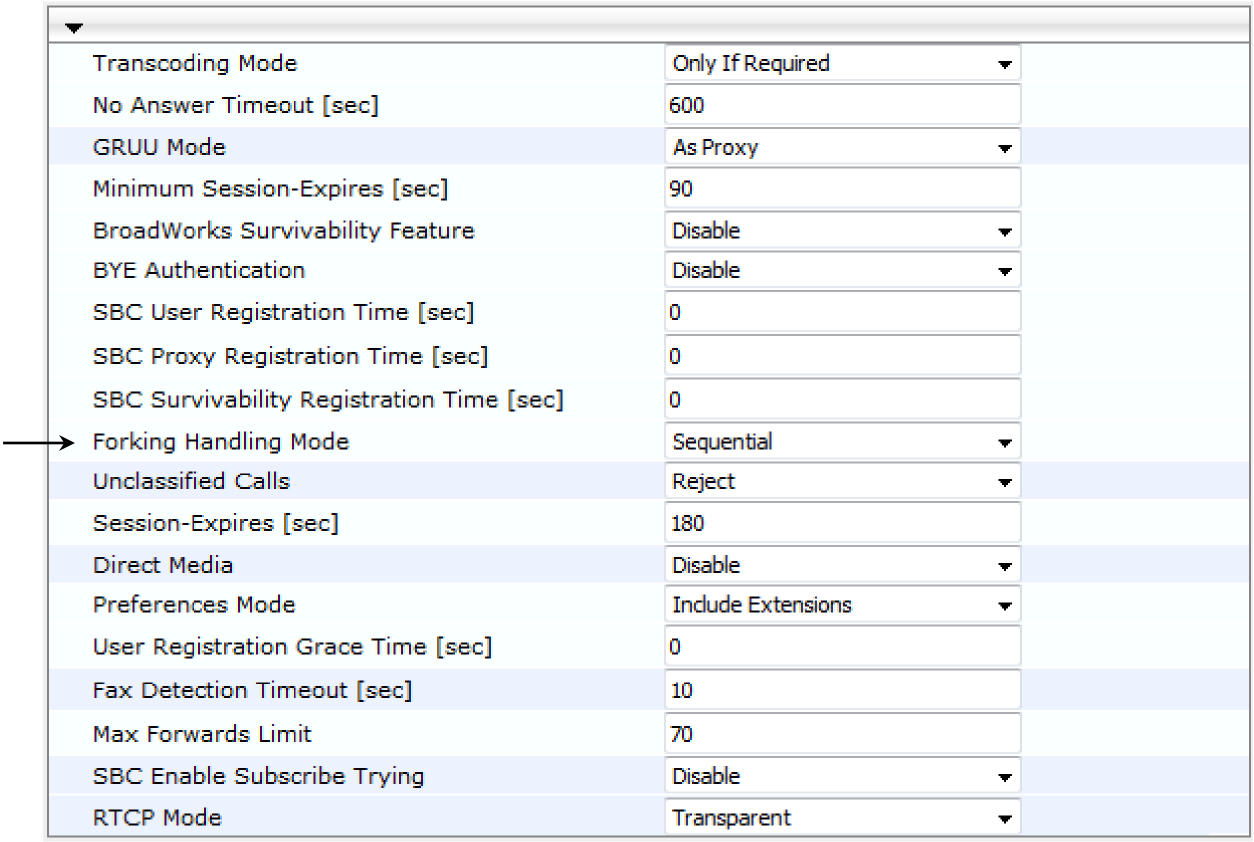
4.14.1 Step 14a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. For the interoperability test topology, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Skype for Business Server 2015 environment.

➢ **To configure call forking:**

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

Figure 4-52: Configuring Forking Mode



3. Click **Submit**.

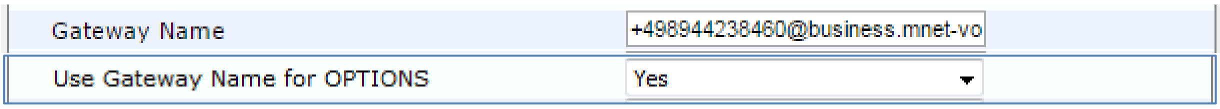
4.14.2 Step 14b: Configuration Needed for Manipulation on OPTIONS

This step describes how to configure the E-SBC to send its string name ("gateway name") in keep-alive SIP OPTIONS messages (host part of the Request-URI).

➢ **To configure Gateway Name:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**).
2. Configure 'Gateway Name' (e.g., **+498944238460@business.mnet-voip.de**).
3. From the 'Use Gateway Name for OPTIONS' drop-down list, select **Yes**.

Figure 4-53: Configuring Gateway Name



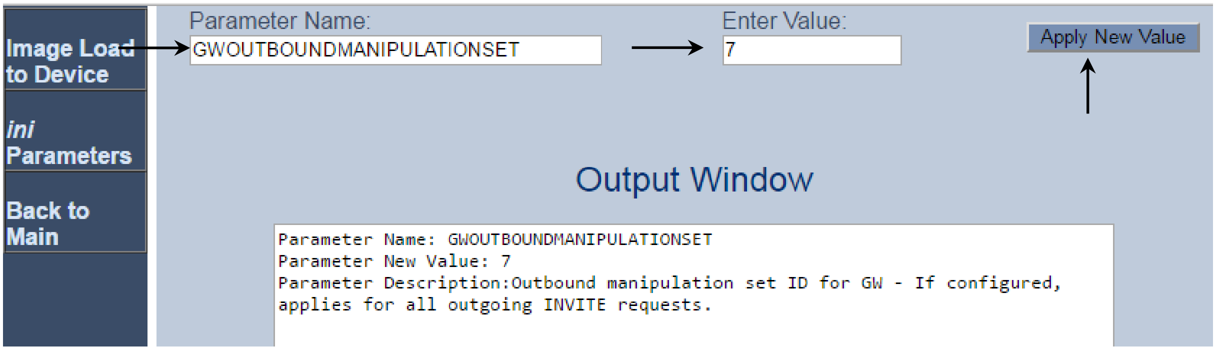
4. Click **Submit**.

The next step describes how to configure the manipulation set ID for manipulation, which needs to be done on SIP OPTIONS messages, sent towards the M-net SIP Trunk.

➢ **To configure GW Outbound Manipulation Set:**

1. Open the Admin page.
2. Append the case-sensitive suffix ‘AdminPage’ to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.10/AdminPage).
3. In the left pane of the page that opens, click ***ini*** **Parameters**.

Figure 4-54: Configuring GW Outbound Manipulation Set via AdminPage



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

Parameter	Value
GWOUTBOUNDMANIPULATIONSET	**7**

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

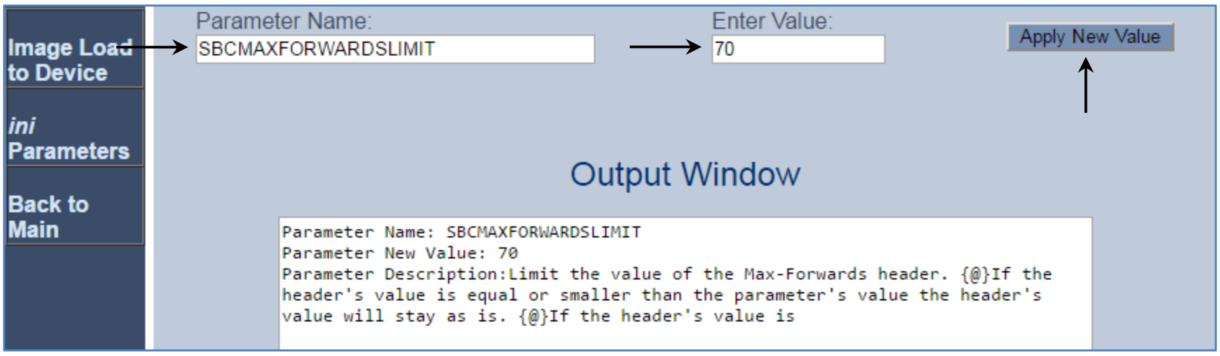
4.14.3 Step 14c: Configure Max Forwards Limit

This step describes how to configure Max Forwards Limit in the E-SBC.

➢ **To configure Max Forwards Limit:**

1. Open the Admin page.
2. Append the case-sensitive suffix ‘AdminPage’ to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.10/AdminPage).
3. In the left pane of the page that opens, click ***ini* Parameters**.

Figure 4-55: Configuring SBC Max Forwards Limit via AdminPage



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

Parameter	Value
SBCMaxForwardsLimit	**70**

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

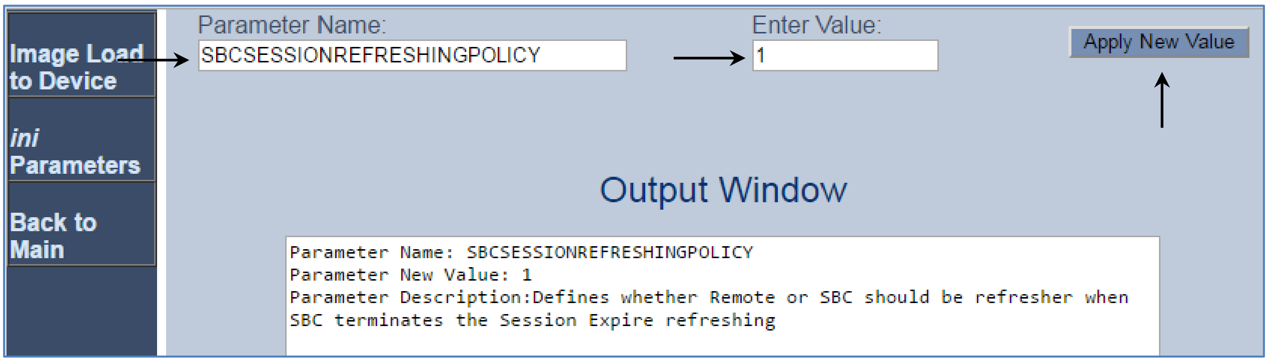
4.14.4 Step 14d: Configure SBC Session Refreshing Policy

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

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

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.17.10/AdminPage).
2. In the left pane of the page that opens, click ***ini* Parameters**.

Figure 4-56: Configuring SBC Session Refreshing Policy in AdminPage



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

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

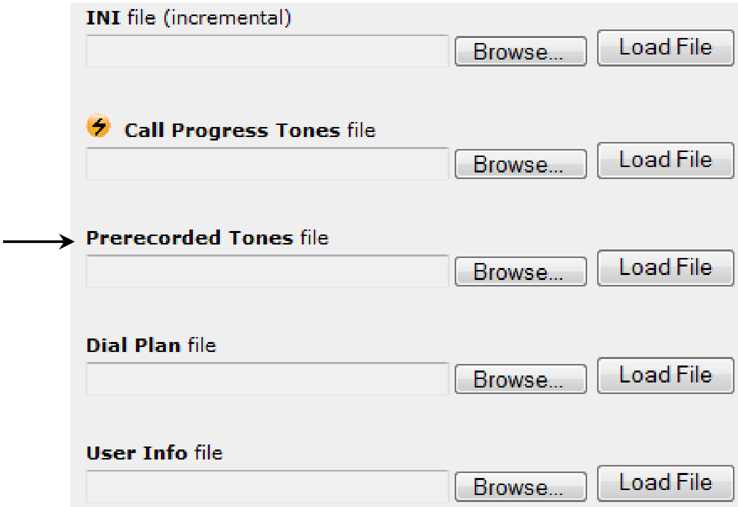
4. Click the **Apply New Value** button for each field.

4.14.5 Step 14e: Loading Prerecorded Tones File

This step describes how to load the prerecorded tones file to overcome the problem with the first incoming RTP packet in the call forwarding scenario, when the Skype for Business user forwards the call to the PSTN user. In this scenario, instead of generating a Ringback Tone as a Call Progress Tone (CPT), which requires DSP, we decided to use the Prerecorded Tones (PRT) file for ringback tones.

➢ **To load PRT file to the device using the Web interface:**

1. Open the Load Auxiliary Files page (**Maintenance** tab > **Software Update** menu > **Load Auxiliary Files**).



> **Note:** The appearance of certain file load fields depends on the installed Software License Key.

2. Click the **Browse** button corresponding to the **Prerecorded Tones** file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Save the loaded auxiliary files to flash memory.

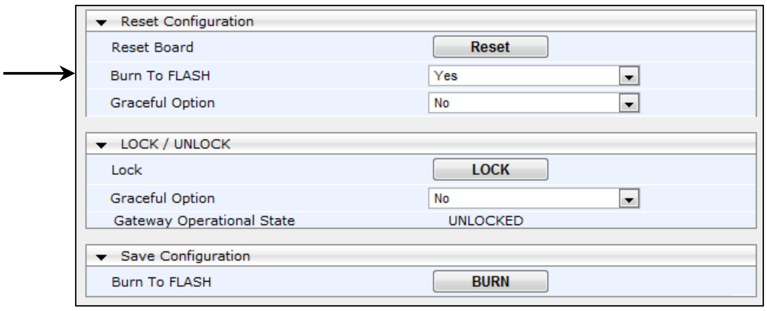
4.15 Step 15: Reset the E-SBC

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

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

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

Figure 4-57: Resetting the E-SBC



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

This page is intentionally left blank.

A Mediant MSBR E-SBC INI File Format

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

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

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

;Board: Mediant 500
;HW Board Type: 69  FK Board Type: 77
;Serial Number: 4965606
;Slot Number: 4
;Software Version: 6.80A.311.003
;DSP Software Version: 5014AE3_R => 680.31
;Board IP Address: 10.15.17.10
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.17.11
;Ram size: 369M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 1  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;;Key features:;Board Type: Mediant 500 ;IP Media: Conf VXML ;DSP Voice
features: RTCP-XR ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;Channel Type: DspCh=30 IPMediaDspCh=30 ;HA ;PSTN
FALLBACK Supported ;FXSPorts=3 ;FXOPorts=1 ;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 ;DATA features:
Routing FireWall&VPN WAN BGP Advanced-Routing 3G FTTX-WAN T1E1-Wan-
Trunks=2 ;Control Protocols: MSFT FEU=100 TestCall=100 MGCP SIP
SASurvivability SBC=60 ;Default features:;Coders: G711 G726;

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


[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
;VpFileLastUpdateTime is hidden but has non-default value
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.27.1'
```

```
LdapSearchServerMethod = 0
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

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

[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]

PrerecordedTonesFileName = 'RingbackTone-Guitar-A-law.dat'
ENABLEMEDIASECURITY = 1

[WEB Params]

SharedSecret = '$1$woS2sLC0opqIjoKZng=='
LogoWidth = '145'
;HTTPSPkeyFileName is hidden but has non-default value

[SIP Params]

REGISTRATIONTIME = 1200
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
SIPGATEWAYNAME = '+498944238460@business.mnet-voip.de'
USEGATEWAYNAMEFOROPTIONS = 1
```

```
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCMAXFORWARDSLIMIT = 70
SBCPREFERENCESMODE = 1
GWOUTBOUNDMANIPULATIONSET = 7
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1

[SCTP Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ DeviceTable ]

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

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.10, 16, 10.15.17.11, "Voice",
10.15.27.1, 0.0.0.0, "vlan 1";

[ \InterfaceTable ]


[ DspTemplates ]

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

[ \DspTemplates ]


[ CpMediaRealm ]
```

```
FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 100, 6990, 0, "", "";
CpMediaRealm 1 = "MRWan", "WAN", "", 7000, 100, 7990, 0, "", "";

[ \CpMediaRealm ]


[ SRD ]

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

[ \SRD ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE.S4B.interop:5067", 2, 1;
ProxyIp 1 = "business.mnet-voip.de", 0, 2;

[ \ProxyIp ]


[ IpProfile ]

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

```
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay, IpProfile_SBCRemoteMultipleAnswersMode,
IpProfile_SBCKeepVIAHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW;
IpProfile 1 = "S4B", 1, 0, 0, 10, 10, 46, 24, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 1, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 1, 3, 1, 1, 0, 3, 2, 1, 0, 1,
1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300, 0, -1, -1, -1, -1, 0;
IpProfile 2 = "M-net", 1, 0, 0, 10, 10, 46, 24, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 0, -1, 0, 2,
0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 2, 2, 2, 1, 3, 0, 1, 0,
1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 300, 0, -1, -1, -1, -1, 0;

[ \IpProfile ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, "-1", -1, -1, "";
ProxySet 1 = "S4B", 1, 60, 1, 1, 0, 0, "-1", 1, -1, "";
ProxySet 2 = "M-net", 1, 60, 1, 0, 1, 0, "-1", 1, 1, "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
```

```
IPGroup_MsgManUserDef2, IPGroup_SIPConnect,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 1 = 0, "S4B", 1, "business.mnet-voip.de", "", 0, -1, -1, 0, -1,
0, "MRLan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "Admin",
"$1$aCkNBwIC", 0, "", "", "", 0, "", "", 0, 0;
IPGroup 2 = 0, "M-net", 2, "business.mnet-voip.de", "", 0, -1, -1, 0, -1,
1, "MRWan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "Admin",
"$1$aCkNBwIC", 0, "", "", "", 0, "", "", 0, 0;

[ \IPGroup ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup,
Account_ServingIPGroup, Account_Username, Account_Password,
Account_HostName, Account_Register, Account_ContactUser,
Account_ApplicationType;
Account 0 = -1, 1, 2, "+498944238460", "$1$eCgeCy0yLUYOtta77Q==",
"business.mnet-voip.de", 1, "+498944238460", 2;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "Terminate OPTIONS", -1, "*", "*", "*", "*", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "S4B to ITSP", 1, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 2, "", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to S4B", 2, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 1, "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 7, "RC4:AES128", "ALL:!ADH", 0, , , 2560, 0;

[ \TLSContexts ]


[ SIPInterface ]
```

```
FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet;
SIPInterface 0 = "S4B", "Voice", 2, 0, 0, 5067, 0, "", "", -1, 0, 500, -
1;
SIPInterface 1 = "M-net", "WAN", 2, 5060, 5060, 0, 1, "", "", -1, 0, 500,
-1;

[ \SIPInterface ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "Change + to 00 Dest", 0, 1, 2, "*", "*", "+",
"*", "*", "", 0, -1, 0, 1, 1, 0, 255, "00", "", 0;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0, "";
CodersGroup0 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup0 ]


[ AllowedCodersGroup0 ]

FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name;
AllowedCodersGroup0 0 = "g711Alaw64k";
AllowedCodersGroup0 1 = "g729";

[ \AllowedCodersGroup0 ]
```

```
[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "OPTIONS", 7, "OPTIONS", "",
"header.contact.url.user", 2, "'+498944238460'", 0;
MessageManipulations 1 = "Call Forward", 4, "invite", "header.history-
info.0 regex (<sip:)(.*)(@)(.*)", "header.from.url.user", 2, "$2", 0;
MessageManipulations 2 = "Call Forward", 4, "", "", "header.history-
info", 1, "", 1;
MessageManipulations 3 = "Call Transfer", 4, "invite", "header.referred-
by exists", "header.from.url.user", 2, "header.referred-by.url.user", 0;
MessageManipulations 4 = "Call Transfer", 4, "", "", "header.p-asserted-
identity.url.user", 2, "header.from.url.user", 1;
MessageManipulations 5 = "Call Transfer", 4, "", "", "header.referred-
by.url.host", 2, "param.ipg.dst.host", 1;
MessageManipulations 6 = "Reject Causes", 4, "any.response",
"header.request-uri.methodtype=='503' OR header.request-
uri.methodtype=='488'", "header.request-uri.methodtype", 2, "'480'", 0;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

B Mediant MSBR E-SBC CLI Script File Format

The following example shows the Mediant MSBR E-SBC CLI configuration file, including the data portion:

```
# Running Configuration Mediant 500


## VoIP Configuration

  configure voip
   tls 0
    name default
    tls-version tls-v1.0_1.1_1.2
    ciphers-server "RC4:AES128"
    ciphers-client "ALL:!ADH"
    ocsp-server disable
    ocsp-port 2560
    ocsp-default-response reject
   exit
   appli-enabling
    enable-sbc on
    activate
   exit
   coders-and-profiles ip-profile 1
    profile-name "S4B"
    sbc-media-security-behaviour srtp
    sbc-prack-mode optional
    sbc-session-expires-mode supported
    sbc-rmt-update-supp supported-only-after-connect
    sbc-rmt-re-invite-supp supported-only-with-sdp
    sbc-rmt-delayed-offer not-supported
    sbc-rmt-refer-behavior handle-locally
    sbc-rmt-3xx-behavior handle-locally
    enable-symmetric-mki enable
    mki-size 1
    sbc-enforce-mki-size enforce
    sbc-rmt-early-media-rtp by-media
    early-answer-timeout 0
    reset-srtp-upon-re-key enable
    generate-srtp-keys always
    activate
   exit
   coders-and-profiles ip-profile 2
    profile-name "M-net"
    sbc-allowed-coders-group-id coders-group-0
    sbc-media-security-behaviour rtp
    sbc-assert-identity add
    sbc-session-expires-mode not-supported
    sbc-rmt-refer-behavior handle-locally
    sbc-rmt-early-media-rtp by-media
    sbc-rmt-can-play-ringback no
    early-answer-timeout 0
    reset-srtp-upon-re-key disable
```

```
  generate-srtp-keys only-if-required
  sbc-play-rbt-to-transferee yes
  activate
 exit
 coders-and-profiles coders-group-0 0
  name "g711Alaw64k"
  p-time 20
  rate 0
  activate
 exit
 coders-and-profiles coders-group-0 1
  name "g729"
  p-time 20
  rate 0
  activate
 exit
 interface network-dev 0
  name "vlan 1"
  activate
 exit
 interface network-if 0
  ip-address 10.15.17.10
  gateway 10.15.17.11
  name "Voice"
  primary-dns 10.15.27.1
  underlying-dev "vlan 1"
  activate
 exit
 voip-network realm 0
  name "MRLan"
  ipv4if "Voice"
  port-range-start 6000
  session-leg 100
  port-range-end 6990
  is-default true
  activate
 exit
 voip-network realm 1
  name "MRWan"
  ipv4if "WAN"
  port-range-start 7000
  session-leg 100
  port-range-end 7990
  activate
 exit
 voip-network srd 0
  name "SRDLan"
  media-realm-name "MRLan"
  activate
 exit
 voip-network srd 1
  name "SRDWan"
  media-realm-name "MRWan"
  activate
 exit
 voip-network sip-interface 0
```

```
  interface-name "S4B"
  network-interface "Voice"
  application-type sbc
  udp-port 0
  tcp-port 0
  tls-port 5067
  activate
 exit
 voip-network sip-interface 1
  interface-name "M-net"
  network-interface "WAN"
  application-type sbc
  tls-port 0
  srd 1
  activate
 exit
 voip-network proxy-set 0
  proxy-name ""
  activate
 exit
 voip-network proxy-set 1
  proxy-name "S4B"
  proxy-enable-keep-alive using-options
  proxy-load-balancing-method round-robin
  is-proxy-hot-swap yes
  proxy-redundancy-mode homing
  activate
 exit
 voip-network proxy-set 2
  proxy-name "M-net"
  proxy-enable-keep-alive using-options
  proxy-load-balancing-method round-robin
  srd-id 1
  proxy-redundancy-mode homing
  dns-resolve-method srv
  activate
 exit
 voip-network ip-group 1
  description "S4B"
  proxy-set-id 1
  sip-group-name "business.mnet-voip.de"
  media-realm-name "MRLan"
  ip-profile-id 1
  username "Admin"
  password aCkNBwIC obscured
  activate
 exit
 voip-network ip-group 2
  description "M-net"
  proxy-set-id 2
  sip-group-name "business.mnet-voip.de"
  srd 1
  media-realm-name "MRWan"
  ip-profile-id 2
  outbound-mesg-manipulation-set 4
  username "Admin"
```

```
 password aCkNBwIC obscured
 activate
exit
gw manipulations general-setting
 outbound-map-set 7
 activate
exit
gw digitalgw rp-network-domains 1
 name "dsn"
 activate
exit
gw digitalgw rp-network-domains 2
 name "dod"
 activate
exit
gw digitalgw rp-network-domains 3
 name "drsn"
 activate
exit
gw digitalgw rp-network-domains 5
 name "uc"
 activate
exit
gw digitalgw rp-network-domains 7
 name "cuc"
 activate
exit
gw digitalgw digital-gw-parameters
 answer-detector-cmd 10486144
 energy-detector-cmd 587202560
 activate
exit
ldap
 ldap-search-server-method sequentialy
 activate
exit
media udp-port-configuration
 udp-port-spacing 10
 activate
exit
media security
 media-security-enable on
 activate
exit
sbc routing ip2ip-routing 0
 route-name "Terminate OPTIONS"
 request-type options
 dst-type dst-address
 dst-address "internal"
 activate
exit
sbc routing ip2ip-routing 1
 route-name "S4B to ITSP"
 src-ip-group-id 1
 dst-ip-group-id 2
 activate
```

```
exit
sbc routing ip2ip-routing 2
 route-name "ITSP to S4B"
 src-ip-group-id 2
 dst-ip-group-id 1
 activate
exit
sbc manipulations ip-outbound-manipulation 0
 manipulation-name "Change + to 00 Dest"
 src-ip-group-id 1
 dst-ip-group-id 2
 dst-user-name-prefix "+"
 manipulated-uri destination
 remove-from-left 1
 prefix-to-add "00"
 activate
exit
sbc manipulations message-manipulations 0
 manipulation-name "OPTIONS"
 manipulation-set-id 7
 message-type "OPTIONS"
 action-subject "header.contact.url.user"
 action-type modify
 action-value "'+498944238460'"
 activate
exit
sbc manipulations message-manipulations 1
 manipulation-name "Call Forward"
 manipulation-set-id 4
 message-type "invite"
 condition "header.history-info.0 regex (<sip:)(.*)(@)(.*)"
 action-subject "header.from.url.user"
 action-type modify
 action-value "$2"
 activate
exit
sbc manipulations message-manipulations 2
 manipulation-name "Call Forward"
 manipulation-set-id 4
 action-subject "header.history-info"
 action-type remove
 row-role use-previous-condition
 activate
exit
sbc manipulations message-manipulations 3
 manipulation-name "Call Transfer"
 manipulation-set-id 4
 message-type "invite"
 condition "header.referred-by exists"
 action-subject "header.from.url.user"
 action-type modify
 action-value "header.referred-by.url.user"
 activate
exit
sbc manipulations message-manipulations 4
 manipulation-name "Call Transfer"
```

```
    manipulation-set-id 4
    action-subject "header.p-asserted-identity.url.user"
    action-type modify
    action-value "header.from.url.user"
    row-role use-previous-condition
    activate
   exit
   sbc manipulations message-manipulations 5
    manipulation-name "Call Transfer"
    manipulation-set-id 4
    action-subject "header.referred-by.url.host"
    action-type modify
    action-value "param.ipg.dst.host"
    row-role use-previous-condition
    activate
   exit
   sbc manipulations message-manipulations 6
    manipulation-name "Reject Causes"
    manipulation-set-id 4
    message-type "any.response"
    condition "header.request-uri.methodtype=='503' OR header.request-
uri.methodtype=='488'"
    action-subject "header.request-uri.methodtype"
    action-type modify
    action-value "'480'"
    activate
   exit
   sbc general-setting
    sbc-forking-handling-mode sequential
    sbc-max-fwd-limit 70
    sbc-preferences with-extensions
    sbc-session-refresh-policy sbc-refresh
    activate
   exit
   sbc allowed-coders-group group-0 0
    name "g711Alaw64k"
    activate
   exit
   sbc allowed-coders-group group-0 1
    name "g729"
    activate
   exit
   services least-cost-routing routing-rule-groups 0
    lcr-default-cost highest-cost
    activate
   exit
   sip-definition proxy-and-registration
    set gw-name "+498944238460@business.mnet-voip.de"
    registration-time 1200
    use-gw-name-for-opt enable
    activate
   exit
   sip-definition advanced-settings
    set ldap-primary-key "telephoneNumber"
    activate
   exit
   sip-definition account 0
```

```
    served-ip-group 1
    serving-ip-group 2
    user-name "+498944238460"
    password eCgeCy0yLUYOtta77Q== obscured
    host-name "business.mnet-voip.de"
    register reg
    contact-user "+498944238460"
    application-type sbc
    activate
   exit
   tdm
    pcm-law-select mulaw
    activate
   exit
   voip-network proxy-ip 0
    proxy-address "FE.S4B.interop:5067"
    transport-type tls
    proxy-set-id 1
    activate
   exit
   voip-network proxy-ip 1
    proxy-address "business.mnet-voip.de"
    transport-type udp
    proxy-set-id 2
    activate
   exit
  exit

## System Configuration

  configure system
   logging
    syslog on
    debug-level detailed
    syslog-ip 10.15.17.100
    activate
   exit
   ntp
    set primary-server "10.15.27.1"
    activate
   exit
   radius
    set shared-secret "$1$woS2sLC0opqIjoKZng=="
    activate
   exit
   snmp
    no activate-keep-alive-trap
    activate
   exit
  no packetsmart enable
  hostname "Mediant 500"
  configuration-version 0
  exit
  configure data
   interface GigabitEthernet 0/0
    ip address 195.189.192.160 255.255.255.128
```

```
  mtu auto
  desc "WAN Copper"
  no ipv6 enable
  speed auto
  duplex auto
  no service dhcp
  ip dns server static
  ip name-server 80.179.52.100 80.179.55.100
  napt
  firewall enable
  no shutdown
 exit
 interface Fiber 0/1
  no ip address
  mtu auto
  desc "WAN Fiber"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no shutdown
 exit
 interface GigabitEthernet 1/1
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
 exit
 interface GigabitEthernet 1/2
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
 exit
 interface GigabitEthernet 1/3
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
 exit
 interface GigabitEthernet 1/4
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
 exit
 interface VLAN 1
  ip address 10.15.17.11 255.255.0.0
  mtu auto
  desc "LAN switch VLAN 1"
  no ipv6 enable
  no service dhcp
  ip dns server static
```

```
    no napt
    no firewall enable
    no link-state monitor
    no shutdown
   exit
   ip nat translation udp-timeout 120
   ip nat translation tcp-timeout 3600
   ip nat translation icmp-timeout 6
   # Note: The following WAN ports are in use by system services,
   #       conflicting rules should not be created:
   #         Ports 82 - 82 --> TR069
   #         Ports 7000 - 7990 --> RealmPortPool::MRWan
   #         Ports 5060 - 5060 --> SIPUDP#1
   #         Ports 5060 - 5060 --> SIPLISTENING#1
   # Note: The following NAT rules are in effect for system services,
   #       conflicting rules should not be created:
   #         RealmPortPool::MRWan: LAN ports 7000-7990 to WAN IP
195.189.192.160 ports 7000-7990, interface GigabitEthernet 0/0
   #         SIPUDP#1: LAN ports 5060-5060 to WAN IP 195.189.192.160
ports 5060-5060, interface GigabitEthernet 0/0
   #         SIPLISTENING#1: LAN ports 5060-5060 to WAN IP
195.189.192.160 ports 5060-5060, interface GigabitEthernet 0/0
   ip route 0.0.0.0 0.0.0.0 195.189.192.129 GigabitEthernet 0/0 1
   ip domain name home
   ip domain localhost msbr
   pm sample-interval minute 5
   pm sample-interval seconds 15
  exit
```

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-13080