Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Mediant E-SBC & Level 3 SIP Trunk

Microsoft Partner
Gold Communications

Level (3) SM
COMMUNICATIONS

Lync

CISCO

AudioCodes

September 2014

Document # LTRT-12340

Table of Contents

Notice

This document describes how to connect the UC System (Microsoft Lync Server 2013) or IP-PBX (Cisco UC Manager 10) and Level 3 SIP Trunk using AudioCodes Mediant E-SBC product series.

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

Date Published:September-10-2014

Trademarks

WEEE EU Directive

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

Customer Support

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

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 Level 3's SIP Trunk and UC System (Microsoft Lync Server 2013) or IP-PBX (Cisco UC Manager 10).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Level 3 Partners who are responsible for installing and configuring Level 3's SIP Trunk and UC Platform/IP-PBX 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 E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_6.80A.231.003
Protocol	▪ SIP/UDP or TCP (to the Level 3 SIP Trunk) ▪ SIP/TCP or TLS (to the Microsoft Lync Server 2013) ▪ SIP/UDP or TCP (to the Cisco UC Manager 10)
Additional Notes	None

2.2 Level 3 SIP Trunking Version

Table 2-2: Level 3 Version

Vendor/Service Provider	Level 3
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Microsoft Lync Server 2013 Version

Table 2-3: Microsoft Lync Server 2013 Version

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

2.4 Cisco UC Manager Version

Table 2-4: Cisco UC Manager Version

Vendor	Cisco
Model	Unified Communications Manager
Software Version	10
Protocol	SIP
Additional Notes	None

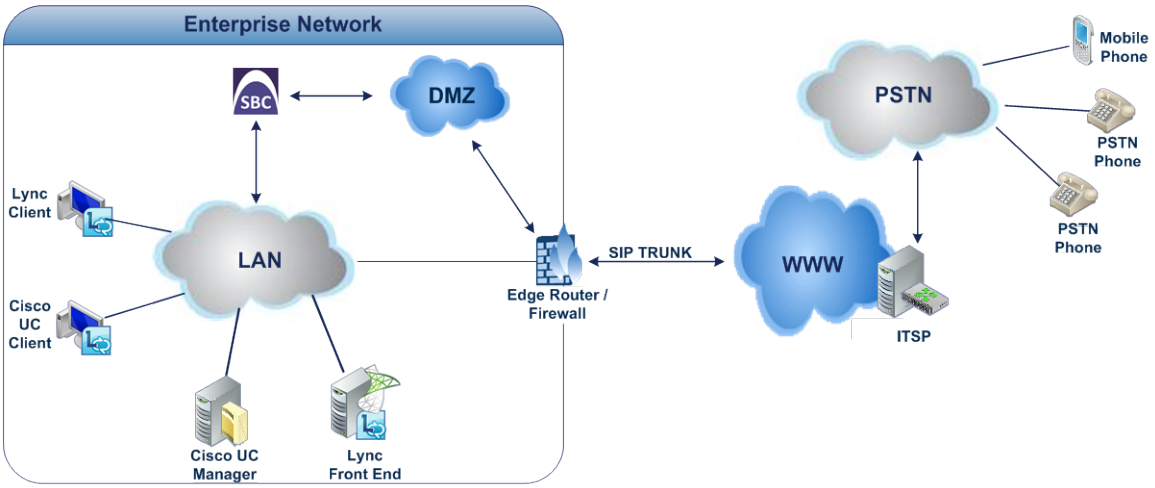
2.5 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Level 3 SIP Trunk with UC System/IP-PBX was done using the following topology setup:

- Enterprise deployed with UC System (Microsoft Lync Server 2013) or IP-PBX (Cisco UC Manager 10) 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 Level 3'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 Enterprise Network in the LAN and Level 3'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 UC System or IP-PBX with Level 3 SIP Trunk



2.5.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-5: Environment Setup

Area	Setup
Network	▪ UC System/IP-PBX environment is located on the Enterprise's LAN ▪ Level 3 SIP Trunk is located on the WAN
Signaling Transcoding	▪ UC System/IP-PBX operates with SIP-over-UDP or SIP-over-TCP or SIP-over-TLS transport type ▪ Level 3 SIP Trunk operates with SIP-over-UDP or SIP-over-TCP transport type
Codecs Transcoding	▪ UC System/IP-PBX supports G.711A-law and G.711U-law coders ▪ Level 3 SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ UC System (Microsoft Lync Server 2013) operates with SRTP or IP-PBX (Cisco UC Manager 10) operates with RTP media type ▪ Level 3 SIP Trunk operates with RTP media type

2.5.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between UC System/IP-PBX and Level 3's SIP Trunk.

3 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between UC System/IP-PBX and the Level 3 SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.5 on page 11, and includes the following main areas:

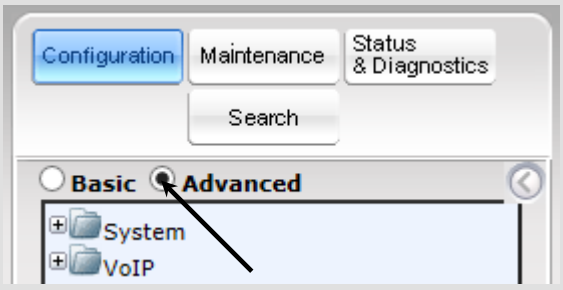
- E-SBC WAN interface - Level 3 SIP Trunking environment
- E-SBC LAN interface – UC System/IP-PBX environment

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

Notes:

- For implementing IP-PBX and Level 3 SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **Microsoft**
  - √ **SBC**
  - √ **Security**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

  For more information about the Software License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the UC System/IP-PBX 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 Full-menu display mode. To do this, select the **Full** option, as shown below:



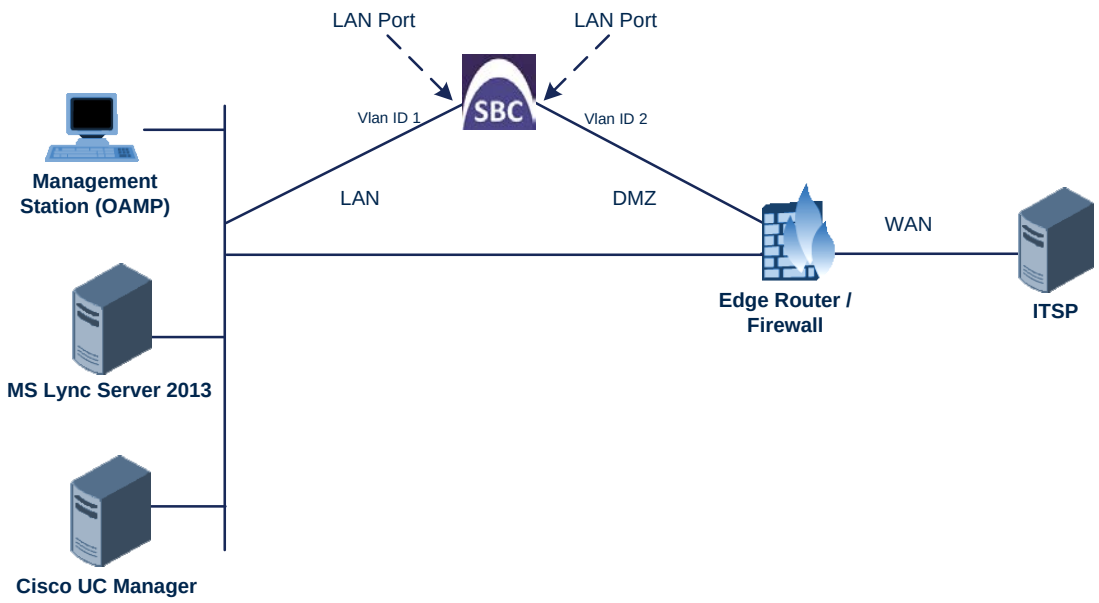
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

3.1 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:
  - UC System/IP-PBX, located on the LAN
  - Level 3 SIP Trunk, located on the WAN
- E-SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and WAN using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

Figure 3-1: Network Interfaces in Interoperability Test Topology



3.1.1 Step 1a: Configure VLANs

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

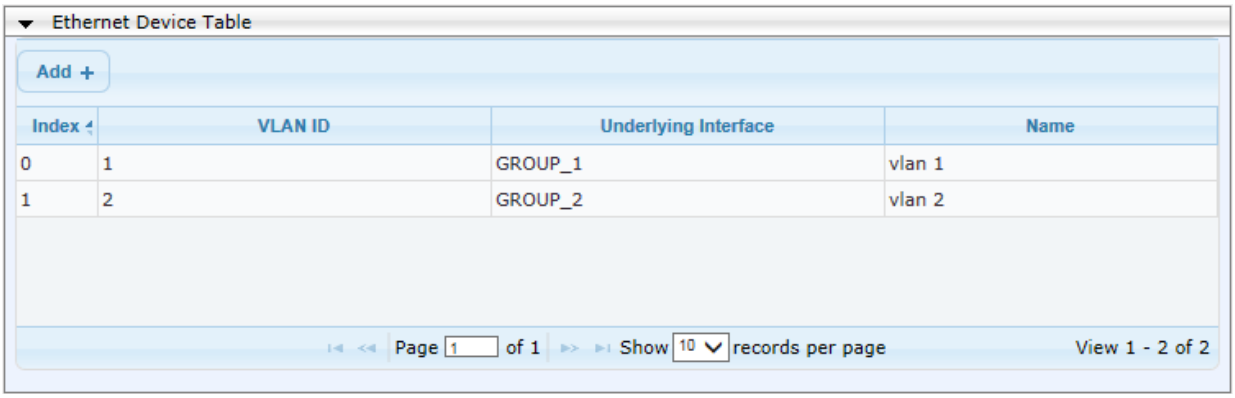
- LAN VoIP (assigned the name "Voice")
- WAN VoIP (assigned the name "WANSP")

➢ **To configure the VLANs:**

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

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

Figure 3-2: Configured VLAN IDs in Ethernet Device Table



3.1.2 Step 1b: Configure Network Interfaces

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

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

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

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

Parameter	Value
IP Address	**10.15.17.77** (IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Gateway	**10.15.0.1**
VLAN ID	**1**
Interface Name	**Voice** (arbitrary descriptive name)
Primary DNS Server IP Address	**10.15.25.1**
Underlying Device	**vlan 1**

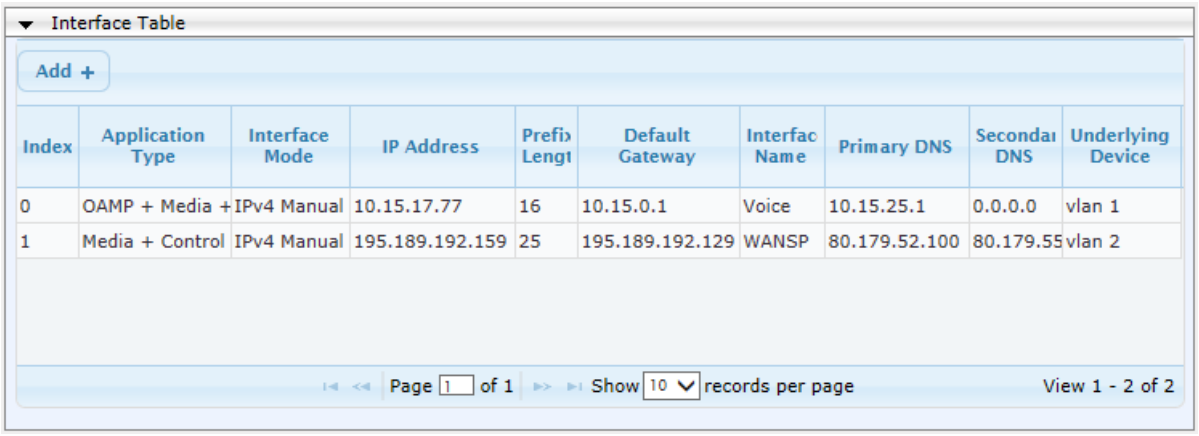
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.189.192.159** (WAN IP address)
Prefix Length	**25** (for 255.255.255.128)
Gateway	**195.189.192.129** (router's IP address)
VLAN ID	**2**
Interface Name	**WANSP**
Primary DNS Server IP Address	**80.179.52.100**
Secondary DNS Server IP Address	**80.179.55.100**
Underlying Device	**vlan 2**

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

The configured IP network interfaces are shown below:

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



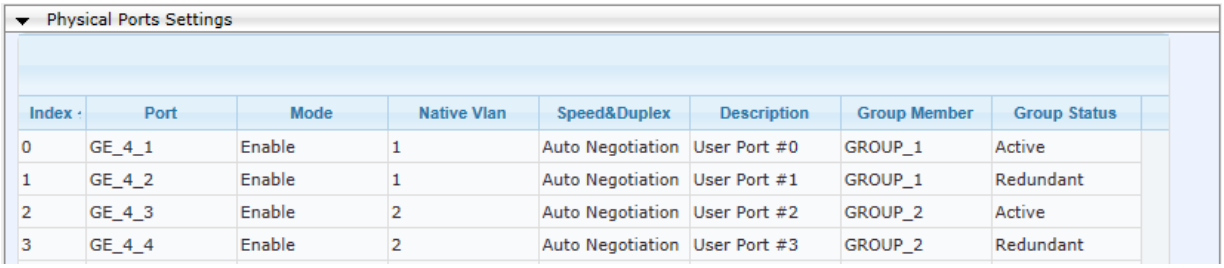
3.1.3 Step 1c: Configure the Native VLAN ID

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

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

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

Figure 3-4: Configured Port Native VLAN



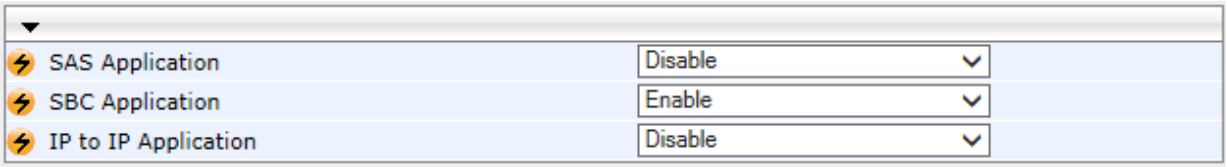
3.2 Step 2: Enable the SBC Application

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 3-5: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 3.14 on page 67).

3.3 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.

3.3.1 Step 3a: Configure Media Realms

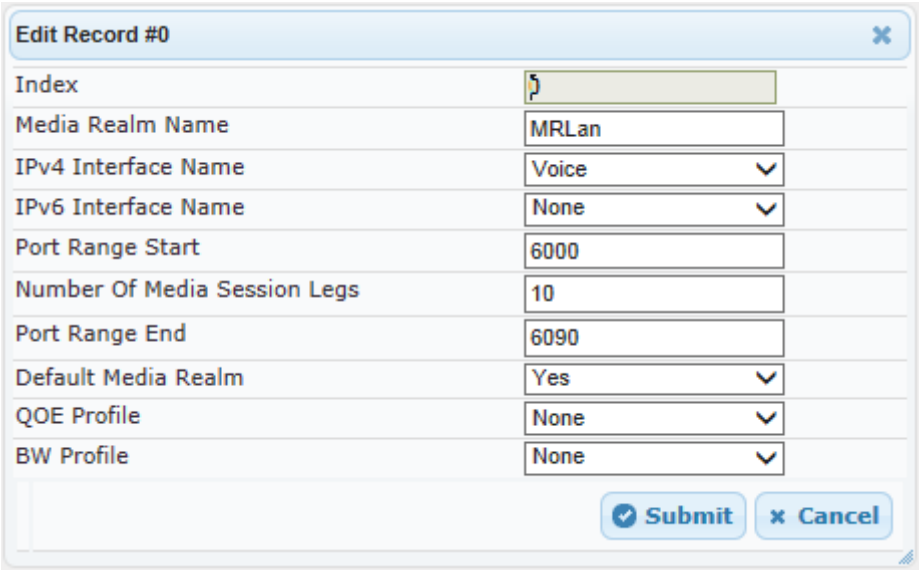
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **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	**10** (media sessions assigned with port range)

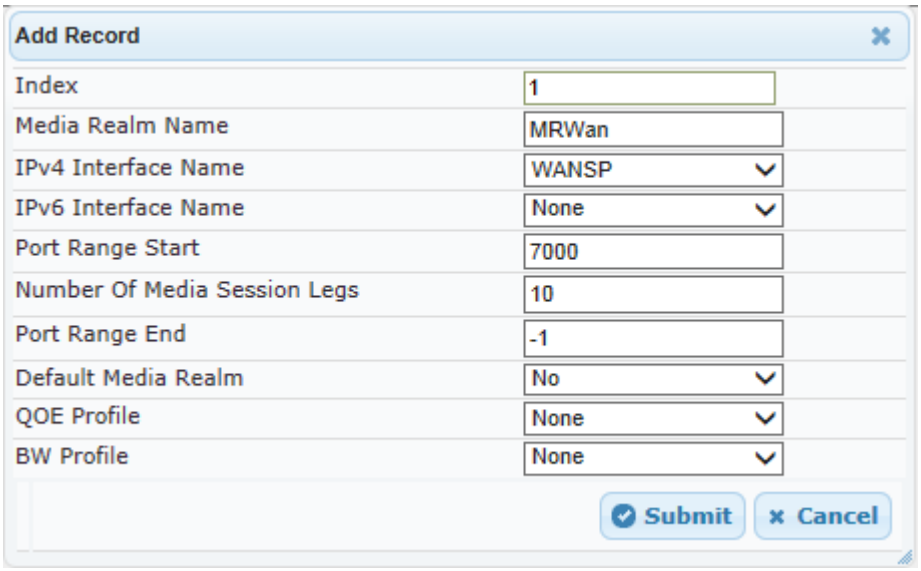
Figure 3-6: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

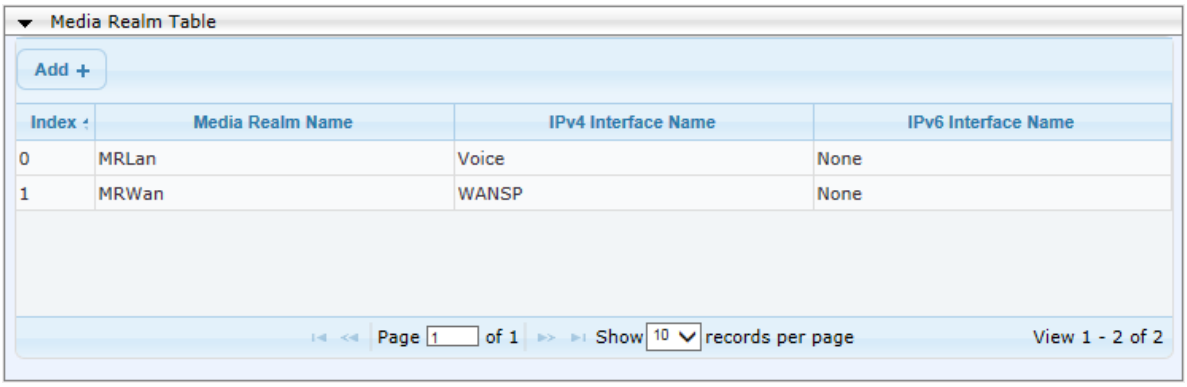
Parameter	Value
Index	**1**
Media Realm Name	**MRWan** (arbitrary name)
IPv4 Interface Name	**WANSP**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

Figure 3-7: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 3-8: Configured Media Realms in Media Realm Table



3.3.2 Step 3b: Configure SRDs

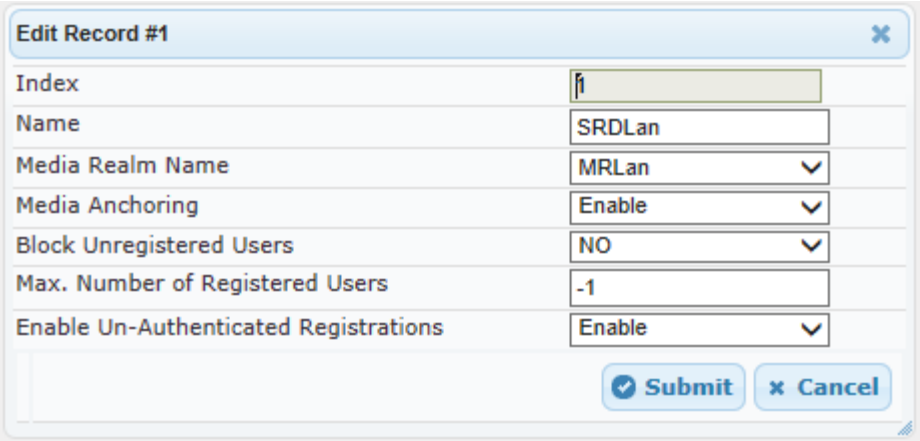
This step describes how to configure the SRDs.

➢ **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 IP-PBX):

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

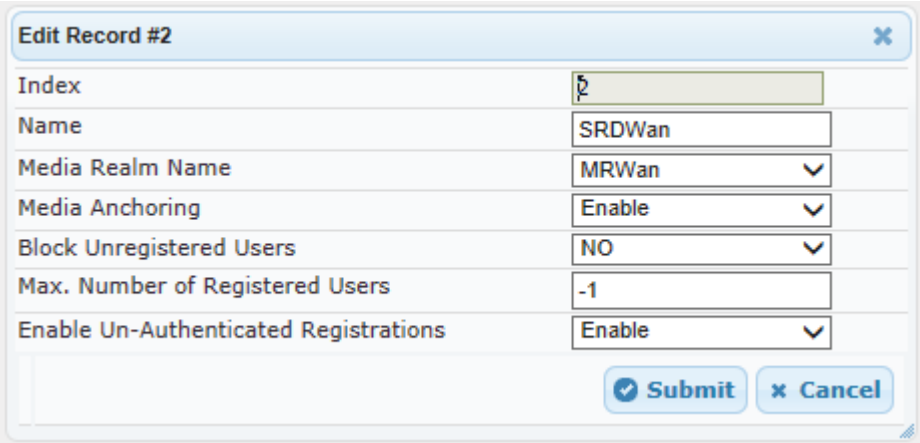
Figure 3-9: Configuring LAN SRD



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

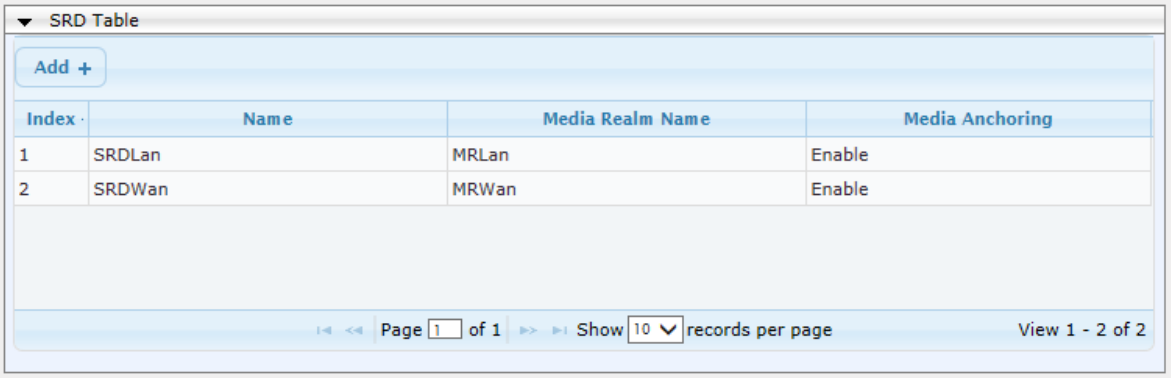
Parameter	Value
SRD Index	**2**
SRD Name	**SRDWan**
Media Realm	**MRWan**

Figure 3-10: Configuring WAN SRD



The configured SRDs are shown in the figure below:

Figure 3-11: Configured SRDs in SRD Table



3.3.3 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 (Microsoft Lync Server 2013 example):

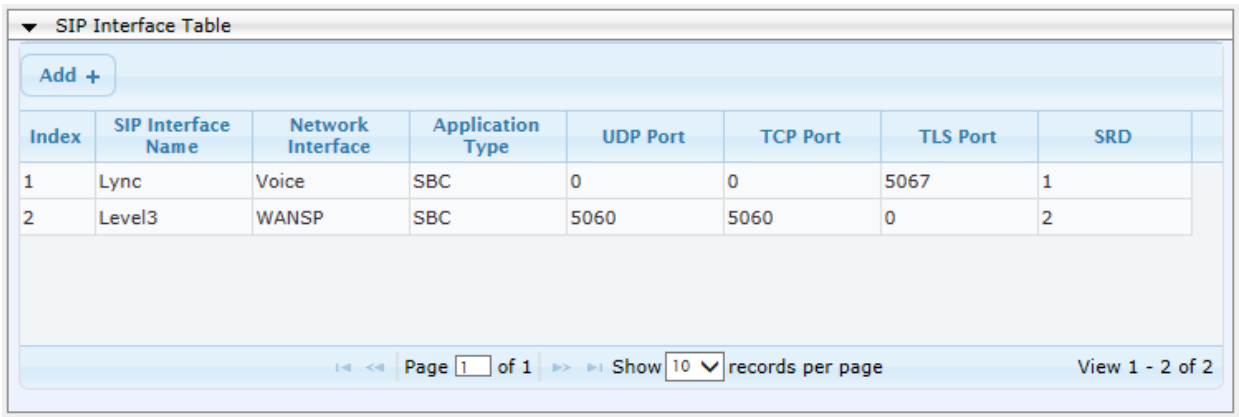
Parameter	Value
Index	**1**
Interface Name	**Lync** (arbitrary descriptive name)
Network Interface	**Voice**
Application Type	**SBC**
TLS Port	**5067**
TCP and UDP	**0**
SRD	**1**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
Interface Name	**Level 3** (arbitrary descriptive name)
Network Interface	**WANSP**
Application Type	**SBC**
UDP and TCP Port	**5060**
TLS	**0**
SRD	**2**

The configured SIP Interfaces are shown in the figure below:

Figure 3-12: Configured SIP Interfaces in SIP Interface Table



3.4 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:

- Level 3 SIP Trunk
- UC System (Microsoft Lync Server 2013)/IP-PBX (Cisco UC Manager 10)

These Proxy Sets will later be associated with IP Groups.

3.4.1 Proxy Set for Level 3 SIP Trunk

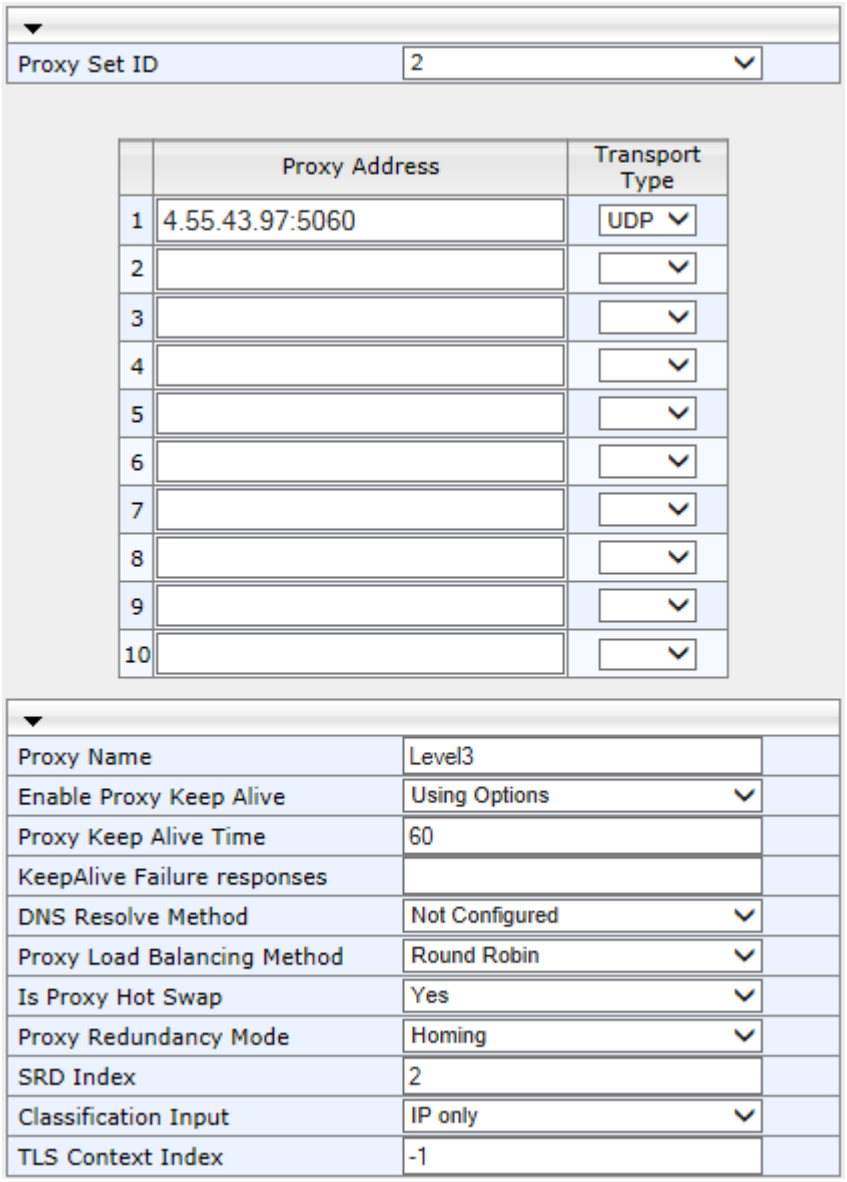
This step describes how to configure the Level 3 SIP Trunk.

➢ **To configure the Level 3 SIP trunk:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for the Level 3 SIP Trunk:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**4.55.43.97:5060** (Level 3 IP address / FQDN and destination port)
Transport Type	**UDP** (for UDP SIP Trunk) or **TCP** (for TCP SIP Trunk)
Proxy Name	**Level 3** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
Is Proxy Hot Swap	**Yes**
SRD Index	**2** (enables classification by Proxy Set for SRD of IP Group belonging to Level 3 SIP Trunk)

Figure 3-13: Configuring Proxy Set for Level 3 SIP Trunk



3.4.2 Proxy Set for Microsoft Lync Server 2013

This step describes how to configure the Proxy Set for Microsoft Lync Server 2013.

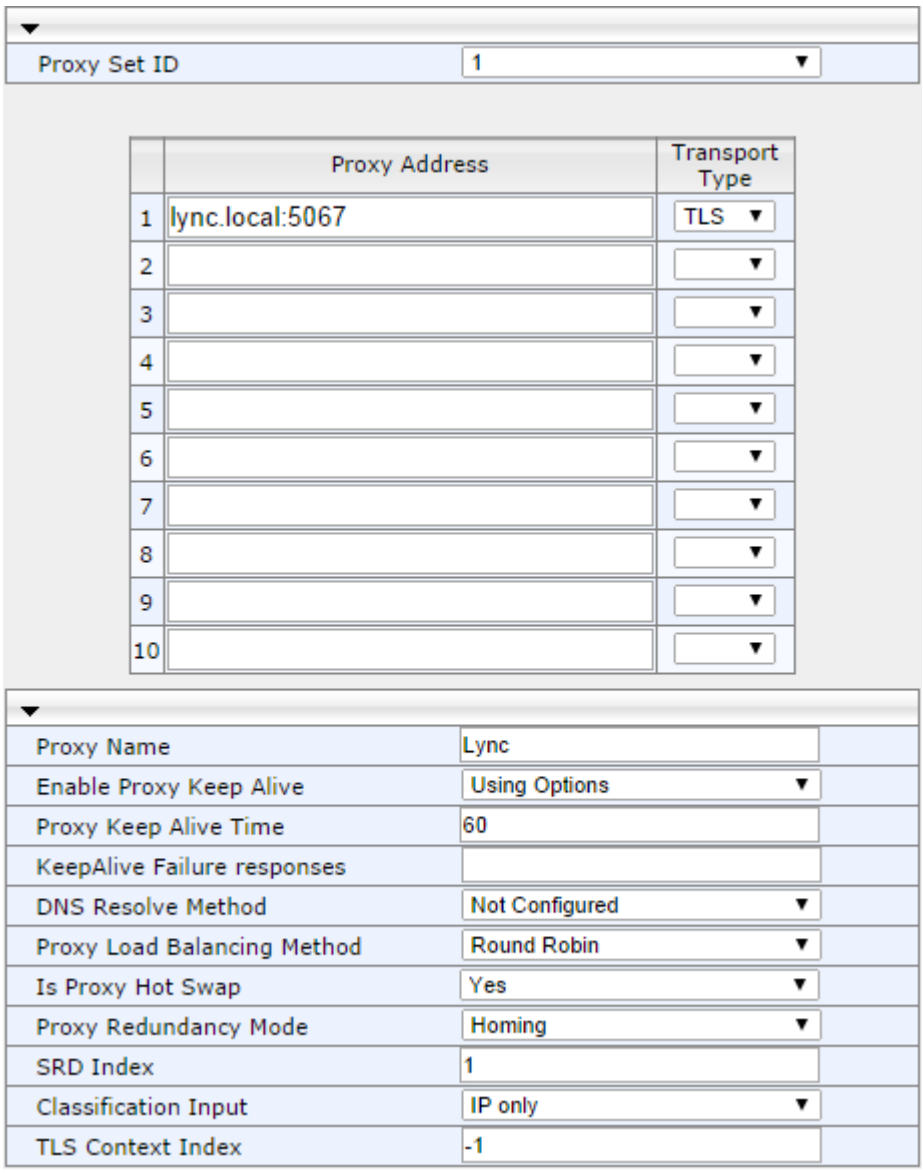
➢ **To configure the proxy set for the Microsoft Lync Server 2013:**

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

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**lync.local:5067** (Lync Server 2013 IP address / FQDN and destination port)
Transport Type	**TLS**

Proxy Name	**Lync** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
SRD Index	**1**

Figure 3-14: Configuring Proxy Set for Lync Server 2013



3.4.3 Proxy Set for Cisco UC Manager 10

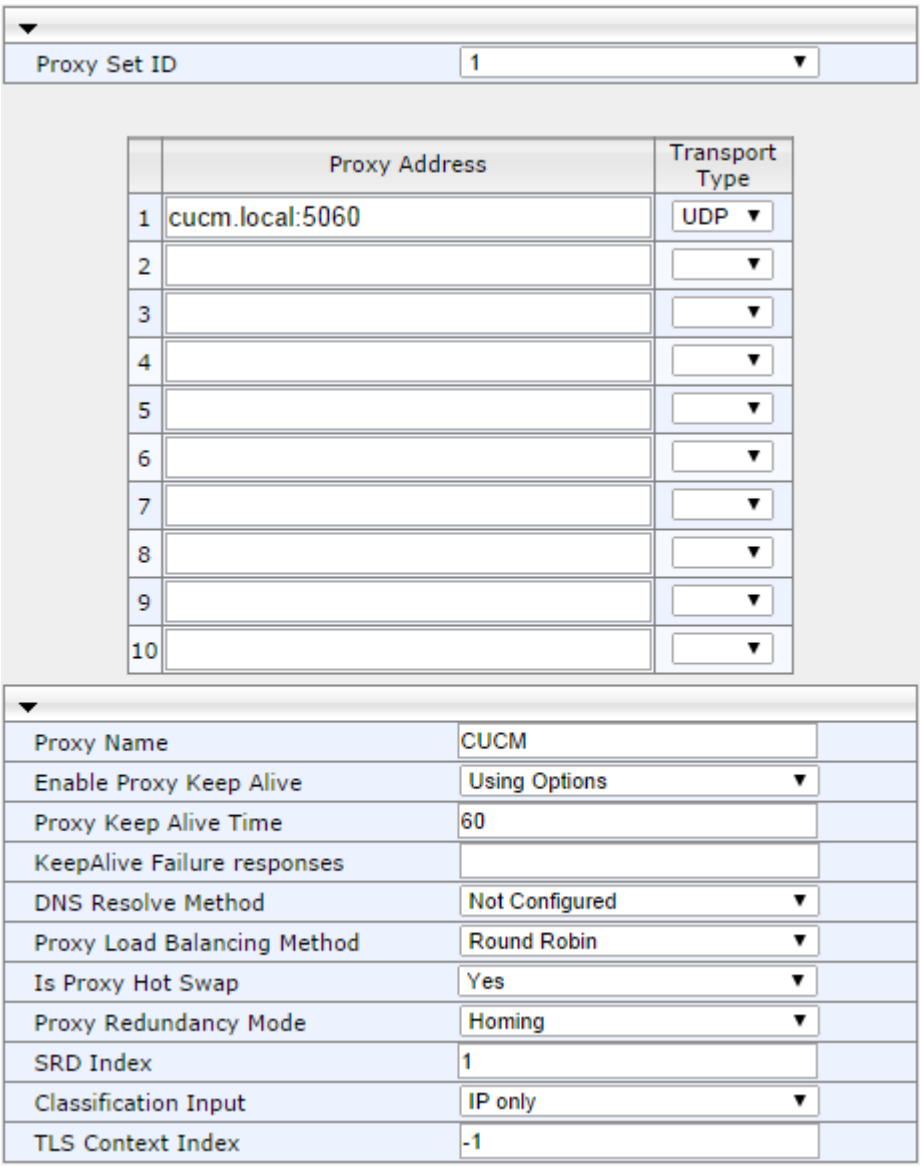
This step describes how to configure the Proxy Set for the Cisco UC Manager.

➢ **To configure the Proxy Set for Cisco UC Manager 10:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for Cisco UC Manager 10:

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**cucm.local:5060** (Cisco UC Manager 10 IP address / FQDN and destination port)
Transport Type	**UDP**
Proxy Name	**CUCM** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
Proxy Load Balancing Method	**Round Robin**
Is Proxy Hot Swap	**Yes**
SRD Index	**1**

Figure 3-15: Configuring Proxy Set for Cisco UC Manager 10



3. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 3.14 on page 67).

3.5 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 the source and destination of the call.

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

- UC System/IP-PBX located on LAN
- Level 3 SIP Trunk located on WAN

3.5.1 IP Group for Level 3 SIP Trunk

This step describes how to configure the Level 3 SIP Trunk.

➢ **To configure the Level 3 SIP trunk:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Configure an IP Group for the Level 3 SIP Trunk:

Parameter	Value
Index	**2**
Type	**Server**
Description	**Level 3** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**195.189.192.159** (according to ITSP requirement)
SRD	**2**
Media Realm Name	**MRWan**
IP Profile ID	**2**

3.5.2 IP Group for Microsoft Lync Server 2013

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

Parameter	Value
Index	**1**
Type	**Server**
Description	**Lync** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**195.189.192.159** (according to ITSP requirement)
SRD	**1**

Media Realm Name	**MRLan**
IP Profile ID	**1**

3.5.3 IP Group for Cisco UC Manager 10

This step describes how to configure the IP Group for Cisco UC Manager 10.

➢ **To configure the IP Group for Cisco UC Manager 10:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Configure an IP Group for the Cisco UC Manager 10:

Parameter	Value
Index	**1**
Type	**Server**
Description	**CUCM** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**195.189.192.159** (according to ITSP requirement)
SRD	**1**
Media Realm Name	**MRLan**
IP Profile ID	**1**

3.6 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:

- Level 3 SIP trunk – to operate in non-secure mode using RTP and UDP
- Microsoft Lync Server 2013 – to operate in secure mode using SRTP and TLS
- Cisco UC Manager 10 – to operate in non-secure mode using RTP and UDP

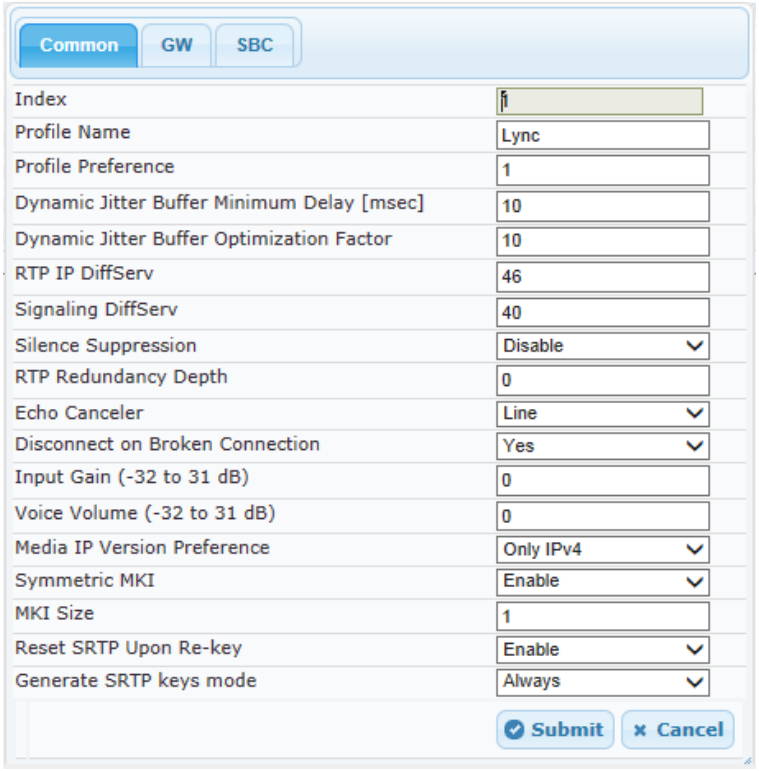
Note that the IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 3.5 on page 29).

3.6.1 Microsoft Lync Server 2013

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

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

Figure 3-16: Configuring IP Profile for Lync Server 2013 – Common Tab

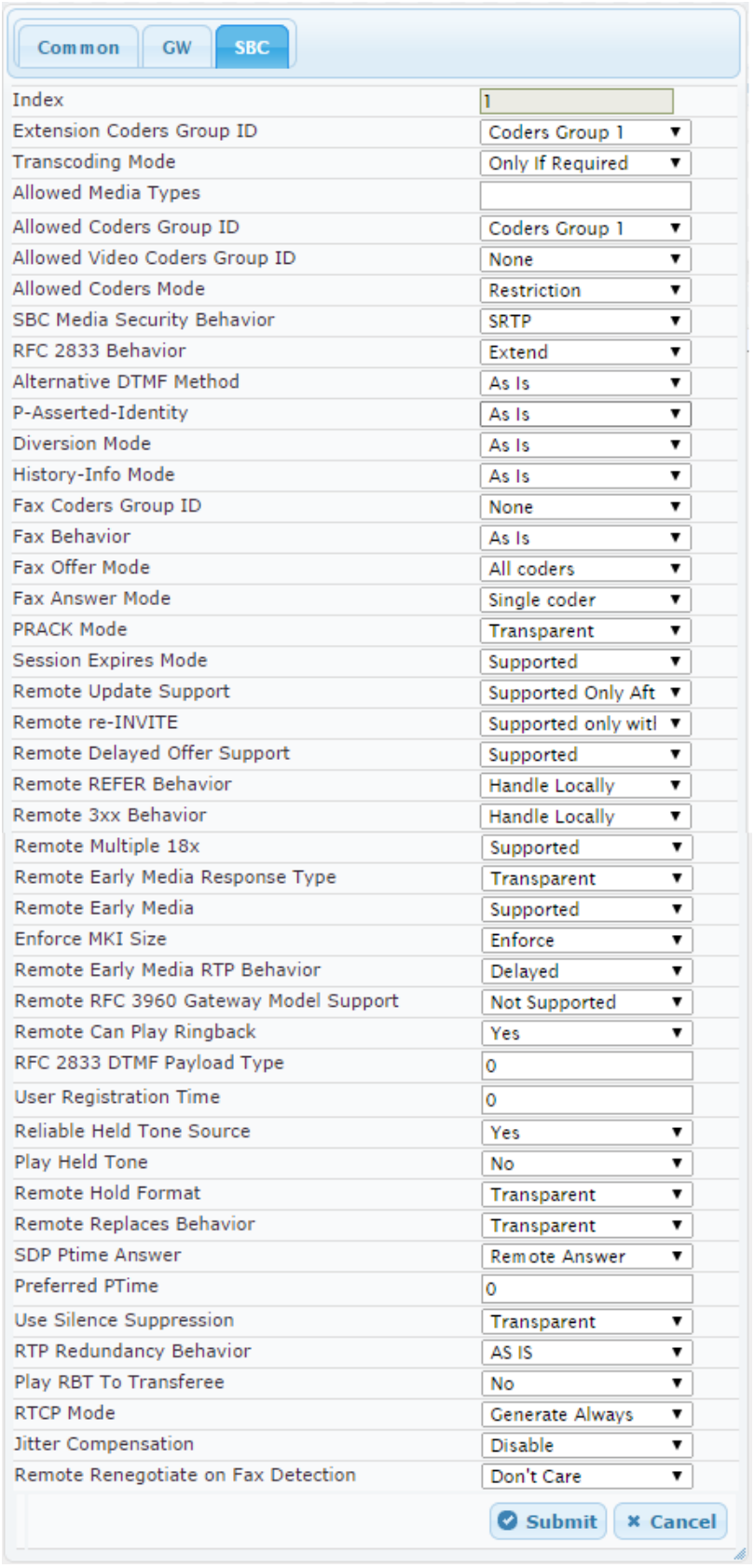


4. Click the **SBC** tab, and then configure the parameters as follows:

Parameter	Value
Extension Coders Group ID	**Coders Group 1**
Allowed Coders Group ID	**Coders Group 1**
Allowed Coders Mode	**Restriction** (only Allowed Coders will be introduced in SDP offer)
Media Security Behavior	**SRTP**
RFC 2833 Behavior	**Extend**
Session Expires Mode	**Supported** (required because Level 3's SIP Trunk does not support Session Timer, so SBC should negotiate it with Lync)
Remote Update Support	**Supported Only After Connect**
Remote Re-Invite Support	**Supported Only With SDP**
Remote Refer Behavior	**Handle Locally** (required, as Lync Server 2013 does not support receipt of SIP REFER)
Remote 3xx Behavior	**Handle Locally** (required, as Lync Server 2013 does not support receipt of SIP 3xx responses)
Enforce MKI Size	**Enforce**
Remote Early Media RTP Behavior	**Delayed** (required, as Lync Server 2013 does not send RTP immediately to remote side when it sends a SIP 18x response)

Parameter	Value
RTCP Mode	**Generate Always** (required, as Level 3 SIP Trunk does not send RTCP packets in active call and in hold call, and in these cases, Microsoft Lync 2013 will terminate the call with network problems as the cause)

Figure 3-17: Configuring IP Profile for Lync Server 2013 – SBC Tab

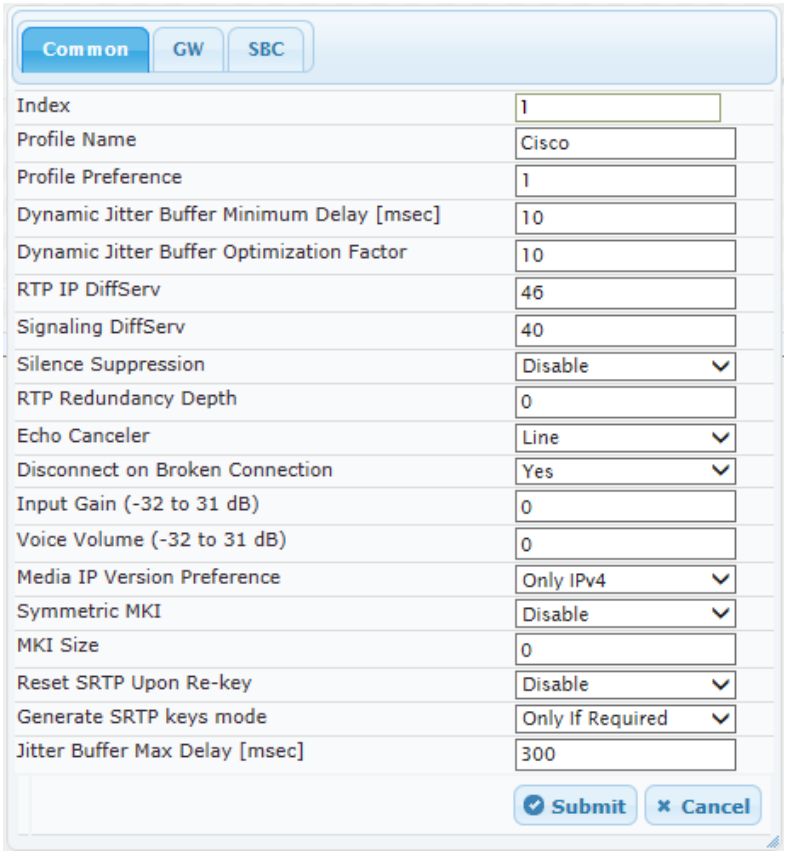


3.6.2 Cisco UC Manager 10

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	**Cisco** (arbitrary descriptive name)

Figure 3-18: Configuring IP Profile for Cisco UC Manager 10 – Common Tab



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

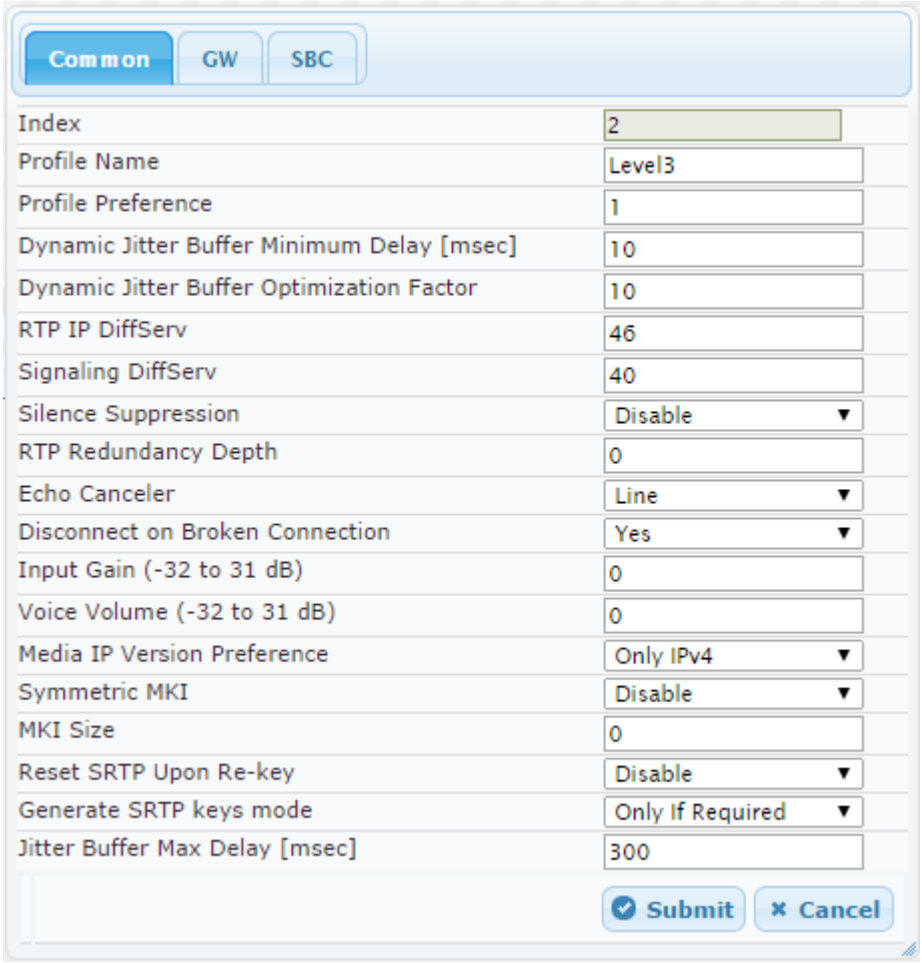
Parameter	Value
Media Security Behavior	**RTP**
Session Expires Mode	**Supported** (required because Level 3's SIP Trunk does not support Session Timer, so SBC should negotiate it with CUCM)
RTCP Mode	**Generate Always** (required, as Level 3 SIP Trunk does not send RTCP packets in active call and in hold call, and in these cases, CUCM will terminate the call with network problems as the cause)

3.6.3 Level 3 SIP Trunk

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	**2**
Profile Name	**Level 3** (arbitrary descriptive name)

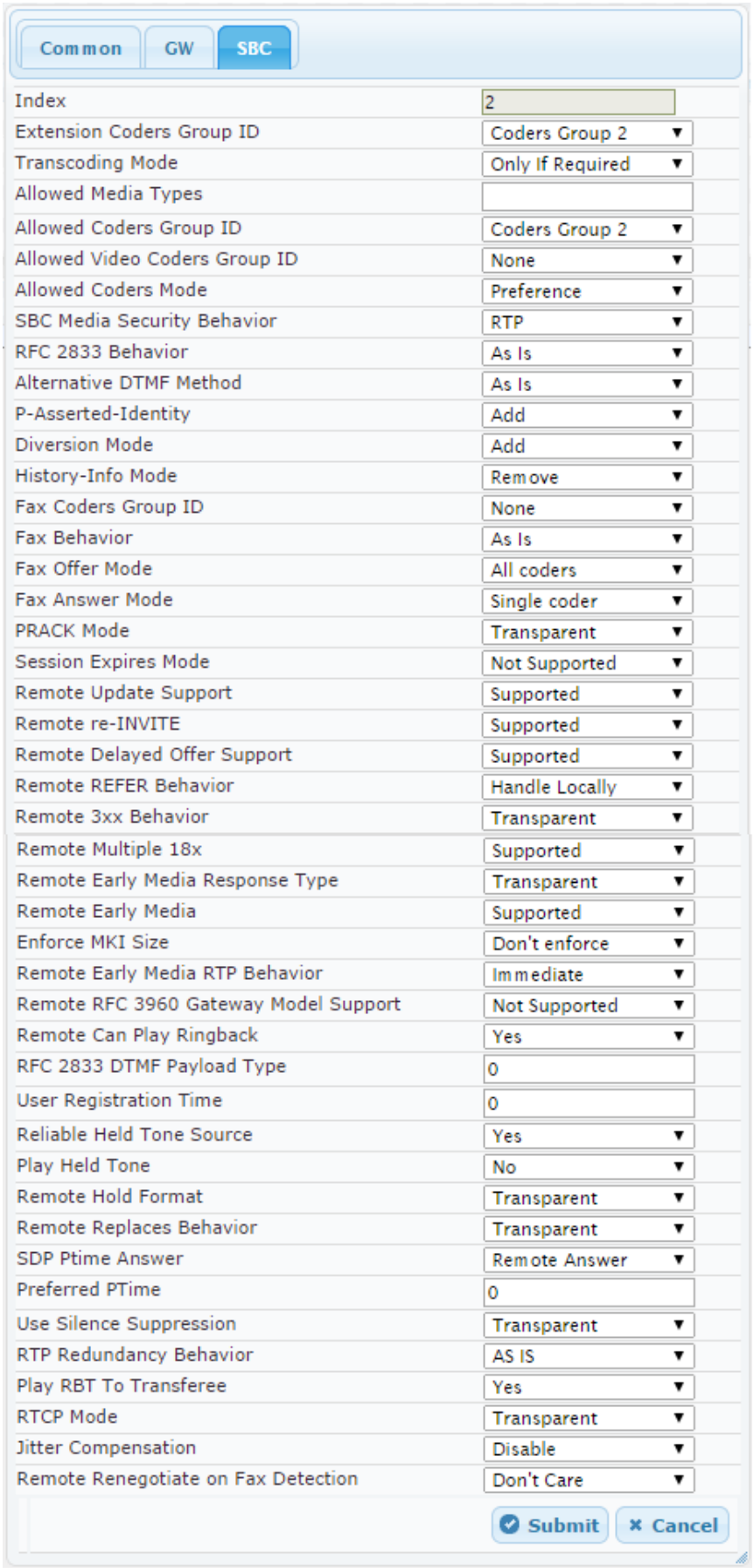
Figure 3-19: Configuring IP Profile for Level 3 SIP Trunk – Common Tab



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

Parameter	Value
Profile ID	**2**
Extension Coders Group ID	**Coders Group 2**
Allowed Coders Group ID	**Coders Group 2**
Allowed Coders Mode	**Preference** (lists Allowed Coders first and then original coders in received SDP offer)
Media Security Behavior	**RTP**
P-Asserted-Identity	**Add** (required for anonymous calls)
Diversion Mode	**Add** (required for forwarded calls)
History-Info Mode	**Remove**
Remote REFER Behavior	**Handle Locally** (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)
Play RBT To Transferee	**Yes** (required for playing ring back tone for transfered calls)

Figure 3-20: Configuring IP Profile for Level 3 SIP Trunk – SBC Tab



3.7 Step 7: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As UC System/IP-PBX can support the G.711 coder while the network connection to Level 3 SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the Level 3 SIP Trunk.

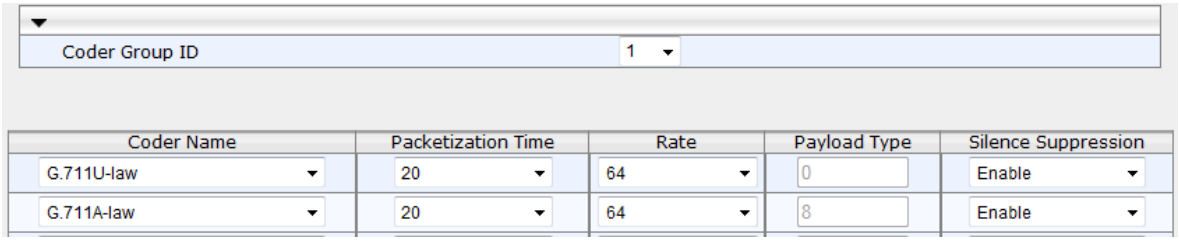
Note that the Coder Group ID for this entity was assigned to its corresponding IP Profile in the previous step (see Section 3.6 on page 31).

➢ **To configure coders:**

1. Open the Coder Group Settings (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**).
2. Configure a Coder Group for UC System/IP-PBX:

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

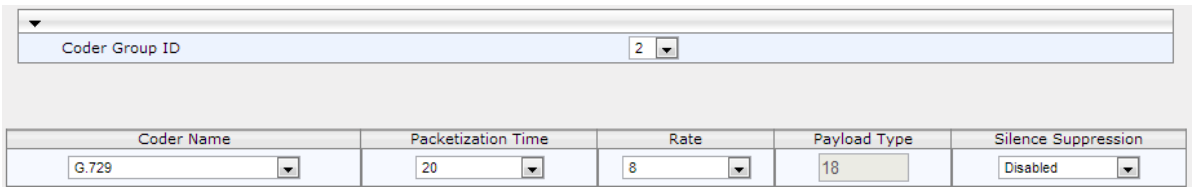
Figure 3-21: Configuring Coder Group for IP-PBX



3. Configure a Coder Group for Level 3 SIP Trunk:

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

Figure 3-22: Configuring Coder Group for Level 3 SIP Trunk



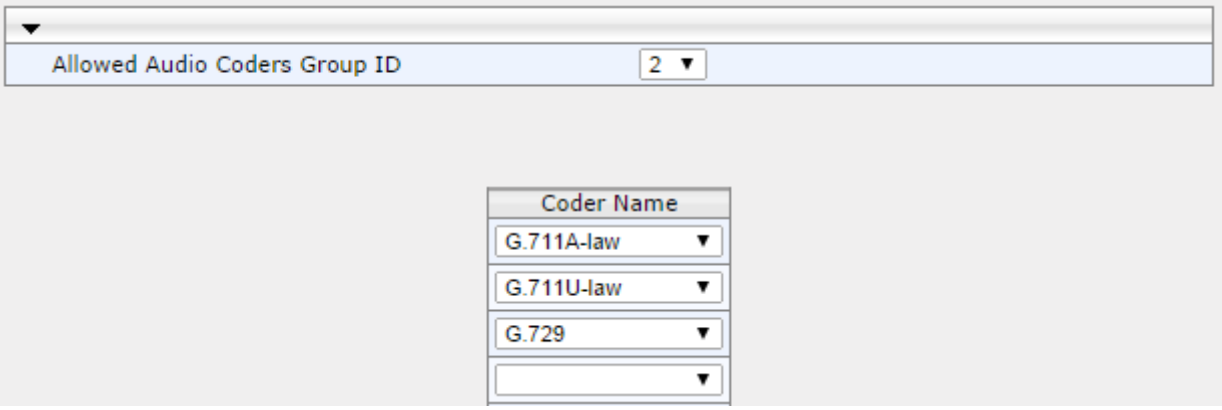
The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Level 3 SIP Trunk uses the coders G.711A-law, G.711U-law or G.729 only. Note that this Allowed Coders Group ID was assigned to the IP Profile belonging to the Level 3 SIP Trunk in the previous step (see Section 3.6 on page 31).

➢ **To set a preferred coder for the Level 3 SIP Trunk:**

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

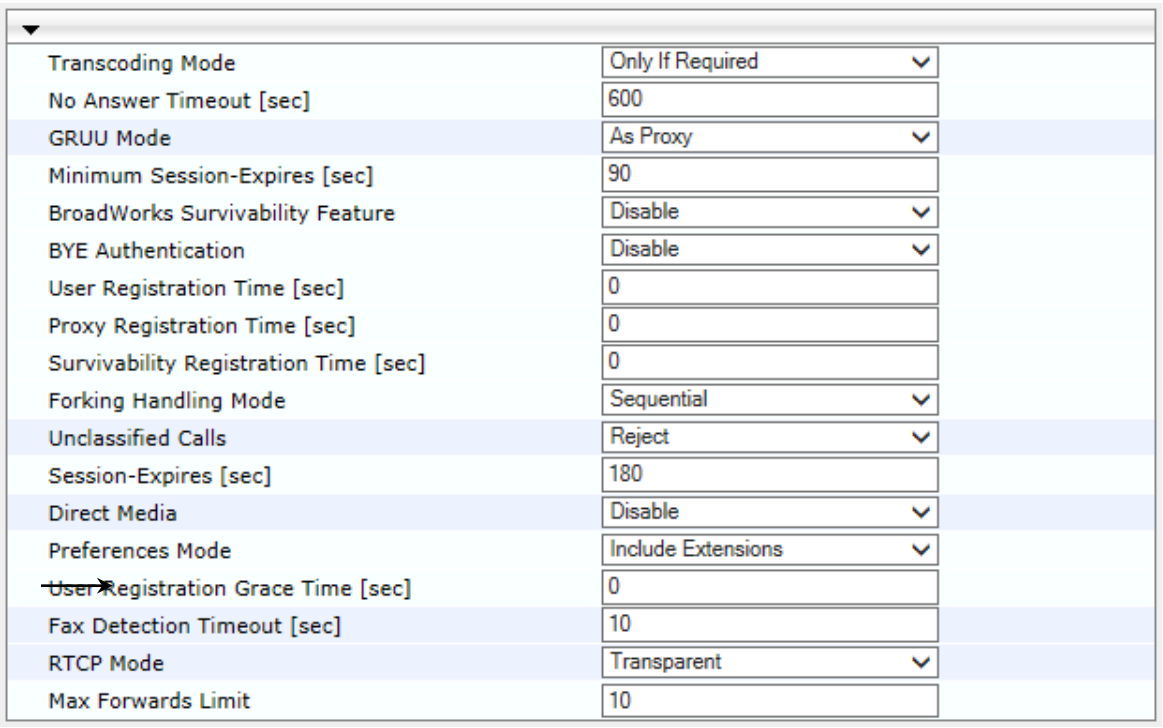
Parameter	Value
Allowed Coders Group ID	**2**
Coder Name	**G.711A-law**
Coder Name	**G.711U-law**
Coder Name	**G.729**

Figure 3-23: Configuring Allowed Coders Group for Level 3 SIP Trunk



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

Figure 3-24: SBC Preferences Mode



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

3.8 Step 8: SIP TLS Connection Configuration

Note: This step is required **only** for UC System (Microsoft Lync Server 2013), which uses a secure SIP TLS connection.

This section describes how to configure the E-SBC for using a TLS connection with the Lync Server 2013 Mediation Server.

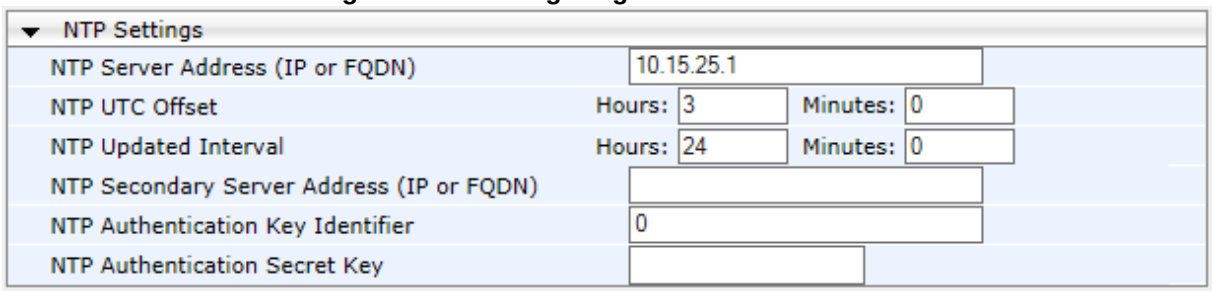
3.8.1 Step 8a: Configure the NTP Server Address

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

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

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

Figure 3-25: Configuring NTP Server Address



3. Click **Submit**.

3.8.2 Step 8b: Configure a Certificate

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

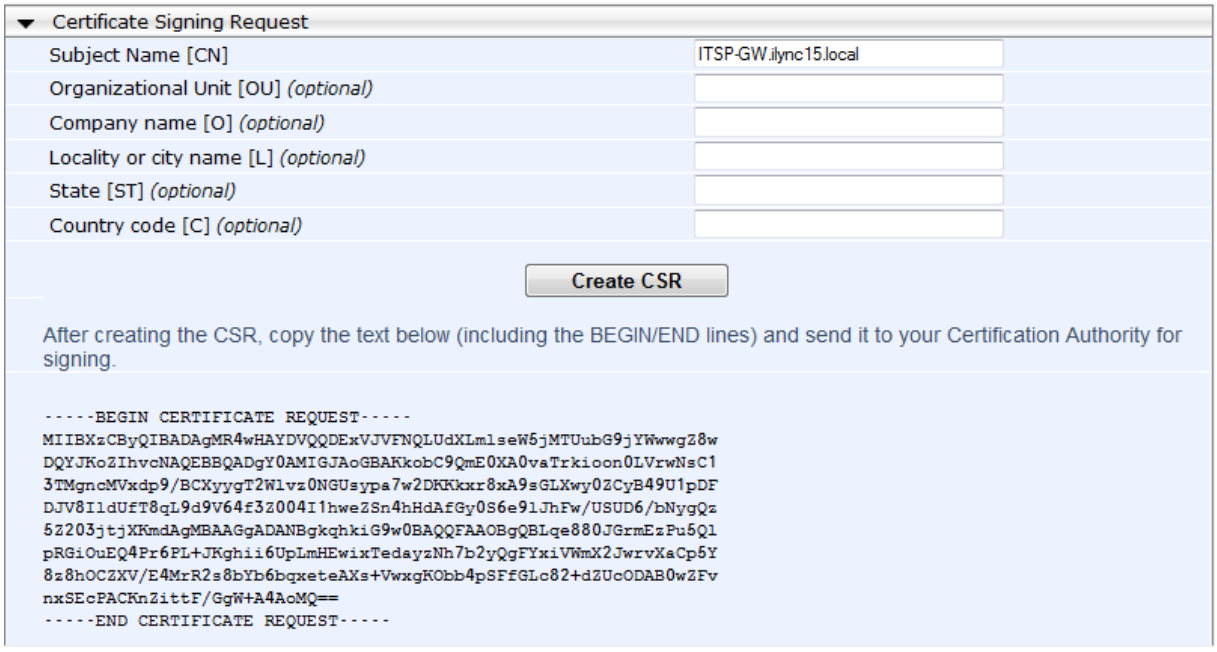
The procedure involves the following main steps:

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

➢ **To configure a certificate:**

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

Figure 3-26: Certificate Signing Request – Creating CSR

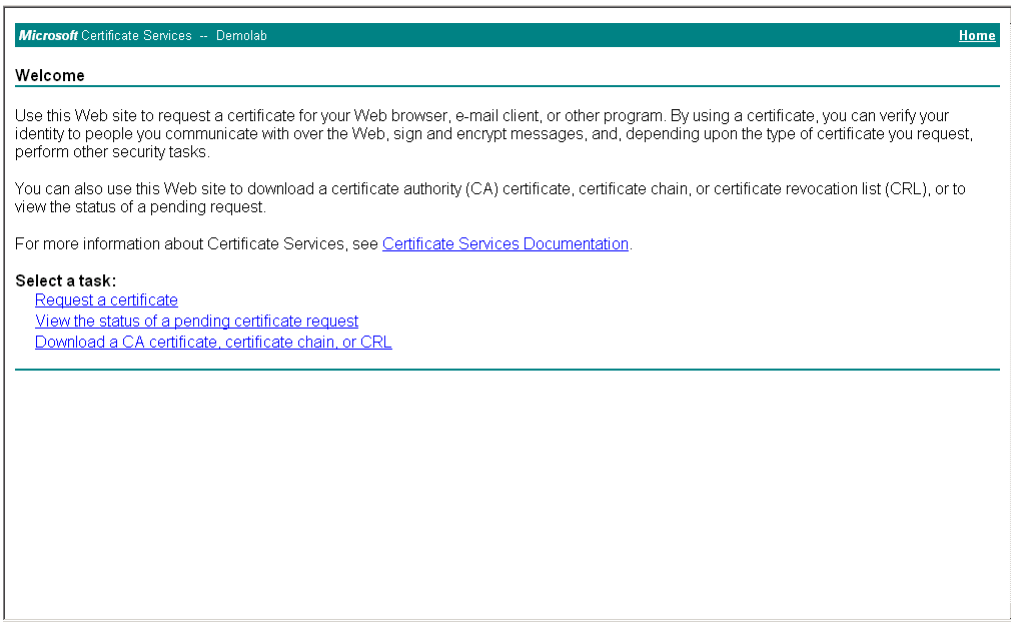


Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013.

5. Copy the CSR from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----**" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, *certreq.txt*.

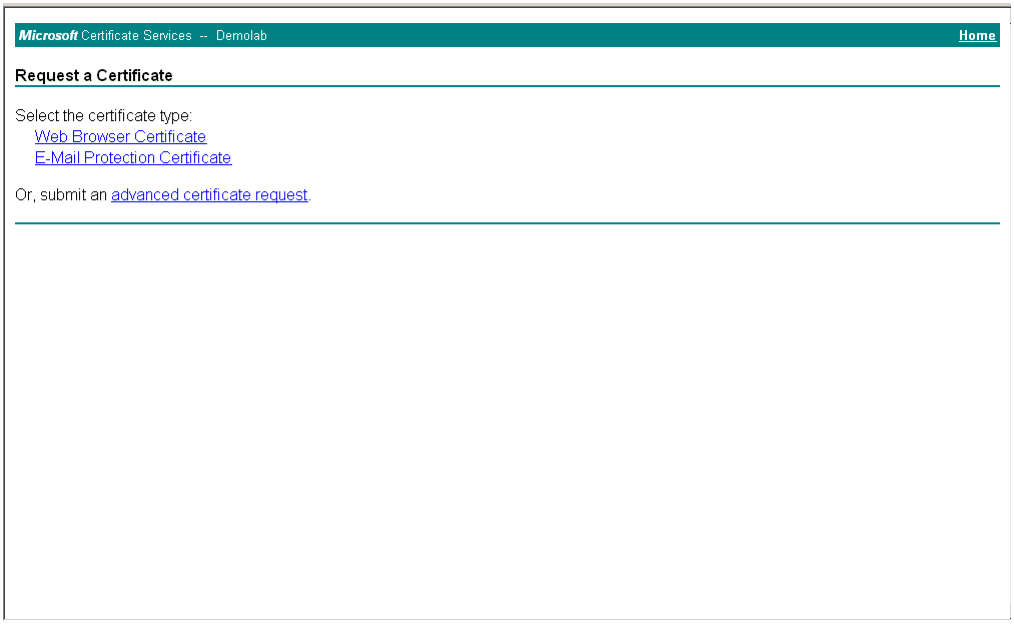
6. Open a Web browser and navigate to the Microsoft Certificates Services Web site at http://<certificate server>/CertSrv.

Figure 3-27: Microsoft Certificate Services Web Page



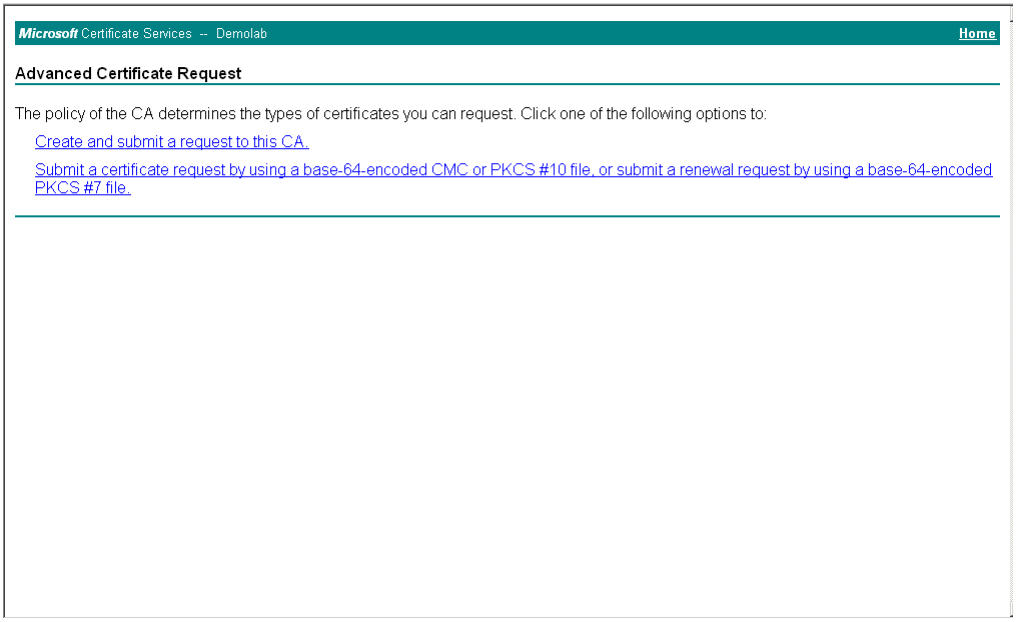
7. Click **Request a certificate**.

Figure 3-28: Request a Certificate Page



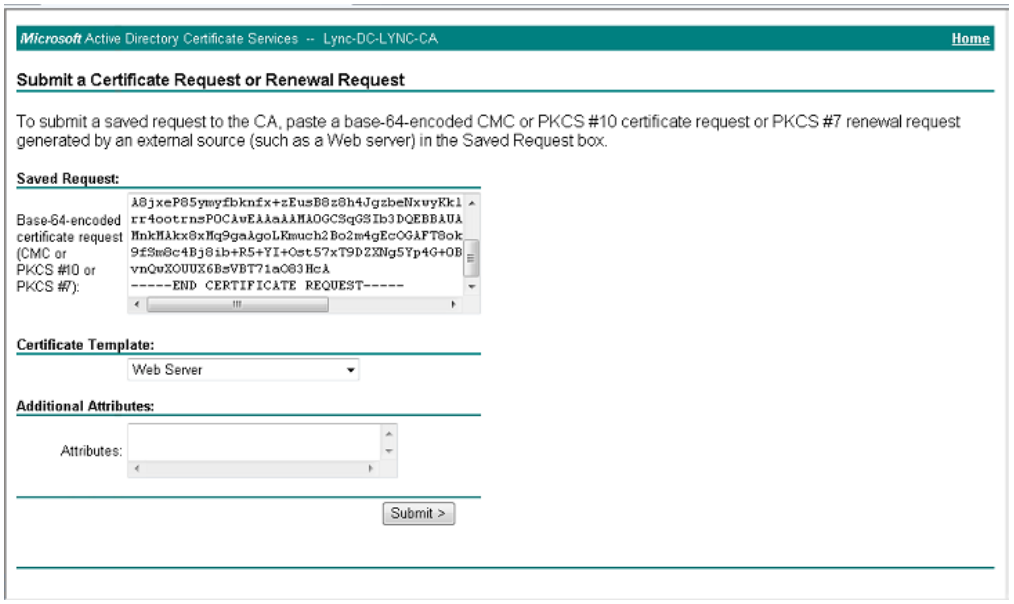
8. Click **advanced certificate request**, and then click **Next**.

Figure 3-29: Advanced Certificate Request Page



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

Figure 3-30: Submit a Certificate Request or Renewal Request Page

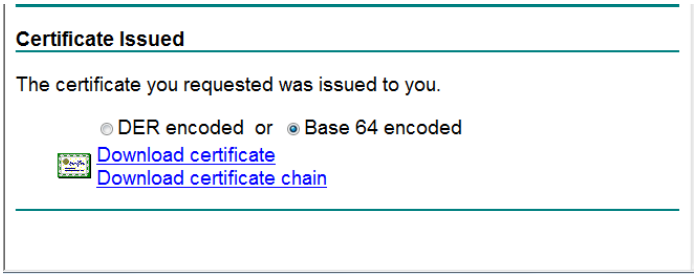


10. Open the *certreq.txt* file that you created and saved in Step 5, and then copy its contents to the 'Saved Request' field.

11. From the 'Certificate Template' drop-down list, select **Web Server**.

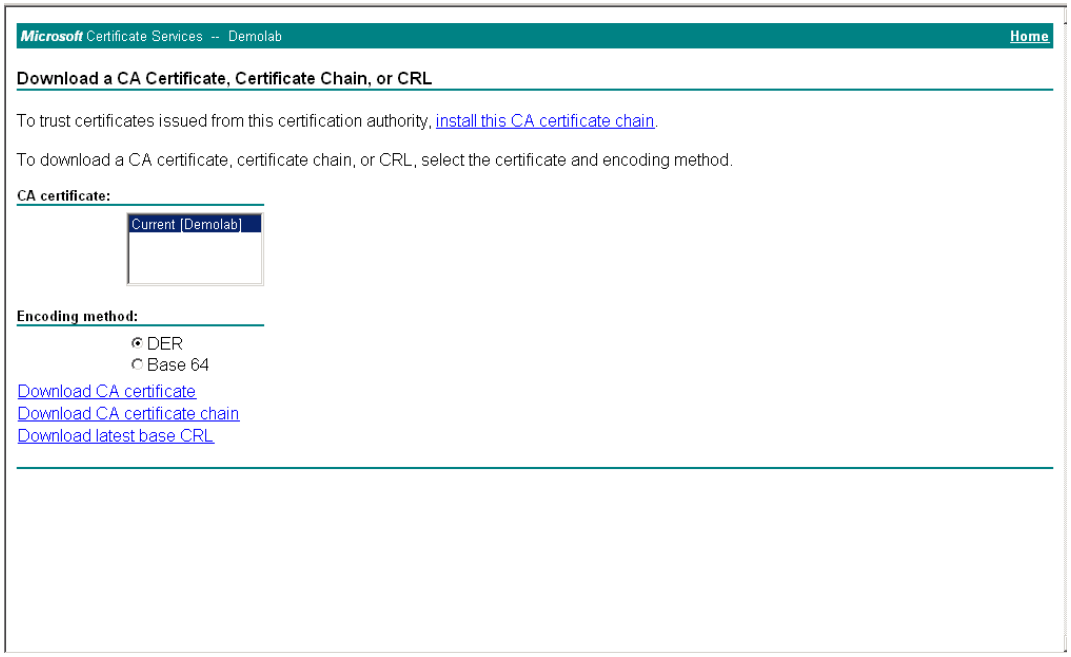
12. Click **Submit**.

Figure 3-31: Certificate Issued Page



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

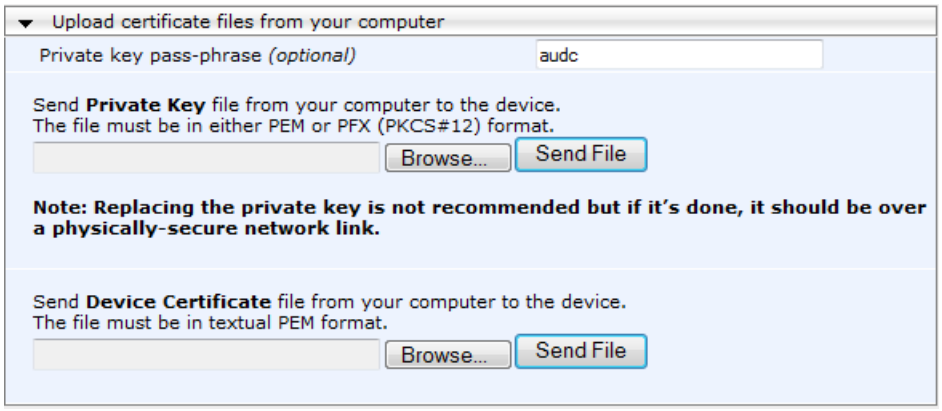
Figure 3-32: Download a CA Certificate, Certificate Chain, or CRL Page



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

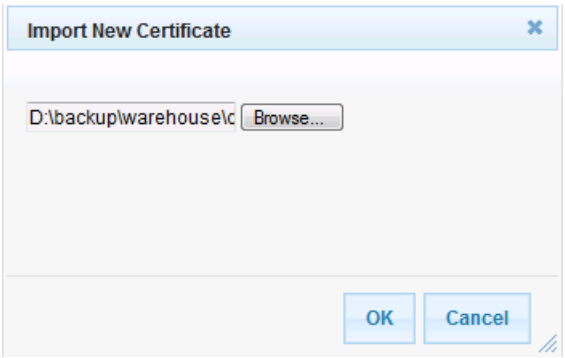
20. In the E-SBC's Web interface, return to the **TLS Contexts** page and do the following:
    a. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the *gateway.cer* certificate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

Figure 3-33: Upload Device Certificate Files from your Computer Group



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

Figure 3-34: Importing Root Certificate into Trusted Certificates Store



21. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
22. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.14 on page 67).

3.9 Step 9: Configure SRTP

Note: This step is required **only** for UC System (Microsoft Lync Server 2013), which uses media security.

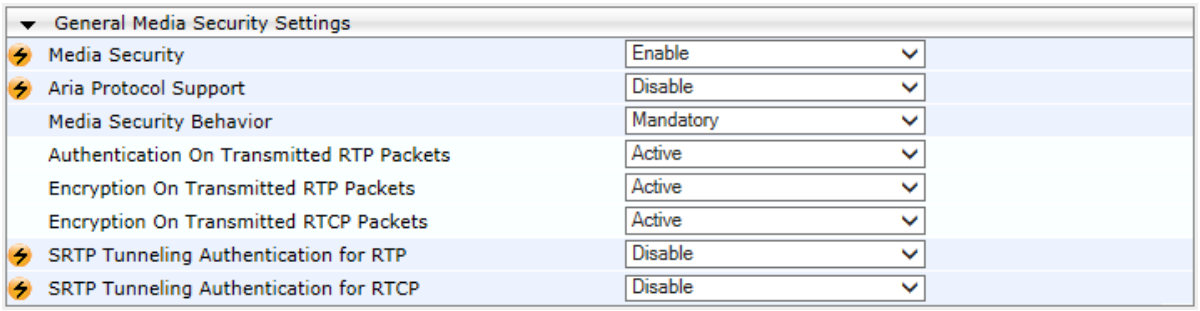
This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 3.6 on page 31).

➢ **To configure media security:**

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

Parameter	Value
Media Security	**Enable**

Figure 3-35: Configuring SRTP



3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.14 on page 67).

3.10 Step 10: Configure Maximum IP Media Channels

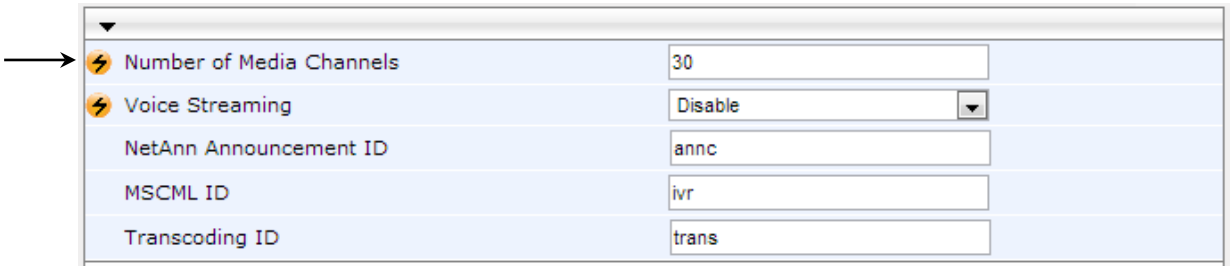
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

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

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

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

Figure 3-36: Configuring Number of IP Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **30**).
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 3.14 on page 67).

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

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.5 on page 29, IP Group 1 represents UC System/IP-PBX, and IP Group 2 represents Level 3 SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between UC System/IP-PBX (LAN) and Level 3 SIP Trunk (WAN):

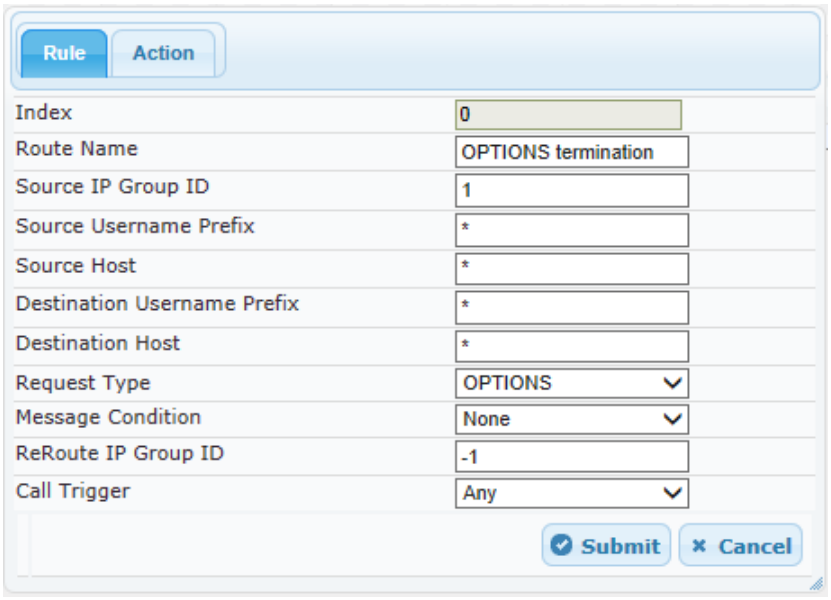
- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from UC System/IP-PBX to Level 3 SIP Trunk
- Calls from Level 3 SIP Trunk to UC System/IP-PBX

➢ **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:
3. Click **Add**.
4. Click the **Rule** tab, and then configure the parameters as follows:

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

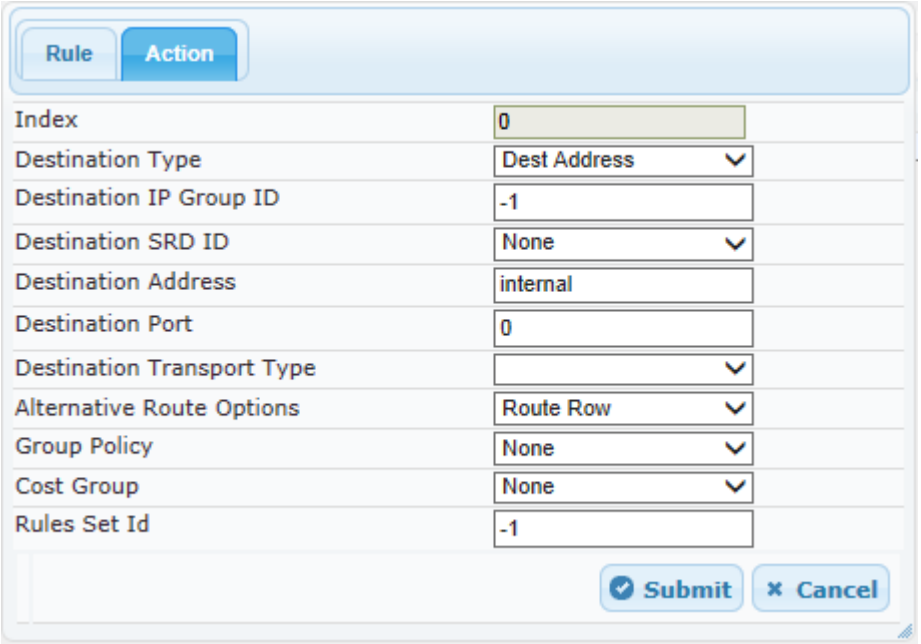
Figure 3-37: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



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

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

Figure 3-38: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

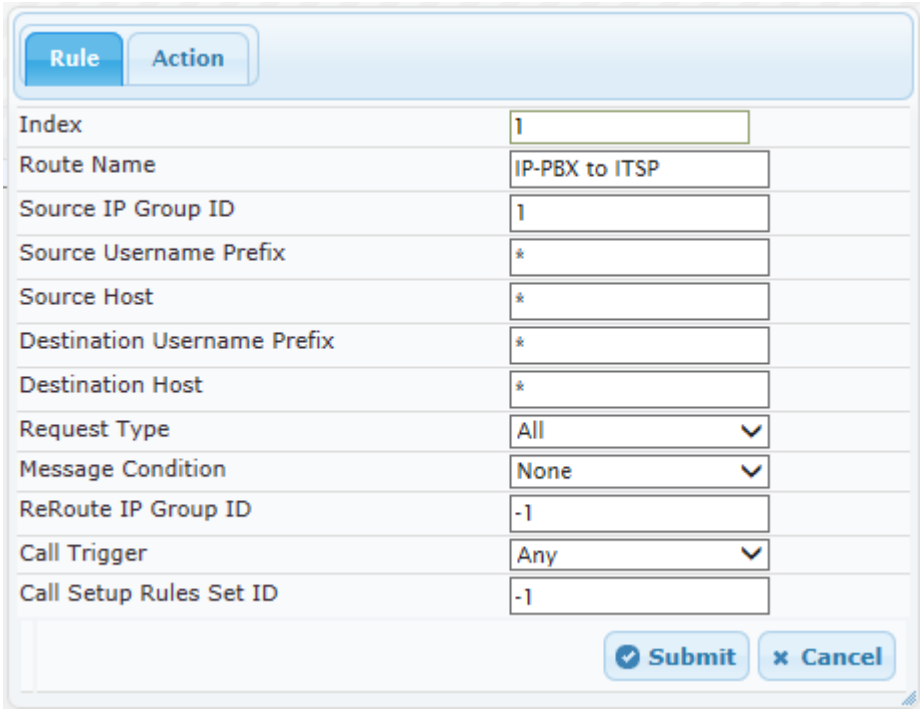


6. Configure a rule to route calls from UC System/IP-PBX to Level 3 SIP Trunk:
7. Click **Add**.

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

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

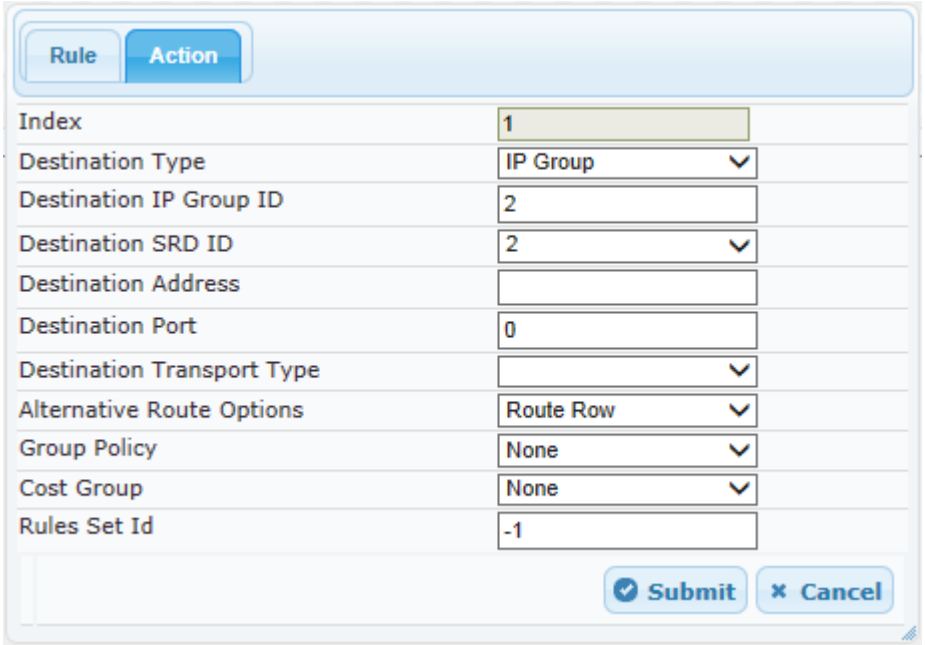
Figure 3-39: Configuring IP-to-IP Routing Rule for IP-PBX to ITSP – Rule tab



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

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

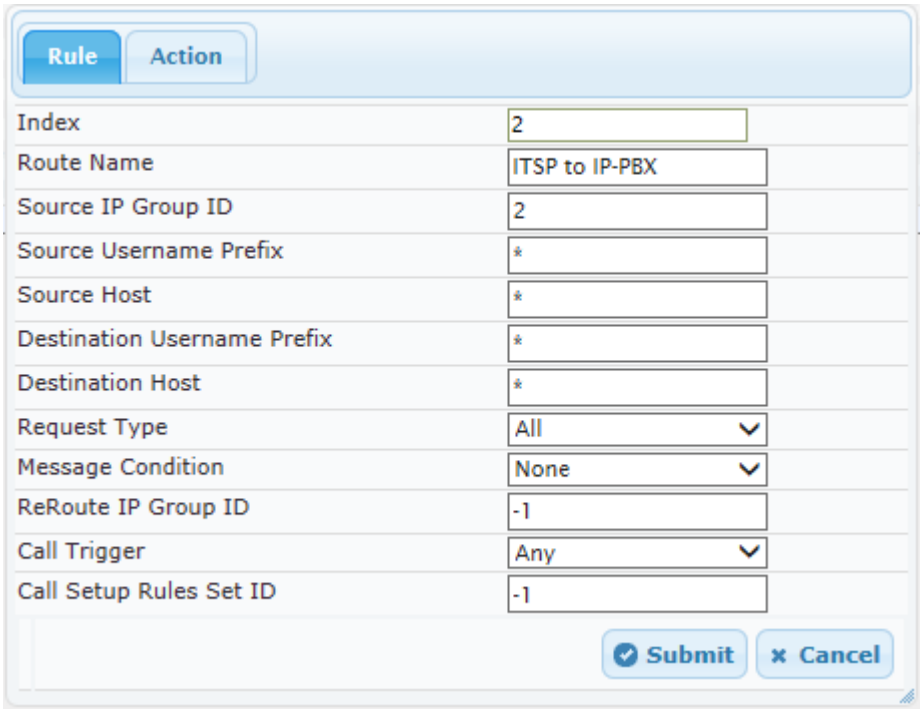
Figure 3-40: Configuring IP-to-IP Routing Rule for IP-PBX to ITSP – Action tab



10. Configure a rule to route calls from Level 3 SIP Trunk to UC System/IP-PBX:
11. Click **Add**.
12. Click the **Rule** tab, and then configure the parameters as follows:

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

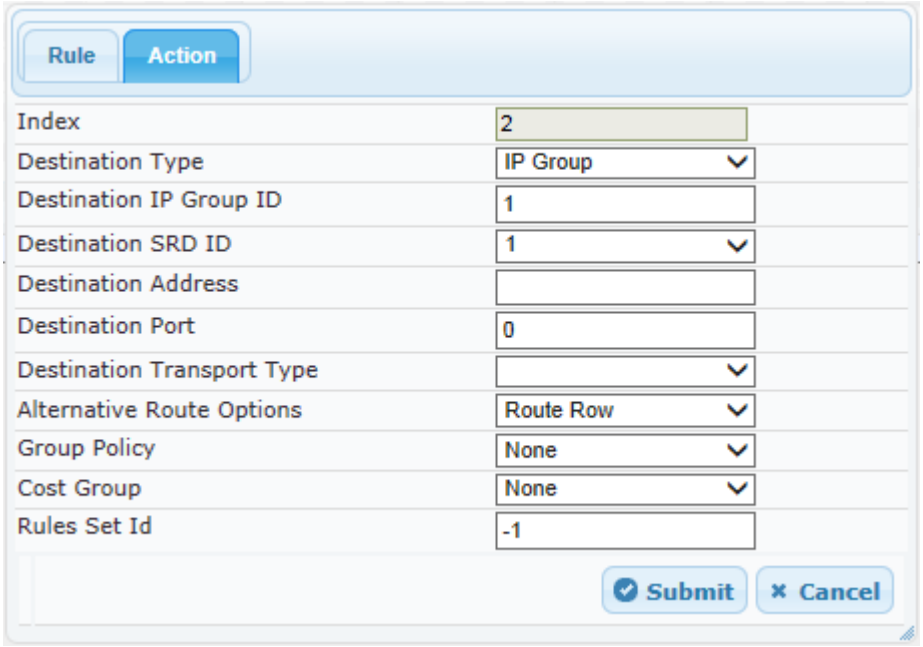
Figure 3-41: Configuring IP-to-IP Routing Rule for ITSP to IP-PBX – Rule tab



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

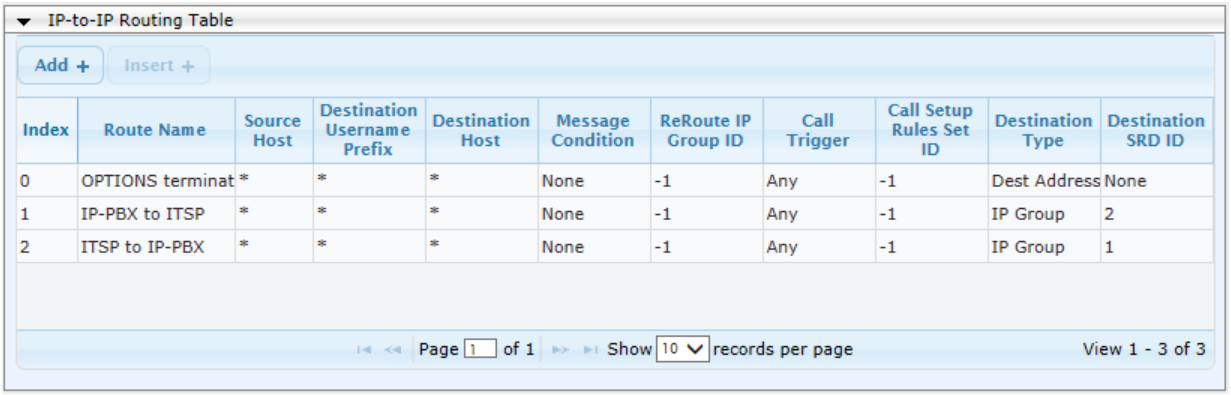
Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 3-42: Configuring IP-to-IP Routing Rule for ITSP to IP-PBX – Action tab



The configured routing rules are shown in the figure below:

Figure 3-43: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



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

3.12 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.

3.12.1 SIP Message Manipulation Rules for Microsoft Lync Server 2013

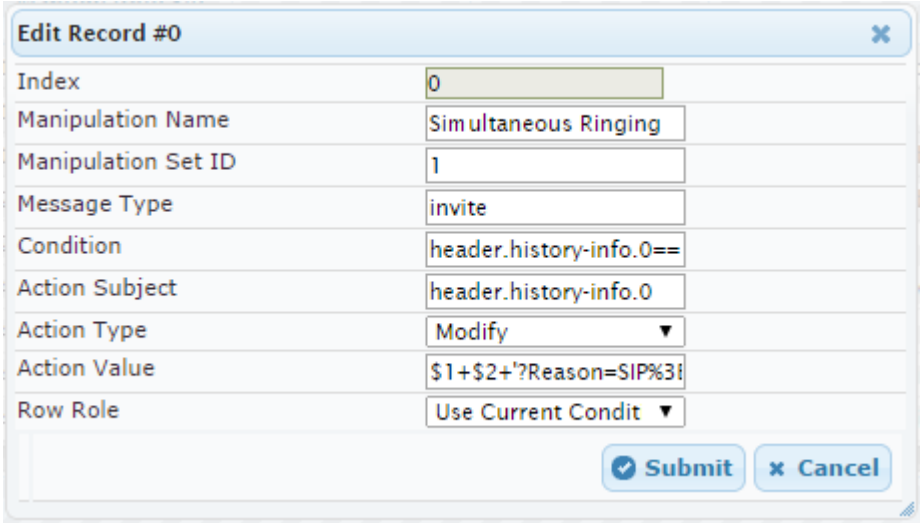
This step describes how to configure the SIP Message Manipulation rules for Microsoft Lync Server 2013.

➢ **To configure SIP Message manipulation rules for Lync 2013:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a manipulation rule (Manipulation Set 1) for Lync Server 2013. This rule applies to messages received from the Lync Server 2013 (IP Group 1) for simultaneous ringing initiated by the Lync Server 2013 (IP Group 1). This rule adds an Action Value containing the Reason for the History-Info header, which causes the E-SBC to add a Diversion Header towards the SIP Trunk.

Parameter	Value
Index	**0**
Manipulation name	**Simultaneous Ringing**
Manipulation Set ID	**1**
Message Type	**invite**
Condition	**header.history-info.0==regex.(<.*)(user=phone)(>)(.*)**
Action Subject	**header.history-info.0**
Action Type	**Modify**
Action Value	**$1+$2+'?Reason=SIP%3Bcause%3D404'+$3+$4**

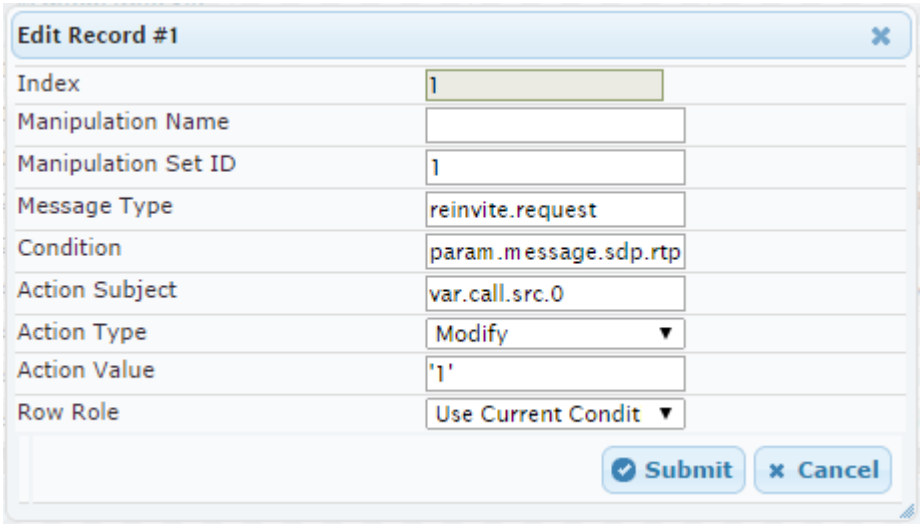
Figure 3-44: Configuring SIP Message Manipulation Rule 0 (for Lync Server 2013)



3. For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-initiated Hold), create a variable and set it to **'1'**. This variable manages how the call will be handled in each state (answer, request, etc.).

Parameter	Value
Index	**1**
Manipulation Set ID	**1**
Message Type	**reinvite.request**
Condition	**param.message.sdp.rtpmode=='sendonly'**
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'1'**
Row Role	**Use Current Condition**

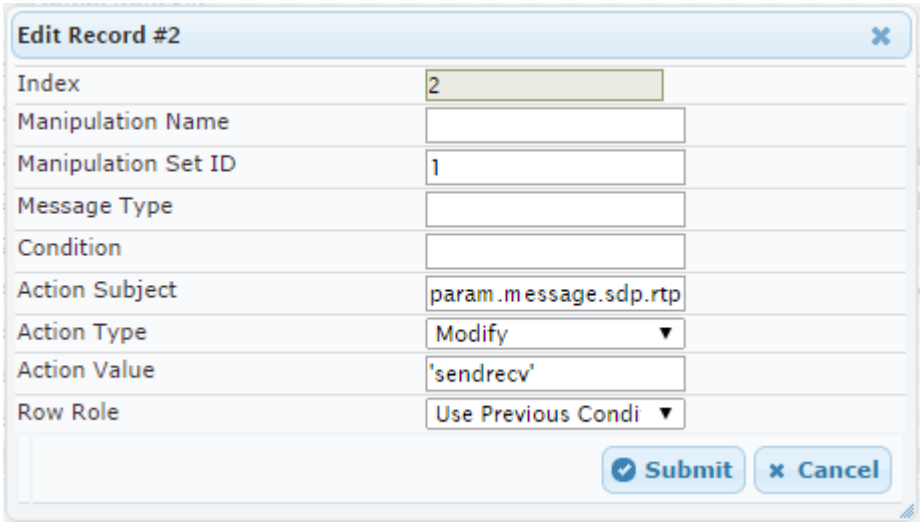
Figure 3-45: Configuring SIP Message Manipulation Rule 1 (for Microsoft Lync)



4. If the manipulation rule Index 1 (above) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to “sendonly”. change it to “sendrecv”.

Parameter	Value
Index	**2**
Manipulation Set ID	**1**
Message Type	
Condition	
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**‘sendrecv’**
Row Role	**Use Previous Condition**

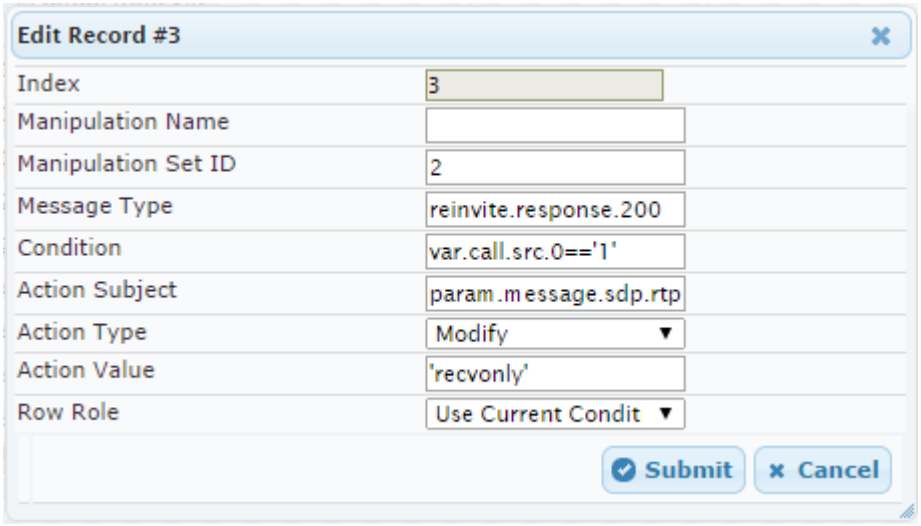
Figure 3-46: Configuring SIP Message Manipulation Rule 2 (for Microsoft Lync)



5. The following rule attempts to normalize the call processing state back to Lync 2013 for the correct reply to the initially received “sendonly”. For every SIP Re-INVITE message with the variable set to **'1'**, change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the Level 3 SIP Trunk to the Lync initiated Hold.

Parameter	Value
Index	**3**
Manipulation Set ID	**2**
Message Type	**reinvite.response.200**
Condition	**var.call.src.0==”1”**
Action Subject	**param.message.sdp.rtpmode**
Action Type	**Modify**
Action Value	**‘recvonly’**
Row Role	**Use Current Condition**

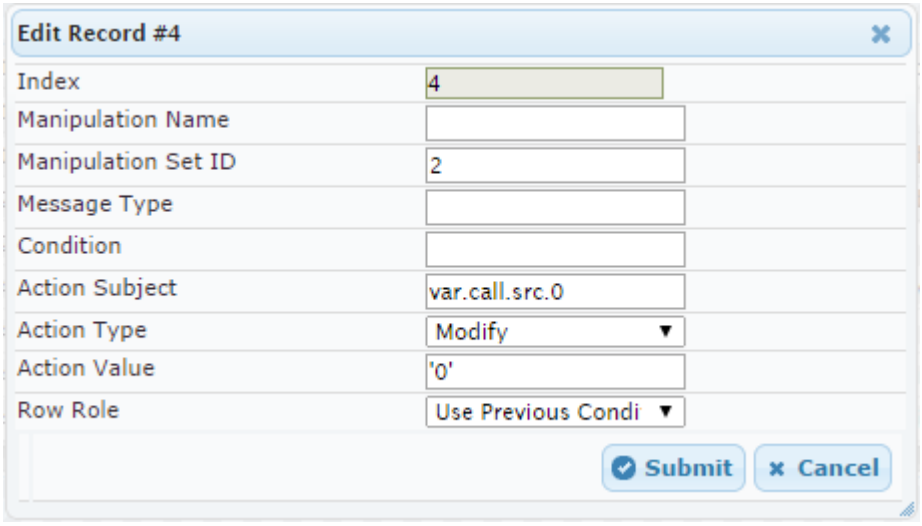
Figure 3-47: Configuring SIP Message Manipulation Rule 3 (for Microsoft Lync)



6. If the manipulation rule Index 3 (above) is executed, then the following rule is also executed. If the variable is determined to be set to **"1"** (in the previous manipulation rule), then set it to **"0"** to normalize the call processing state. Lync now sends Music on Hold to the Level 3 SIP Trunk. The call is now truly on hold with Music on Hold.

Parameter	Value
Index	**4**
Manipulation Set ID	**2**
Message Type	
Condition	
Action Subject	**var.call.src.0**
Action Type	**Modify**
Action Value	**'0'**
Row Role	**Use Previous Condition**

Figure 3-48: Configuring SIP Message Manipulation Rule 4 (for Microsoft Lync)



3.12.2 SIP Message Manipulation Rules for Level 3 SIP Trunk

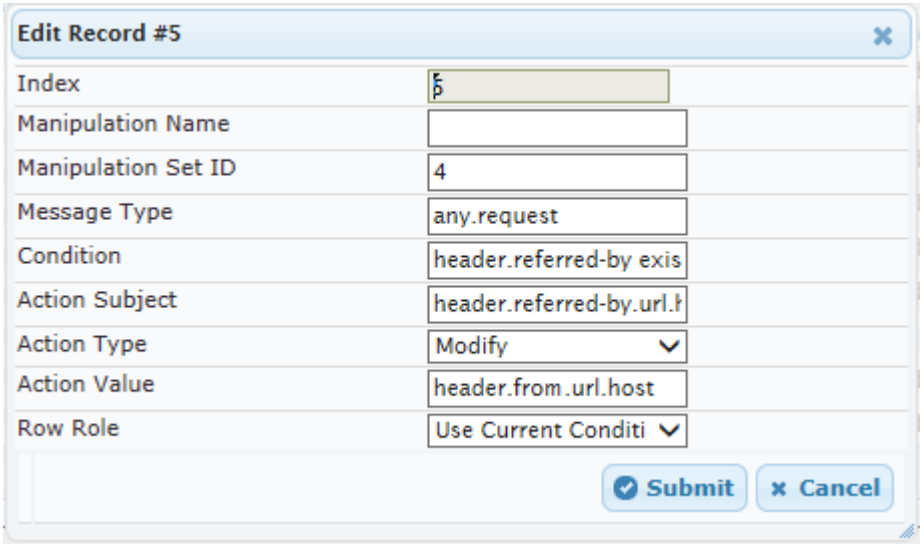
This step describes how to configure the SIP Message Manipulation rules for Level 3 SIP Trunk.

➢ **To configure SIP Message manipulation rules for Level 3 SIP Trunk:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure another manipulation rule (Manipulation Set 4) for the Level 3 SIP Trunk. This rule applies to messages sent to the Level 3 SIP Trunk (IP Group 2). This replaces the host part of the Referred-By Header with the value from SIP From Header.

Parameter	Value
Index	**5**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header.referred-by exists**
Action Subject	**header.referred-by.url.host**
Action Type	**Modify**
Action Value	**header.from.url.host**

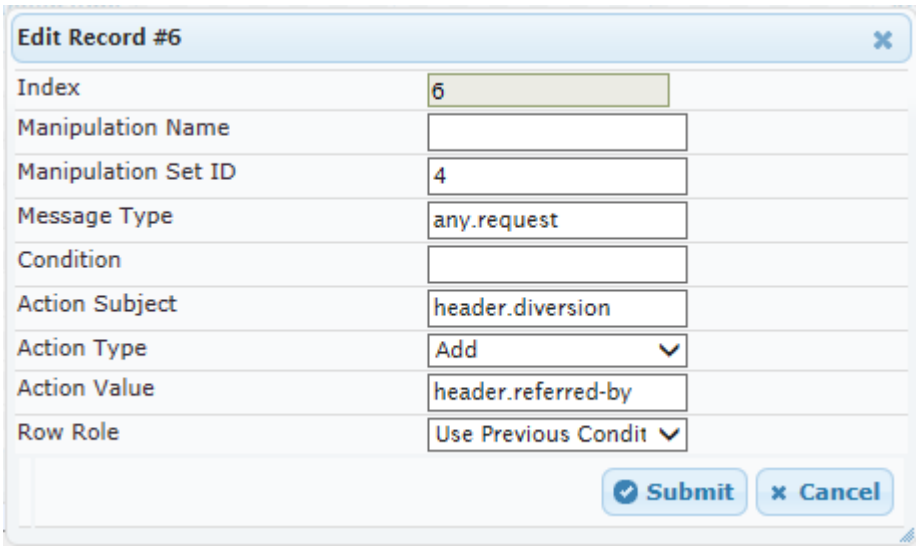
Figure 3-49: Configuring SIP Message Manipulation Rule 5 (for Level 3 SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 4) for Level 3 SIP Trunk. This rule applies to messages sent to the Level 3 SIP Trunk (IP Group 2) based on the previous rule condition. This rule adds the SIP Diversion Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	**6**
Manipulation Set ID	**4**
Message Type	**any.request**
Action Subject	**header.diversion**
Action Type	**Add**
Action Value	**header.referred-by**
Row Role	**Use Previous Condition**

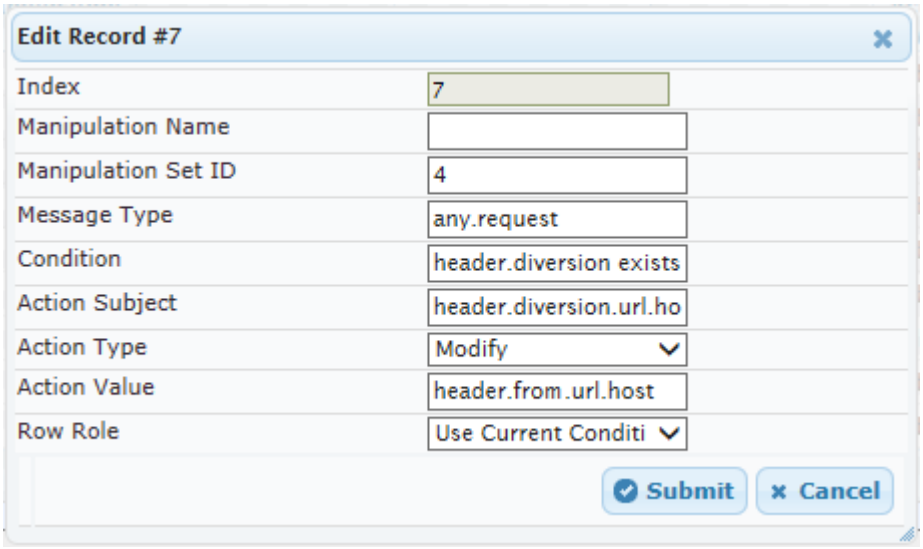
Figure 3-50: Configuring SIP Message Manipulation Rule 6 (for Level 3 SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 4) for Level 3 SIP Trunk. This rule applies to messages sent to the Level 3 SIP Trunk (IP Group 2). This rule replaces the host part of the Diversion Header with the value from From Header.

Parameter	Value
Index	**7**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header.diversion exists**
Action Subject	**header.diversion.url.host**
Action Type	**Modify**
Action Value	**header.from.url.host**

Figure 3-51: Configuring SIP Message Manipulation Rule 7 (for Level 3 SIP Trunk)



5. Configure another manipulation rule (Manipulation Set 4) for Level 3 SIP Trunk. This rule is applied to different response messages sent to the Level 3 SIP Trunk (IP Group 2) for Rejected Calls initiated by the IP-PBX (IP Group 1). This replaces the method types '406' , '503' and '603' with the value '486', because Level 3 SIP Trunk does not recognizes the '603' method type.

Parameter	Value
Index	**8**
Manipulation Name	**Reject Call**
Manipulation Set ID	**4**
Message Type	**any.response**
Condition	**header.request-uri.methodtype=='603'||'503'||'406'**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'486'**
Row Role	**Use Current Condition**

Figure 3-52: Configuring SIP Message Manipulation Rule 8 (for Level 3 SIP Trunk)

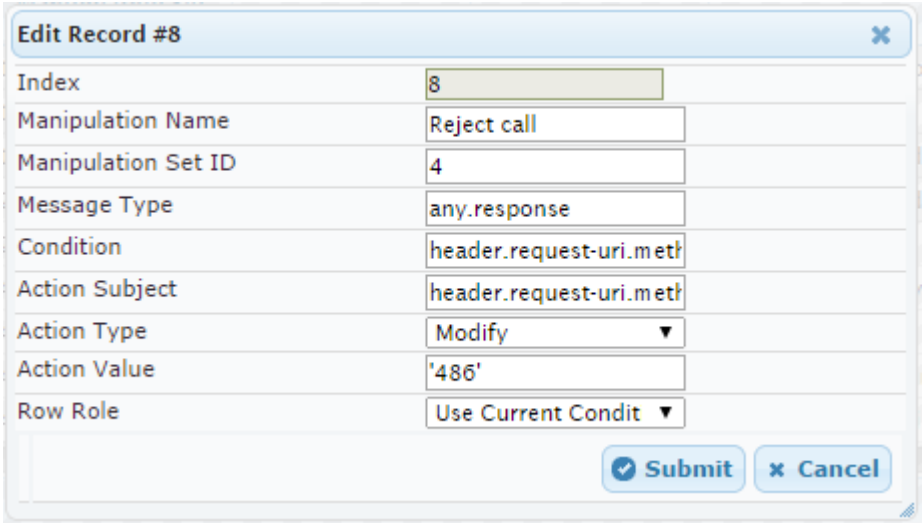
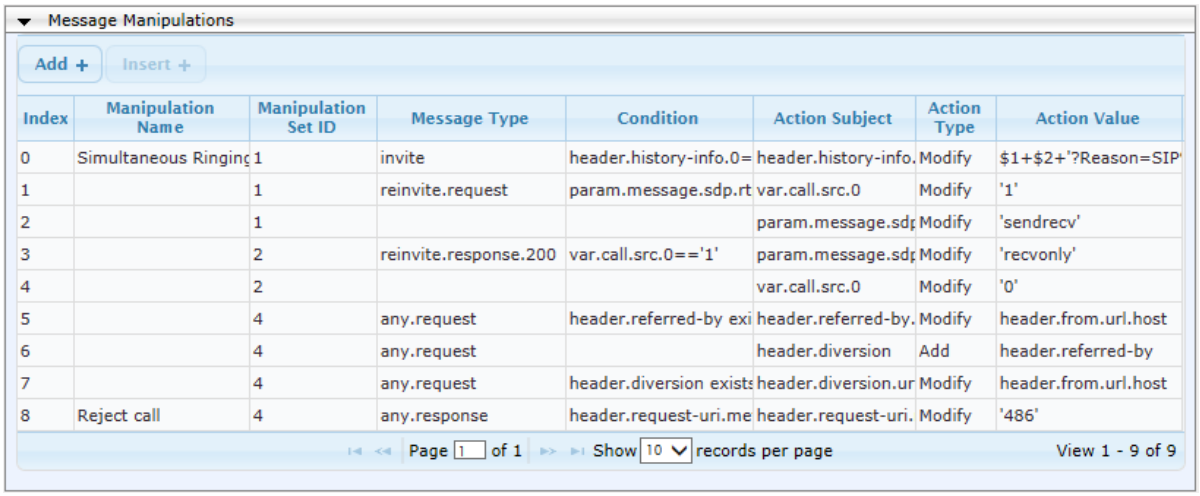


Figure 3-53: Configured SIP Message Manipulation Rules



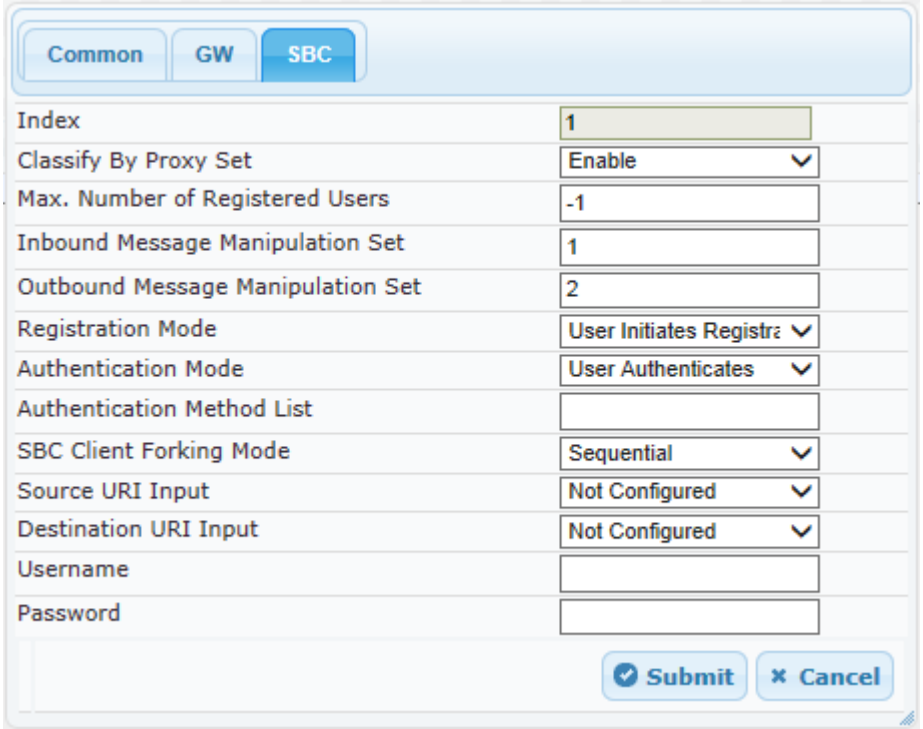
The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set IDs 1, 2, and 4) which are executed for messages sent to and from the Level 3 SIP Trunk (IP Group 2) as well as the Lync Server 2013 (IP Group 1). These rules are specifically required to enable proper interworking between Level 3 SIP Trunk and Lync Server 2013. The specific items are needed to support Music on Hold (rules 1-4). Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule applies to messages received from the Lync Server 2013 (IP Group 1), for simultaneous ringing initiated by the Lync Server 2013 (IP Group 1). This rule adds an Action Value containing the Reason for the History-Info header, causing the E-SBC to add a Diversion Header towards the SIP Trunk.	

Rule Index	Rule Description	Reason for Introducing Rule
1	For every SIP Re-INVITE request with SDP, where RTP mode = "sendonly" (occurs in a Lync 2013-initiated Hold), create a variable and set it to **'1'**. This variable manages how the call will be handled in each state (answer, request, etc.).	In the Call Park scenario, Microsoft Lync sends Re-INVITE messages twice. The first message is sent with the SDP, where the RTP mode is set to "a=inactive". The second message is sent with "a=sendonly". The Level 3 SIP Trunk has a problem recognizing two sequential Re-INVITE messages with different RTP modes. This causes the loss of the Music On Hold functionality in the Call Park scenario. These four rules are applied to work around this limitation.
2	If the previous manipulation rule (Index 0) is executed, then the following rule is also executed on the same SIP message: if RTP mode within the SDP is set to "sendonly", change it to "sendrecv".	
3	This rule attempts to normalize the call processing state back to Lync 2013 for the correct reply to the initially received "sendonly". For every SIP Re-INVITE message with the variable set to **'1'**, change RTP mode to "recvonly". This SIP Re-INVITE message is the response sent from the Level 3 SIP Trunk to the Lync-initiated Hold.	
4	If the manipulation rule Index 2 (above) is executed, then the following rule is also executed. If the variable is determined to be set to **"1"** (in the previous manipulation rule), then set it to **"0"** to normalize the call processing state. Lync now sends Music on Hold to the Level 3 SIP Trunk even without the Level 3 SIP Trunk knowing how to receive MoH. The call is now truly on hold with MoH.	
5	This rule applies to messages sent to the Level 3 SIP Trunk (IP Group 2). This rule replaces the host part of the Referred-By Header with the value from SIP From Header.	
6	This rule applies to messages sent to the Level 3 SIP Trunk (IP Group 2) based on the previous rule condition. This rule adds the SIP Diversion Header with the value from the SIP Referred-By Header.	For Call Transfer initiated by Lync/Cisco IP-PBX, Level 3 SIP Trunk needs to replace the SIP Referred-By Header with the Diversion Header.
7	This rule applies to messages sent to the Level 3 SIP Trunk (IP Group 2). This rule replaces the host part of the SIP Diversion Header with the value from SIP From Header.	
8	Level 3 SIP Trunk not recognizes '406', '503' and '603' method types.	This rule is applied to response messages sent to the Level 3 SIP Trunk (IP Group 2) for Rejected Calls initiated by the Lync/Cisco IP-PBX (IP Group 1). This replaces the method types '406', '503' and '603' with the value '486'.

6. Assign Manipulation Set IDs 1 and 2 to IP Group 1:
   a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
   b. Select the row of IP Group 1, and then click **Edit**.
   c. Click the **SBC** tab.
   d. Set the 'Inbound Message Manipulation Set' field to **1**.
   e. Set the 'Outbound Message Manipulation Set' field to **2**.

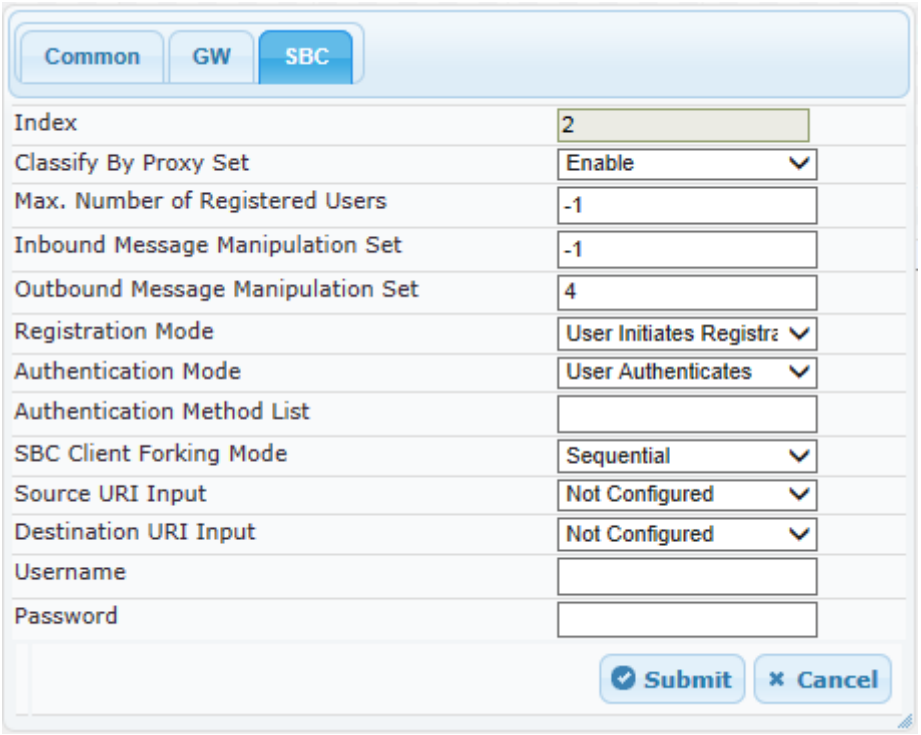
Figure 3-54: Assigning Manipulation Set to IP Group 1



   f. Click **Submit**.

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

Figure 3-55: Assigning Manipulation Set 4 to IP Group 2



   e. Click **Submit**.

3.13 Step 13: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

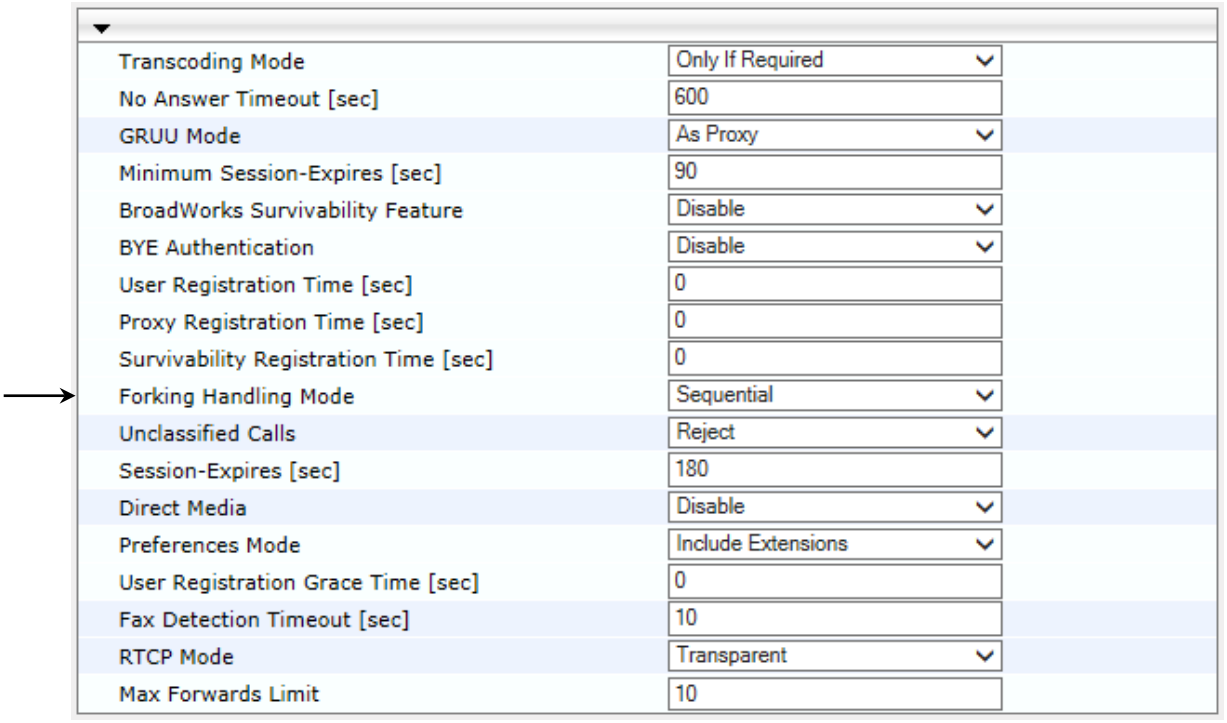
3.13.1 Step 13a: Configure Call Forking Mode

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

➢ **To configure call forking:**

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

Figure 3-56: Configuring Forking Mode



3. Click **Submit**.

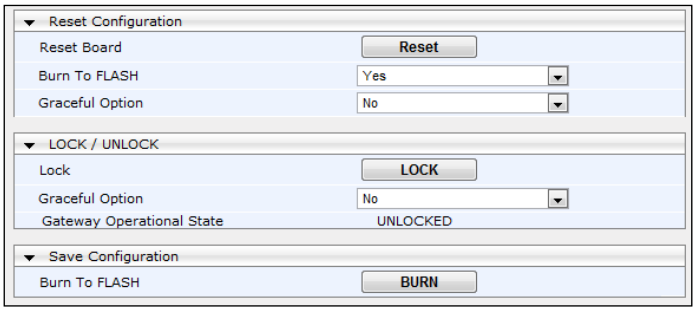
3.14 Step 14: Reset the E-SBC

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 3-57: 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 left intentionally blank

4 Configuration Requirements for SIP Third-party Vendor

This chapter describes the configuration requirements for the UC Solution/IP-PBX to operate with AudioCodes E-SBC towards the Level 3 SIP Trunk.

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

4.1 Required Configuration for Microsoft Lync Server 2013

The SIP History-Info header provides a method to verify the identity (ID) of the call forwarder (i.e., the Lync user number). This ID is required by the Level 3 SIP Trunk in the P-Asserted-Identity header. Therefore, 'Forward Call History' should be enabled on Lync Server 2013.

4.2 Required Configuration for Cisco UC Manager 10

The SIP Diversion header provides a method to verify the identity (ID) of the call forwarder (i.e., the Cisco UC user number). This ID is required by the Level 3 SIP Trunk in the SIP Diversion header. Therefore, the SIP Diversion header should be enabled on the Cisco UC Manager.

This page is intentionally left blank

A AudioCodes INI File Example

The *ini* configuration file of the E-SBC for Level 3 UDP SIP Trunk with Microsoft Lync Server 2013, corresponding to the Web-based configuration as described in Section 3 on page 13, 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 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 2265355
;Slot Number: 1
;Software Version: 6.80A.231.003
;DSP Software Version: 5014AE3_R => 680.22
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 369M   Flash size: 64M   Core speed: 300Mhz
;Num of DSP Cores: 3  Num DSP Channels: 62
;Num of physical LAN ports: 12
;Profile: NONE
;;Key features:;Board Type: 72 ;IP Media: Conf VXML
VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC ;System features: POE-
AF ;DSP Voice features: IpmDetector RTCP-XR AMRPolicyManagement ;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
;QOE features: VoiceQualityMonitoring MediaEnhancement ;Channel Type: RTP
DspCh=62 IPMediaDspCh=62 ;PSTN FALLBACK Supported ;E1Trunks=2 ;T1Trunks=2
;FXSPorts=4 ;FXOPorts=4 ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;Control Protocols: MGCP MEGACO H323 SIP TPNCP
SASurvivability SBC=60 MSFT CLI TRANSCODING=60 FEU=60 TestCall=60
SIPRec=60 CODER-TRANSCODING=60 EMS SBC-SIGNALING=60 SBC-MEDIA=60 ;Default
features:;Coders: G711 G726;

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


[SYSTEM Params]

SyslogServerIP = 10.15.17.100
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = 7200
```

```
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '10.15.25.1'
;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

[BSP Params]

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

[Analog Params]

FarEndDisconnectType = 7

[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]

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

[PSTN Params]


[SS7 Params]


[Voice Engine Params]

ENABLEMEDIASECURITY = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

UseRProductName = 'Mediant 800 E-SBC'
WebLogoText = 'Level 3'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSCertFileName is hidden but has non-default value
;HTTPSRootFileName is hidden but has non-default value
;INILoadMode is hidden but has non-default value
```

```
[SIP Params]

MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
MEDIASECURITYBEHAVIOUR = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SCTP Params]


[IPsec Params]


[Audio Staging Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 1, 4, "LAN Port#1", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "LAN Port#2", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "WAN Port#1", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "WAN Port#2", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 0, 1, 4, "User Port #4", "None", "  ";
PhysicalPortsTable 5 = "FE_5_2", 0, 1, 4, "User Port #5", "None", "  ";
PhysicalPortsTable 6 = "FE_5_3", 0, 1, 4, "User Port #6", "None", "  ";
PhysicalPortsTable 7 = "FE_5_4", 0, 1, 4, "User Port #7", "None", "  ";
PhysicalPortsTable 8 = "FE_5_5", 1, 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 1, 4, "User Port #11", "GROUP_6",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]
```

```
FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

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

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, 1, "Voice",
10.15.25.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.159, 25, 195.189.192.129, 2,
"WANSP", 80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]


[ DspTemplates ]

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

[ \DspTemplates ]


[ CpMediaRealm ]
```

```
FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "Voice", "", 6000, 10, 6090, 1, "", "";
CpMediaRealm 1 = "MRWan", "WANSP", "", 7000, 10, 7090, 0, "", "";

[ \CpMediaRealm ]


[ SRD ]

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

[ \SRD ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "lync.local:5067", 2, 1;
ProxyIp 1 = "4.55.43.97:5060", 0, 2;

[ \ProxyIp ]


[ IpProfile ]

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

```
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 1, 0, 0, "", 1, -1, 0, 1, 1,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3, 1, 1, 1, 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, 1, 0,
0, 300;
IpProfile 2 = "Level 3", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", 2, 0, 0, "", 2, -1, 1, 2,
0, 0, 1, 0, 8, 300, 400, 1, 2, 0, -1, 0, 0, 1, 3, 2, 2, 2, 1, 3, 0, 1, 0,
1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 300;

[ \IpProfile ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 1 = "Lync", 1, 60, 1, 1, 1, 0, "-1", 1, -1, "";
ProxySet 2 = "Level 3", 1, 60, 1, 1, 2, 0, "-1", 1, -1, "";

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "Lync", 1, "195.189.192.159", "", 0, -1, -1, 0, -1, 1,
"MRLan", 1, 1, -1, 1, 2, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "",
"", "", 0, "", "";
```

```
IPGroup 2 = 0, "Level 3", 2, "195.189.192.159", "", 0, -1, -1, 0, -1, 2,
"MRWan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "",
"", "", 0, "", "";

[ \IPGroup ]


[ IP2IPRouting ]

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

[ \IP2IPRouting ]


[ TLSContexts ]

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

[ \TLSContexts ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet;
SIPInterface 1 = "Lync", "Voice", 2, 0, 0, 5067, 1, "", "", -1, 0, 500, -
1;
SIPInterface 2 = "Level 3", "WANSP", 2, 5060, 5060, 0, 2, "", "", -1, 0,
500, -1;

[ \SIPInterface ]


[ CodersGroup0 ]
```

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

[ \CodersGroup0 ]


[ CodersGroup1 ]

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

[ \CodersGroup1 ]


[ CodersGroup2 ]

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

[ \CodersGroup2 ]


[ AllowedCodersGroup1 ]

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

[ \AllowedCodersGroup1 ]


[ AllowedCodersGroup2 ]

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

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Simultaneous Ringing", 1, "invite",
"header.history-info.0==regex.(<.*)(user=phone)(>)(.*)", "header.history-
info.0", 2, "$1+$2+'?Reason=SIP%3Bcause%3D404'+$3+$4", 0;
MessageManipulations 1 = "", 1, "reinvite.request",
"param.message.sdp.rtpmode=='sendonly'", "var.call.src.0", 2, "'1'", 0;
```

```
MessageManipulations 2 = "", 1, "", "", "param.message.sdp.rtpmode", 2,
"'sendrecv'", 1;
MessageManipulations 3 = "", 2, "reinvite.response.200",
"var.call.src.0=='1'", "param.message.sdp.rtpmode", 2, "'recvonly'", 0;
MessageManipulations 4 = "", 2, "", "", "var.call.src.0", 2, "'0'", 1;
MessageManipulations 5 = "", 4, "any.request", "header.referred-by
exists", "header.referred-by.url.host", 2, "header.from.url.host", 0;
MessageManipulations 6 = "", 4, "any.request", "", "header.diversion", 0,
"header.referred-by", 1;
MessageManipulations 7 = "", 4, "any.request", "header.diversion exists",
"header.diversion.url.host", 2, "header.from.url.host", 0;
MessageManipulations 8 = "Reject call", 4, "any.response",
"header.request-uri.methodtype=='603'||'503'||'406'", "header.request-
uri.methodtype", 2, "'486'", 0;

[ \MessageManipulations ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

AudioCodes

Configuration Note

www.audiocodes.com