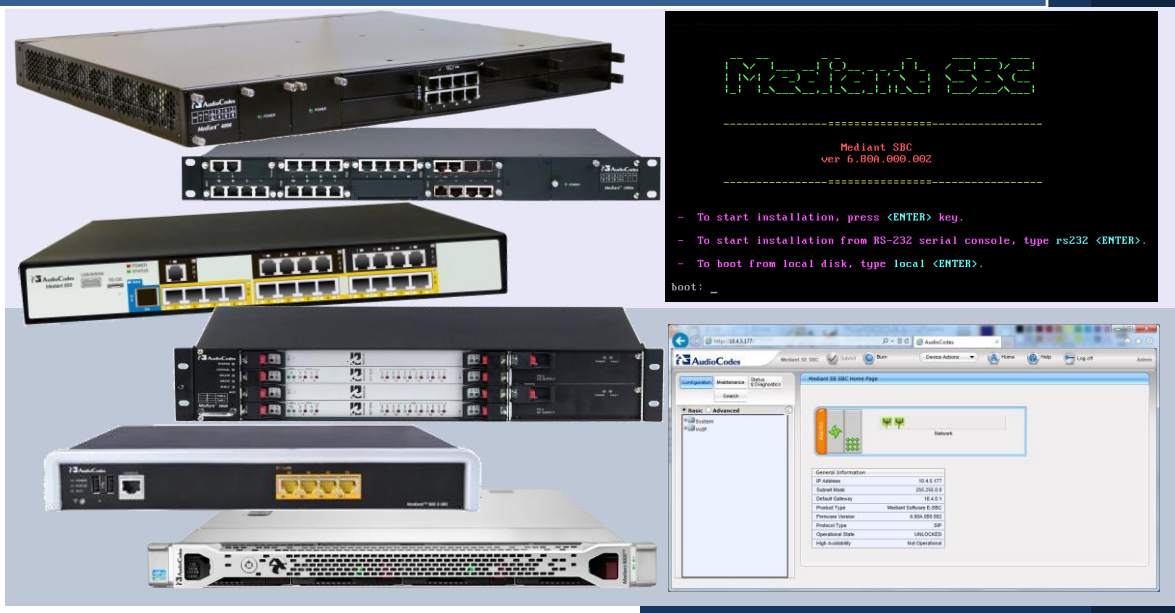
Session Border Controllers (SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

SAP Contact Center & Colt SIP Trunk using Mediant SBC



colt
smarter / faster / further

SAP

AudioCodes

April 2014

Document # LTRT-12290

Table of Contents

Reader's Notes

Notice

This Note shows how to connect a SAP Contact Center and Colt SIP Trunk using AudioCodes Mediant SBC product series, which includes the Mediant 500 E-SBC, Mediant 800 Gateway & E-SBC, Mediant 1000B Gateway & E-SBC, Mediant 2600 E-SBC, Mediant 3000 Gateway & E-SBC, Mediant 4000 SBC, Mediant 9000 SBC and Mediant Software SBC Server Edition and Virtual Edition.

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: April-22-2014

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.

Reader's Notes

1 Introduction

This Note shows how to configure AudioCodes' Session Border Controller (hereafter referred to as SBC) for interworking between Colt's SIP Trunk and SAP Contact Center (formally 'SAP Business Communications Management').

AudioCodes SBCs include the Mediant 500 E-SBC, Mediant 800 Gateway & E-SBC, Mediant 1000B Gateway & E-SBC, Mediant 2600 E-SBC, Mediant 3000 Gateway & E-SBC, Mediant 4000 SBC, Mediant 9000 SBC and Mediant Software SBC Server Edition and Virtual Edition.

Note: Throughout this document, the term 'SBC' also refers to AudioCodes' Mediant E-SBC product series.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and SAP Contact Center Partners who are responsible for installing and configuring Colt's SIP Trunk and SAP Contact Center for enabling VoIP calls using AudioCodes' SBC.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the enterprise and the Service Provider's VoIP networks.

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

1.3 About SAP Contact Center

SAP Contact Center provides you with a comprehensive communications platform and tools to deliver superior customer service. It helps you efficiently manage contact center operations, including inbound and outbound customer communications across multiple channels. The bundled contact center solution helps you improve customer service, adapt your contact center operations in real time, and lower the total cost of ownership.

Reader's Notes

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (Server Edition and Virtual Edition)
Software Version	SIP_ 6.80A.218.002
Protocol	▪ SIP/UDP (to the Colt SIP Trunk) ▪ SIP/UDP, TCP or TLS (to the SAP Contact Center system)
Additional Notes	None

2.2 Colt SIP Trunking Version

Table 2-2: Colt Version

Vendor/Service Provider	Colt
SSW Model/Service	Sonus
Software Version	8.4.4
Protocol	SIP
Additional Notes	None

2.3 SAP Contact Center Version

Table 2-3: SAP Contact Center Version

Vendor	SAP
Software Version	SAP Contact Center 7 SP6 Patch1
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

SAP Contact Center can be connected to the SIP trunk with an SBC in a number of possible topological scenarios:

- SAP Contact Center can be provided as a service and SIP trunks connect to the SAP Contact Center Service Provider
- SAP Contact Center can be provided as a service and SIP trunks connect to the customer network
- SAP Contact Center can be an in-house system and SIP trunks can be connected to the in-house network
- SAP Contact Center can be connected to an IP PBX or UC system over a SIP trunk

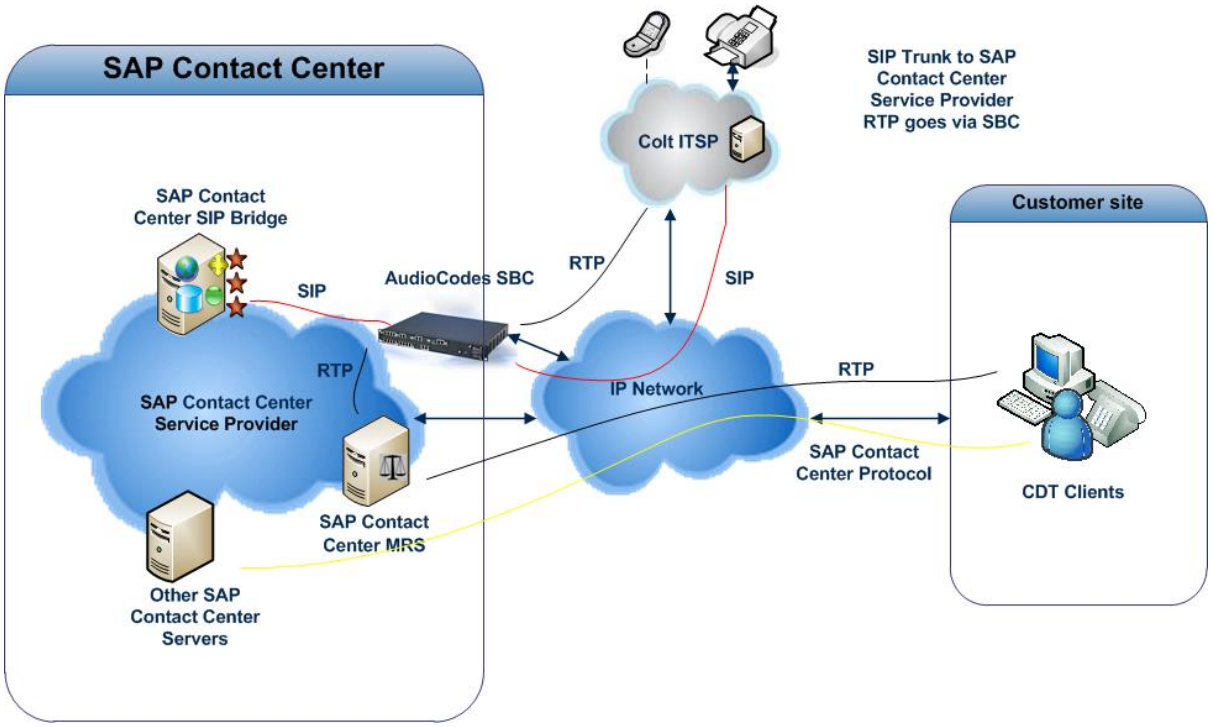
Note: Contact your SAP Contact Center support channel for more information about topological scenarios.

Interoperability testing between AudioCodes SBC and Colt SIP Trunk with SAP Contact Center 7.x was performed using the following topology:

- Enterprise deployed with a SAP Contact Center as a service using robust contact center functionality and interactive voice response (IVR) to efficiently connect customers with the right agents and information at the right time.
- Enterprise connected the SAP Contact Center system to the PSTN network using Colt's SIP Trunking service (Internet Telephony Service Provider / ITSP).
- Colt SIP Trunk connected to the enterprise using the public external network.
- AudioCodes' SBC deployed to interconnect between the SAP Contact Center and the SIP trunk.
  - The SBC is connected to SAP Contact Center SIP Bridge in the SAP Contact Center internal network, and to Colt SIP Trunk located in the public network.
  - The SAP Contact Center SIP Bridge is effectively a protocol translator that translates between SIP and SAP Contact Center's proprietary control protocol using CDT agents.
  - RTP from/to Colt SIP trunk flow via an SBC to/from SAP Contact Center Media Routing Server (MRS).

The figure below illustrates the interoperability test topology:

Figure 2-1: Interoperability Test Topology



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ SAP Contact Center environment as a service is located on the SAP Contact Center Service Provider network ▪ SAP Contact Center terminals (CDT, SIP phone) is located on the enterprise's LAN ▪ Colt SIP Trunk is located on the WAN
Signaling Transcoding	▪ SAP Contact Center operates with SIP-over-UDP, TCP or TLS transport type ▪ Colt SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ SAP Contact Center supports G.711A-law and G.711U-law and G.729 coders ▪ Colt SIP Trunk supports G.729, G.711A-law, and G.726 coders
Media Transcoding	▪ SAP Contact Center and Colt SIP Trunk operate with RTP
DTMF	▪ SAP Contact Center supports delivering DTMF using SIP INFO message and RFC 2833 Named Telephony events ▪ Colt supports only RFC 2833
Session Expire	▪ SAP Contact Center supports session expire negotiation ▪ Colt SIP Trunk does not support session expire negotiation

3 Configuring AudioCodes SBC

This section shows how to configure AudioCodes SBC for interworking between SAP Contact Center and the Colt SIP Trunk. The configuration is based on the interoperability test topology described in Section 2.4 on page 10, and includes:

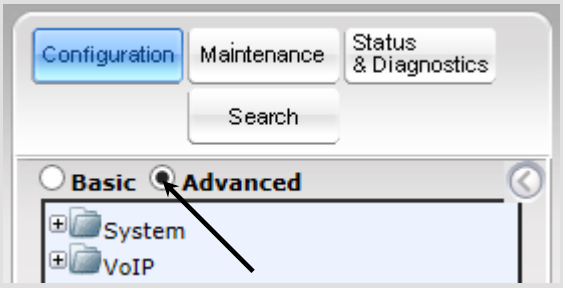
- SBC WAN interface - Colt SIP Trunking environment
- SBC LAN interface - SAP Contact Center environment

Configuration is performed using the SBC's embedded Web server (hereafter referred to as *Web interface*).

Notes:

- To implement the SAP Contact Center and Colt SIP Trunk based on the configuration described in this section, the SBC must be installed with a Software License Key that includes the following software features:
  - √ **SBC**
  - √ **Security**
  - √ **RTP**
  - √ **SIP**

  For more information about the Software License Key, contact your AudioCodes Sales Representative.
- The scope of this document does *not* cover security aspects of connecting the SIP Trunk to the SAP Contact Center environment. Security measures should be implemented in line with the enterprise's security policies. For basic security guidelines, refer to the *Recommended Security Guidelines* document.
- Before you begin configuring the SBC, ensure that the SBC's Web interface navigation tree is in **Advanced** display mode, selectable as shown below:



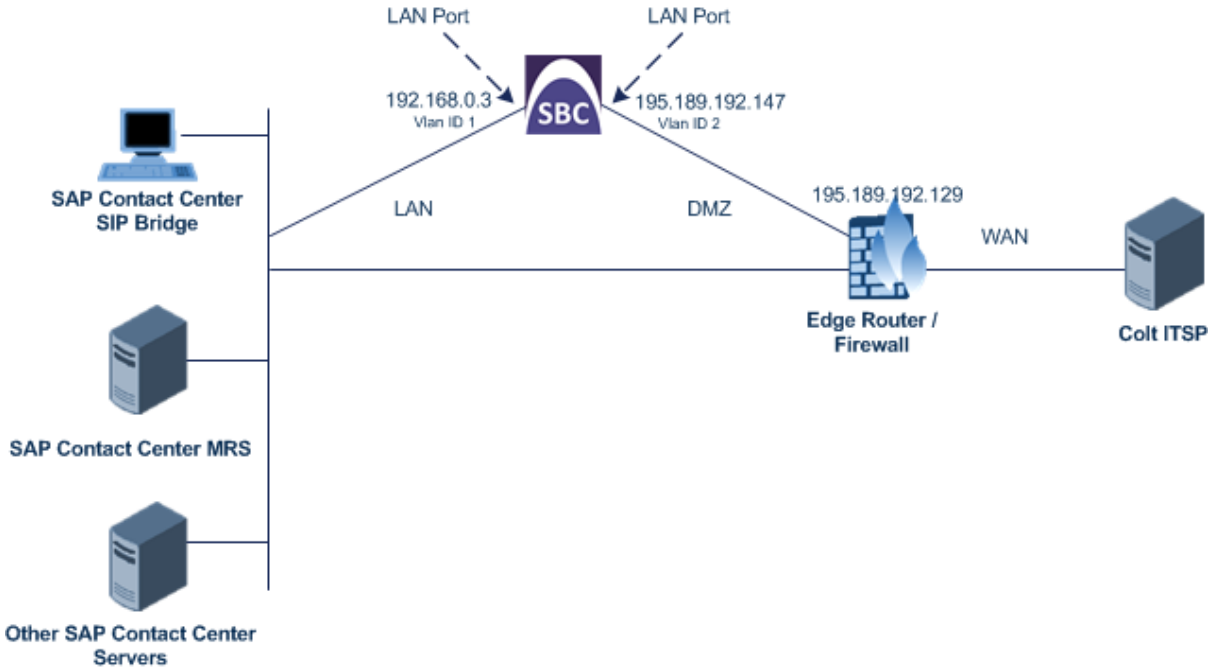
Note that when the SBC is reset, the navigation tree reverts to **Basic** display mode.

3.1 Step 1: Configure IP Network Interfaces

This step shows how to configure the SBC's IP network interfaces. A number of methods can be used to deploy the SBC; the interoperability test topology uses this method:

- SBC interfaces with these IP entities:
  - SAP Contact Center, located on the SAP Contact Center Service Provider network (LAN)
  - Colt SIP Trunk, located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection to the LAN: Type depends on the method used to connect to the SAP Contact Center Service Provider's network. In the interoperability test topology, SBC connects to the LAN and WAN using dedicated LAN ports (i.e., using two ports and two network cables).
- 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 shows how to define VLANs for each of the following interfaces:

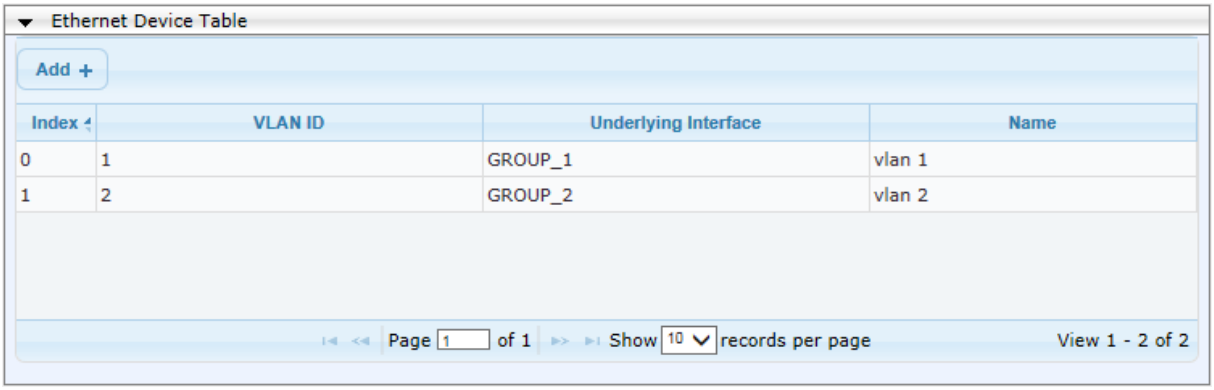
- LAN VoIP (assigned the name "SAP")
- WAN VoIP (assigned the name "ITSP")

➢ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**); In the table you'll see an existing row for VLAN ID 1 and underlying interface GROUP_1.
2. Add another VLAN ID 2 for the WAN side as follows:

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

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



3.1.2 Step 1b: Configure Network Interfaces

This step shows how to configure the

- LAN VoIP interface (assigned the name "SAP")

  -and-

- WAN VoIP interface (assigned the name "ITSP")

➢ **To configure these 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** option of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface as follows:

Parameter	Value
IP Address	**192.168.0.3** (IP address of SBC)
Prefix Length	**24** (subnet mask in bits for 255.255.255.0)
Gateway	**192.168.0.1**
VLAN ID	**1**
Interface Name	**SAP** (arbitrary descriptive name)
Primary DNS Server IP Address	Add DNS Server IP address in this network
Underlying Device	**vlan 1**

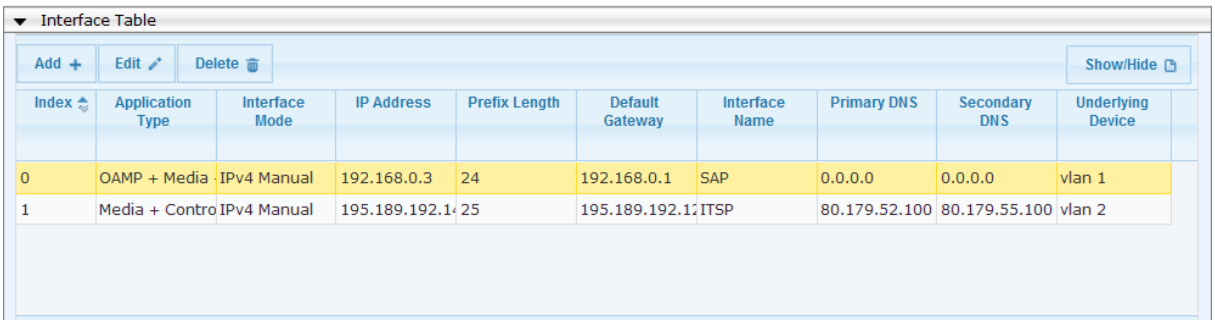
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**195.189.192.147** (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	**ITSP**
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 shows how to configure the Native VLAN ID for the LAN and WAN interfaces.

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

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

Figure 3-4: Configured Port Native VLAN

Physical Ports Settings

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

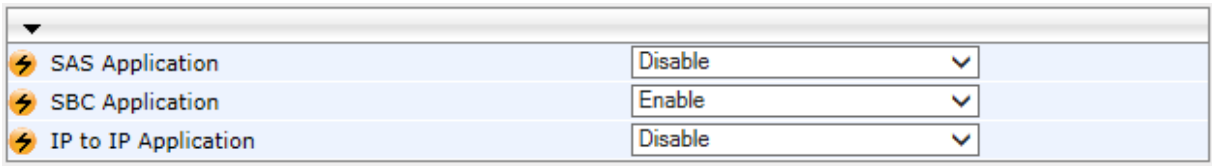
3.2 Step 2: Enable the SBC Application

This step shows how to enable the SBC application.

➢ **To enable the SBC application:**

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

Figure 3-5: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the SBC with a burn to flash for the setting to take effect (see Section 3.12 on page 48).

3.3 Step 3: Configure Signaling Routing Domains

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

The SRD comprises:

- Media Realm: defines a UDP port range for RTP/SRTP (media) traffic on a specific logical IP network interface of the 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 SBC.

3.3.1 Step 3a: Configure Media Realms

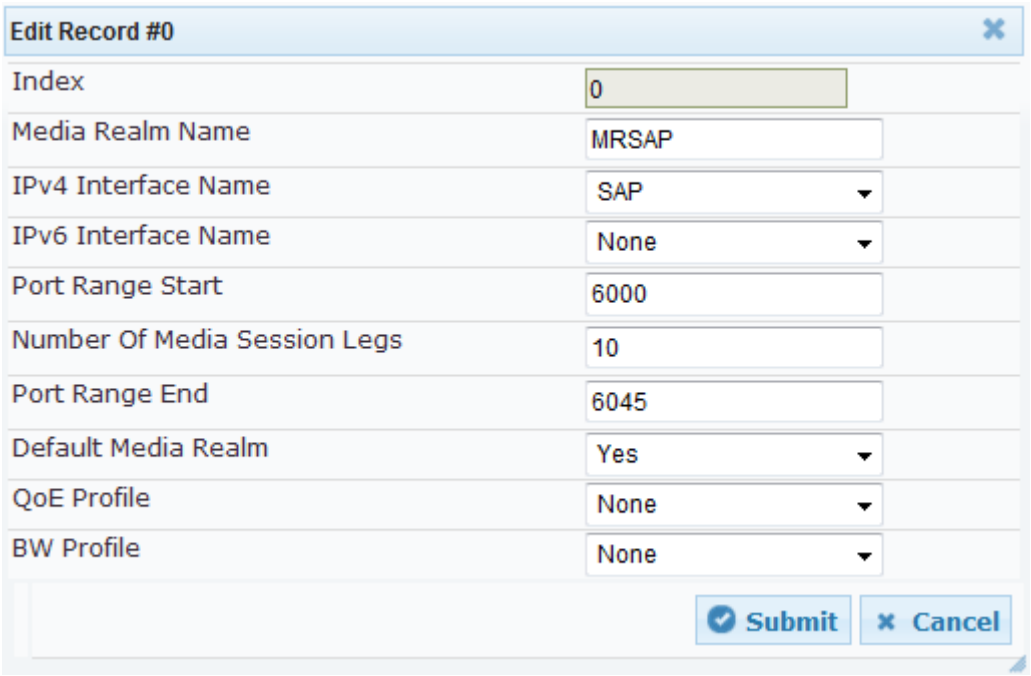
This step shows how to configure Media Realms. The simplest way is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **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	**MRSAP** (descriptive name)
IPv4 Interface Name	**SAP**
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)

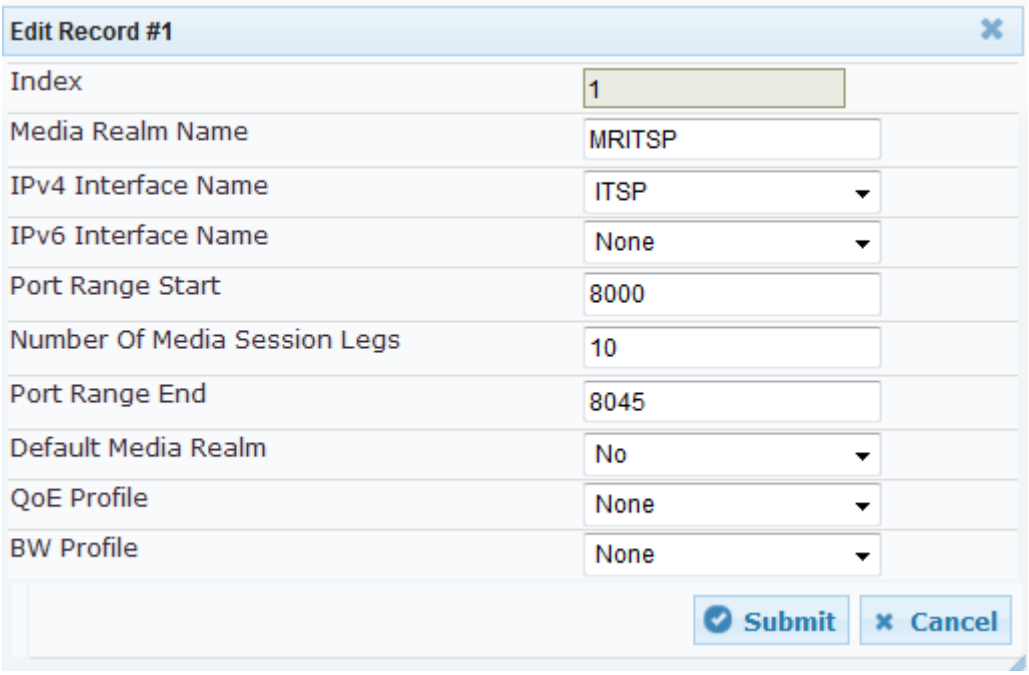
Figure 3-6: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

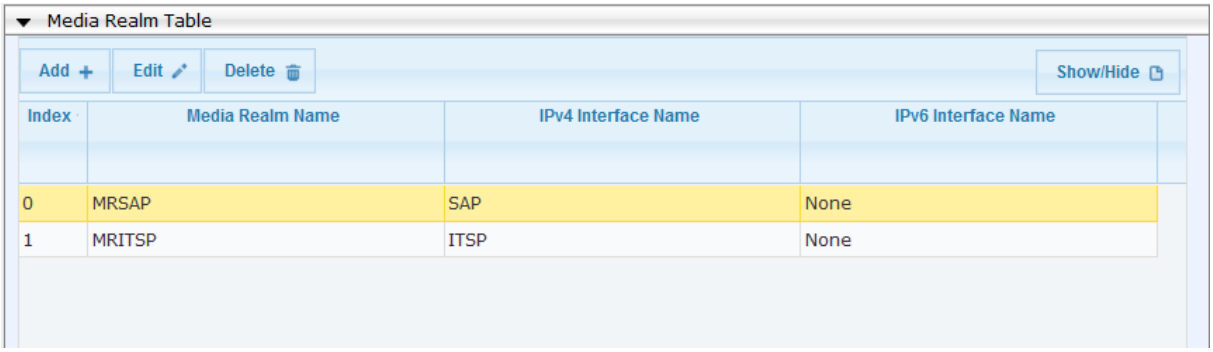
Parameter	Value
Index	**1**
Media Realm Name	**MRITSP** (arbitrary name)
IPv4 Interface Name	**ITSP**
Port Range Start	**8000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**10** (media sessions assigned with port range)

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

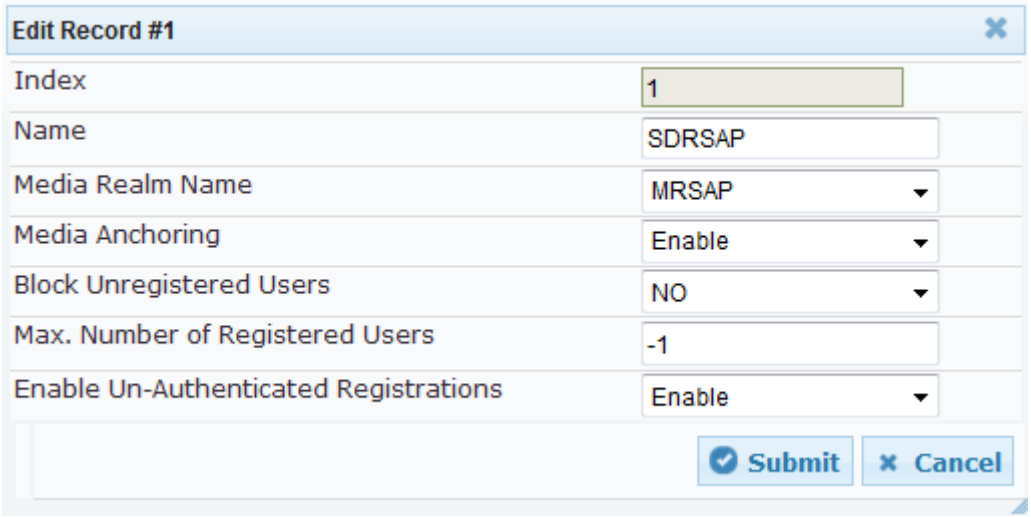
This step shows how to configure SRDs.

➢ **To configure SRDs:**

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

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

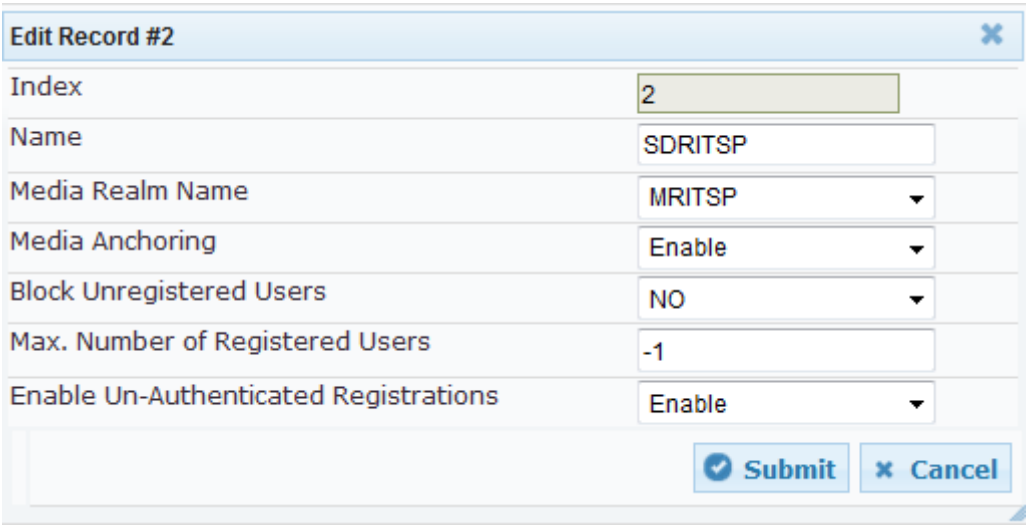
Figure 3-9: Configuring LAN SRD



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

Parameter	Value
SRD Index	**2**
SRD Name	**SRDITSP**
Media Realm	**MRITSP**

Figure 3-10: Configuring WAN SRD



3.3.3 Step 3c: Configure SIP Signaling Interfaces

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

➢ **To configure SIP Interfaces:**

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

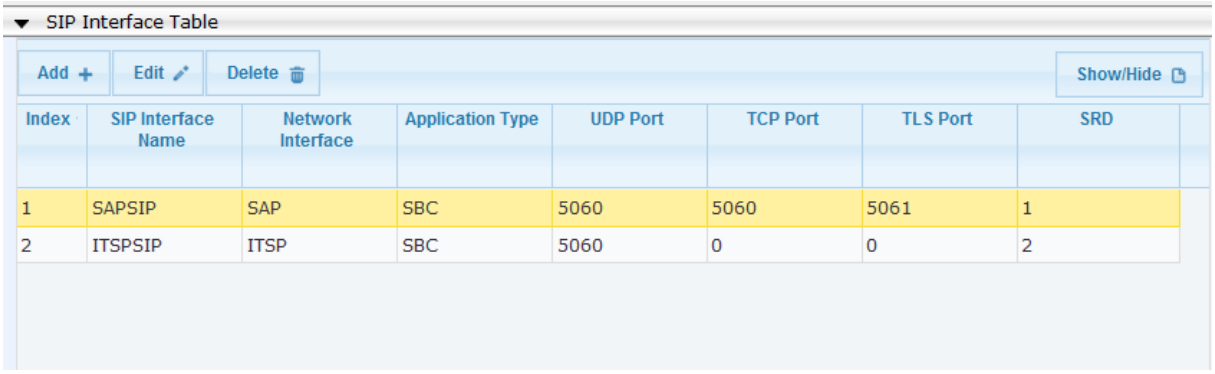
Parameter	Value
Index	**1**
Interface Name	**SAPSIP**(arbitrary descriptive name)
Network Interface	**SAP**
Application Type	**SBC**
TCP and UDP	**5060**
TLS Port	**5061**
SRD	**1**

3. Configure a SIP interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

Figure 3-11: Configured SIP Interfaces in SIP Interface Table



3.4 Step 4: Configure Proxy Sets

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

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

- SAP Contact Center SIP Bridge Server
- Colt SIP Trunk

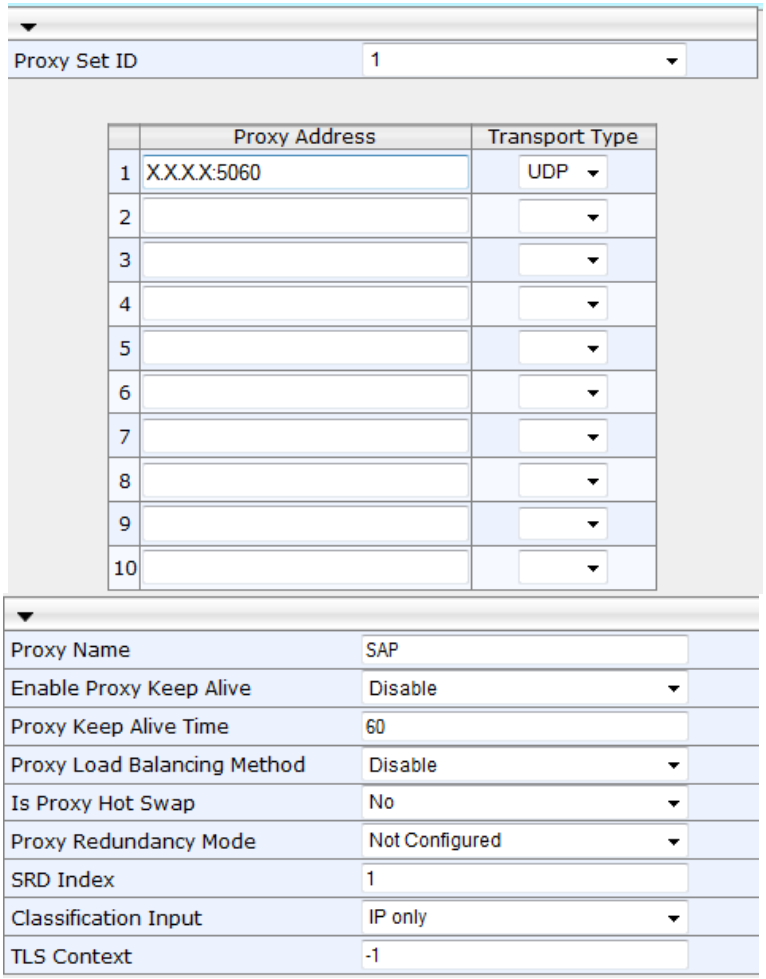
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for SAP Contact Center:

Parameter	Value
Proxy Set ID	**1**
Proxy Address	**X.X.X.X:5060** SAP Contact Center IP address / FQDN and destination port For UDP and TCP, the port is **5060**. If TLS is used, the port must be **5061**.
Transport Type	**UDP, TCP** or **TLS** depend on the configuration of SAP Contact Center Transport Type
Proxy Name	**SAP** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
SRD Index	**1**

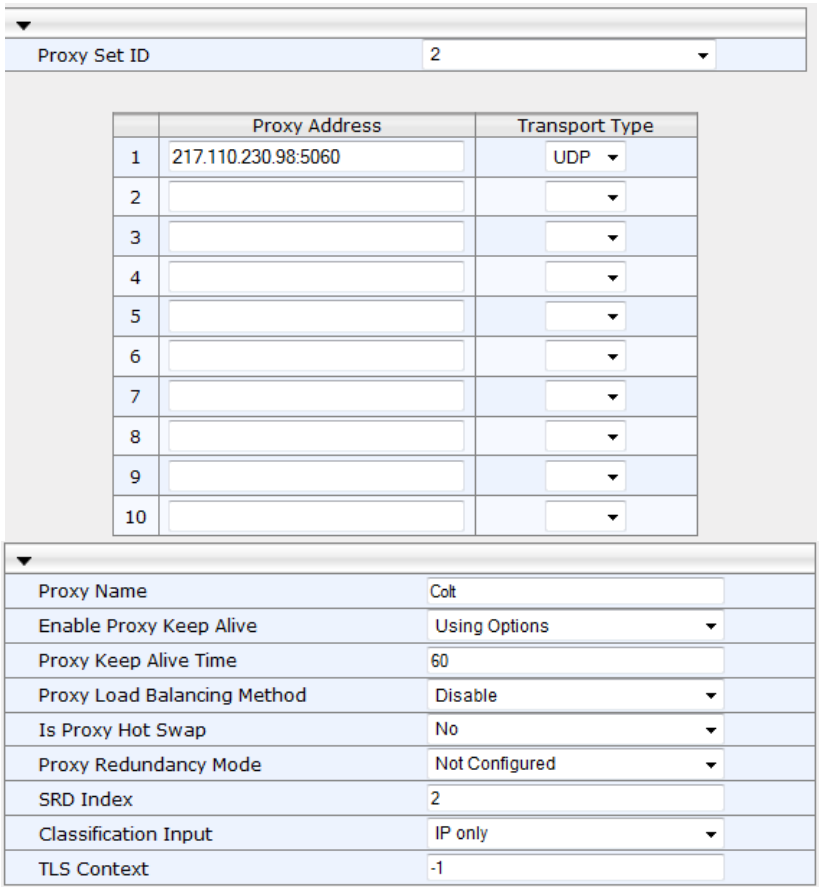
Figure 3-12: Configuring Proxy Set for SAP Contact Center SIP Bridge Server



3. Configure a Proxy Set for the Colt SIP Trunk:

Parameter	Value
Proxy Set ID	**2**
Proxy Address	**217.110.230.98:5060** (Colt IP address / FQDN and destination port)
Transport Type	**UDP**
Proxy Name	**Colt** (arbitrary descriptive name)
Enable Proxy Keep Alive	**Using Options**
SRD Index	**2** (enables classification by Proxy Set for SRD of IP Group belonging to Colt SIP Trunk)

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



3.5 Step 5: Configure IP Groups

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

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

- SAP Contact Center located on LAN
- Colt SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Configure an IP Group for the SAP Contact Center Server:

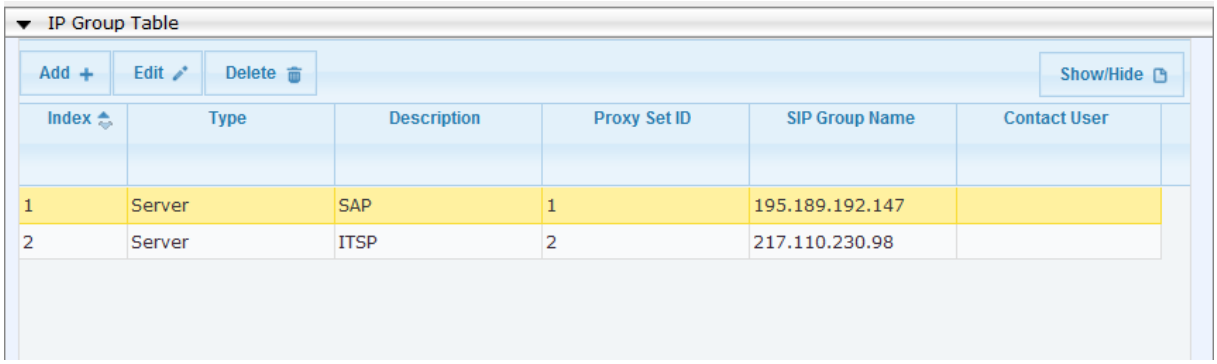
Parameter	Value
Index	**1**
Type	**Server**
Description	**SAP** (arbitrary descriptive name)
Proxy Set ID	**1**
SIP Group Name	**195.189.192.147** (according to ITSP requirement)
SRD	**1**
Media Realm Name	**MRSAP**
IP Profile ID	**1**

3. Configure an IP Group for the Colt SIP Trunk:

Parameter	Value
Index	**2**
Type	**Server**
Description	**ITSP** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**217.110.230.98** (according to ITSP requirement)
SRD	**2**
Media Realm Name	**MRITSP**
IP Profile ID	**2**

The configured IP Groups are shown in the figure below:

Figure 3-14: Configured IP Groups in IP Group Table



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:

- SAP CONTACT CENTER
- Colt SIP trunk

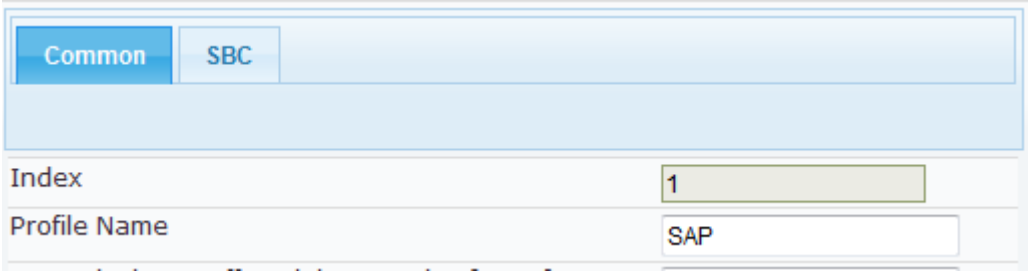
Note: The IP Profiles were assigned to these entities (i.e., IP Groups) in the previous step (see Section 3.5 on page 26).

➢ **To configure IP Profiles:**

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

Parameter	Value
Index	**1**
Profile Name	**SAP** (arbitrary descriptive name)

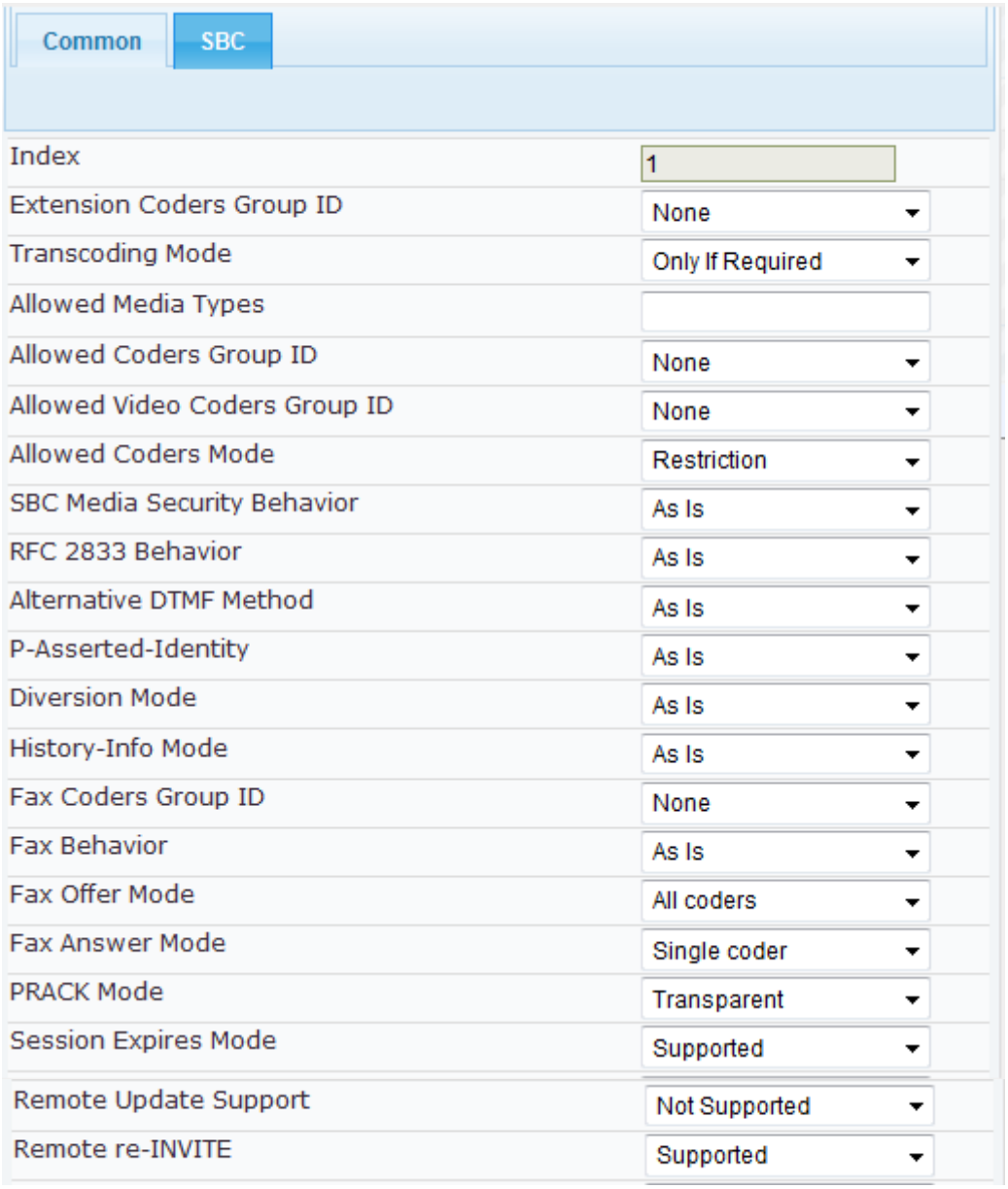
Figure 3-15: Configuring IP Profile for SAP Contact Center – Common Tab



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

Parameter	Value
Media Security Behavior	**'As is'**
Session Expires Mode	**Supported** (To terminate the Session Expires, since Colt do not support Session Expires negotiation)
Remote Update Support	**Not Supported**

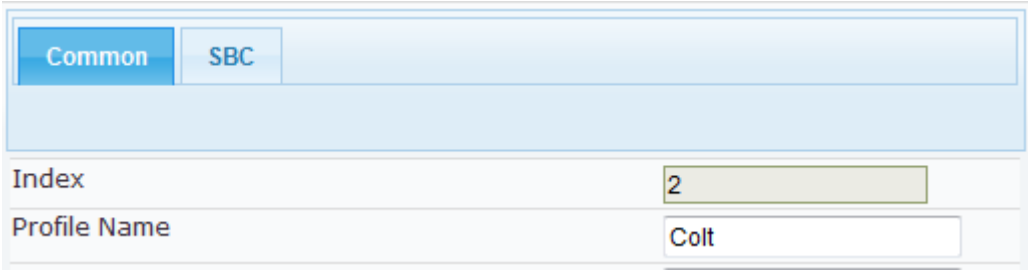
Figure 3-16: Configuring IP Profile for SAP Contact Center – SBC Tab



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

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

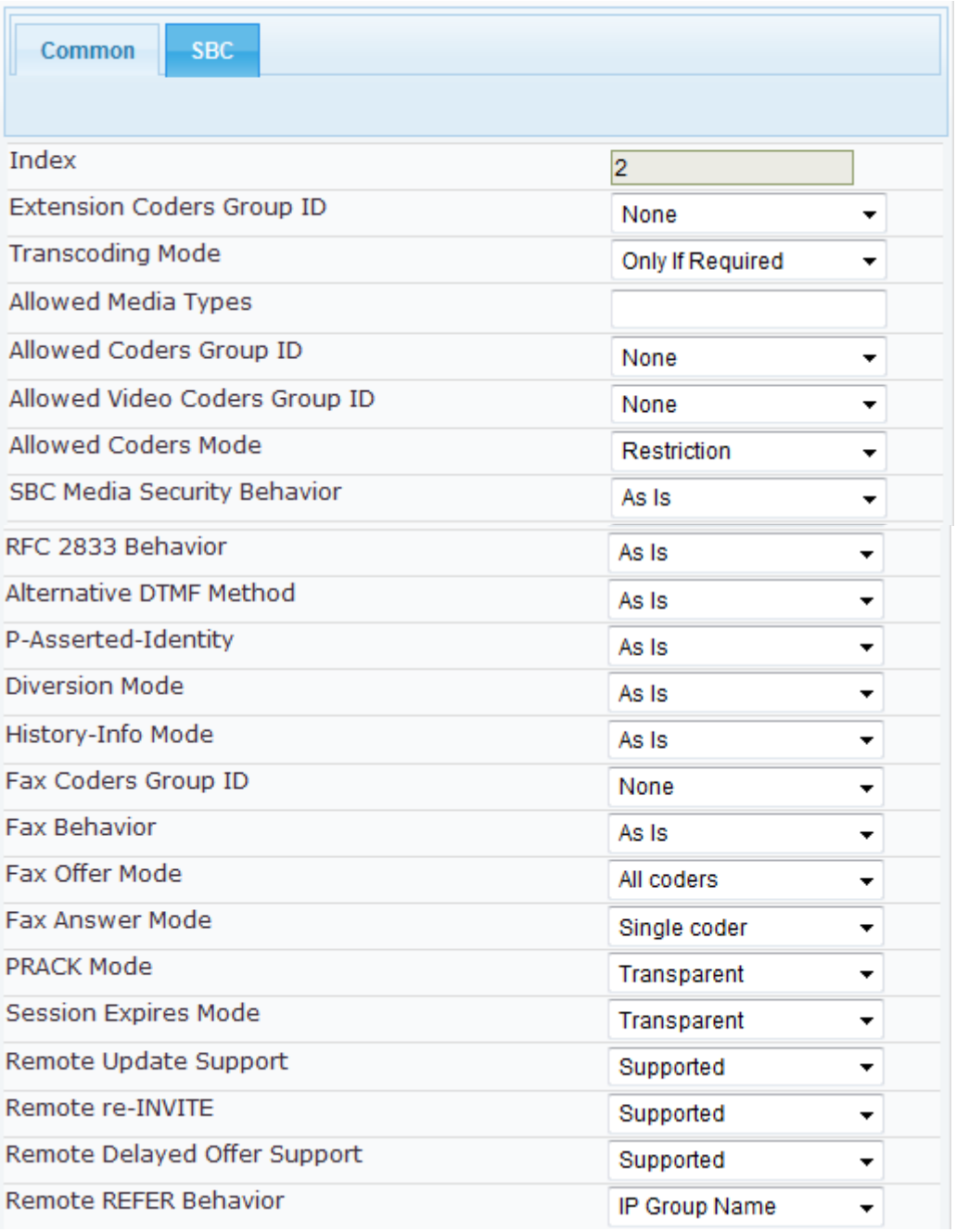
Figure 3-17: Configuring IP Profile for Colt SIP Trunk – Common Tab



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

Parameter	Value
Media Security Behavior	**'As Is'**
Remote REFER Behavior	**IP Group Name** (To change the host name on the Refer-To header, to the ITSP host name)

Figure 3-18: Configuring IP Profile for Colt SIP Trunk – SBC Tab



3.7 Step 7: Configure Coders

The Colt SIP Trunk supports G.729, G.711A-law, and G.726 coders.

The SAP Contact Center supports G.711A-law and G.711U-law and G.729 coders.

Since both entities have common codecs supported, no transcoding is needed; therefore no special SBC configuration is needed either.

However, if support is required in the deployment for G.711U-law or G.726 (not supported on either), an SBC transcoding configuration is needed. See the *SBC User's Manual* for Coder Transcoding configuration.

Note: DSP channels Feature Key and definition is needed for Coder Transcoding.

3.8 Step 8: Configure a SIP TLS Connection

This section shows how to configure the SBC for using a TLS connection with the SAP Contact Center. This is essential for a secure SIP TLS connection.

3.8.1 Step 8a: Configure a Certificate

This step shows how to exchange a certificate with the SAP Contact Center system. The certificate is used by the SBC to authenticate the connection with the SAP Contact Center SIP Server.

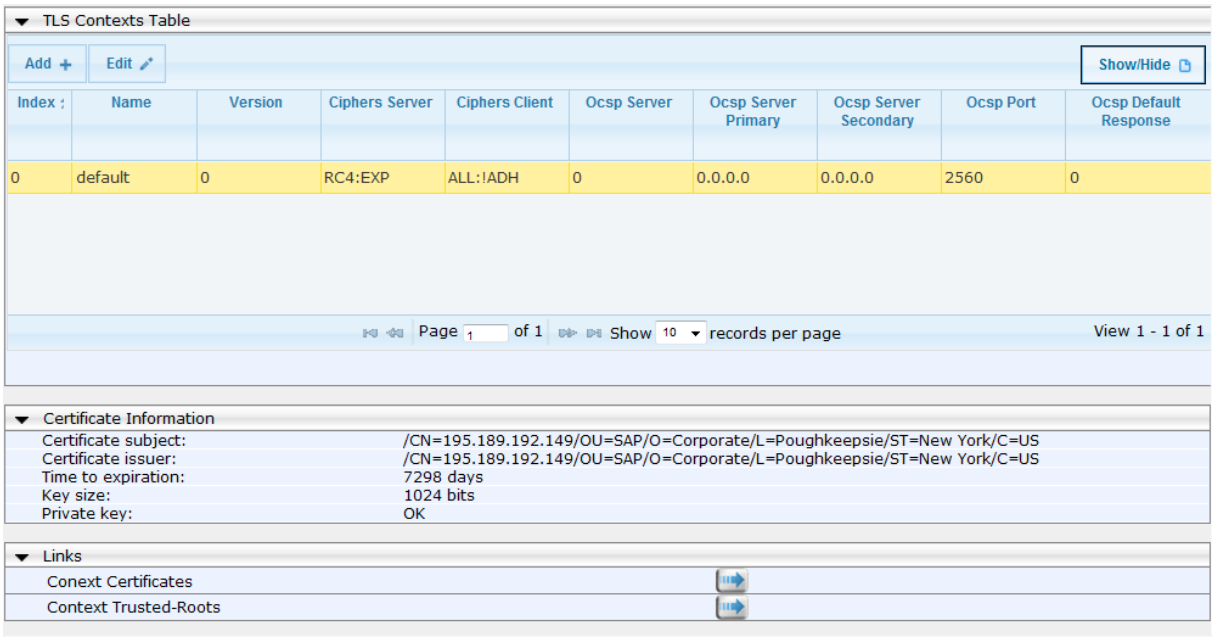
Two main steps:

1. Change the subject name and regenerate a self-signed certificate
2. Deploy a Trusted Root Certificates on the SBC.

➢ **To generate a self-signed certificate:**

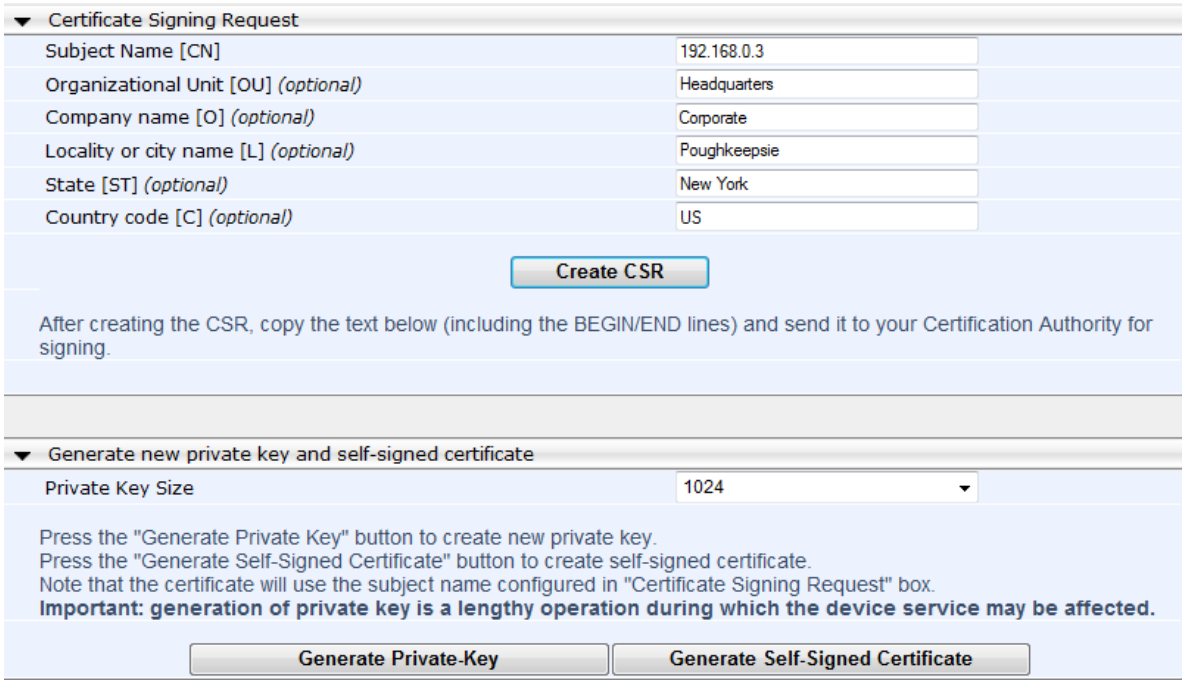
1. Open the Certificates page (**Configuration** tab > **System** > **TLS Contexts Table**).

Figure 3-19: TLS Contexts Page



2. Click on the 'Context Certificates' arrow to open this page:

Figure 3-20: Context Certificates Web Page



3. In the 'Subject Name' field, enter the SBC IP Address as seen by the SAP Contact Center system.
4. Click **Generate Self-Signed Certificate**; a new self-signed certificate is generated.
5. Export the Device Certificate, and send it to SAP Contact Center for loading it to their system as follows:

➢ **To export the self-signed certificate:**

1. Open a Telnet/RS-232 connection to the SBC device.
2. Enter the system configuration layer:

```
Mediant 4000# conf system
```

3. Enter the TLS configuration layer:

```
Mediant 4000(config-system)# tls
```

4. Export the certificate using the **`certificate export`** command:

```
Mediant 4000(tls-0)# certificate export
```

Local certificate:

```
-----BEGIN CERTIFICATE-----
MIICVTCCAb4CAQAwDQYJKoZIhvcNAQEFBQAwczEYMBYGA1UEAxMPMTk1LjE4
OS4xOTIuMTQ5MQwwCgYDVQQLEwNTQVAxEjAQBgNVBAoTCUNvcnBvcmF0ZTE
VMBMGA1UEBxMMUG91Z2hrZWVwc2llMREwDwYDVQQIEwhOZXcgW9yazELMAk
GA1UEBhMCVVMwHhcNMTQwMjI4MTkwMDMyWhcNMzQwMjIzMjEwMDMyWjBzM
RgwFgYDVQQDEw8xOTUuMTg5LjE5Mi4xNDkxDDAKBgNVBAsTA1NBUDESMBAG
A1UEChMJQ29ycG9yYXRlMRUwEwYDVQQHEwxQb3VnaGtlZXBzaWUxETAPBgNV
BAgTCE5ldyBZb3JrMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBj
QAwgYkCgYEAulVh4F6ZE6ud7ouPWtYcgr65cikb1fjAc2vzr/YII8EOzNomLiykWJsWs/
0F1XnCXkQyPt9xPrDt/uTwngUn+UtK09WHdJZlze+1KznXr/fcpjSe20JC7R1az0zxVcv
YpKuSVtZQOnbSFWmXpJmCRptWSer/YA2WX3N6Lm++Zg0CAwEAATANBgkqhkiG
9w0BAQUFAAOBgQANU0SdVYvPvygfUOuidpm9Zud2vUSPo3gavpqAJ6Z4vhX/gRC
YGJPSIrDUWn8H0xbiorylV16SepFiaZ0b8ZAv4q7s2XvkWfkzaSK/jAYPdrAu7Felq31b
FkhZst75OrZ5kNUAW++9OqnTb/bAkUv7Lb5asW8SGV/5Ag2USb8HUw==
-----END CERTIFICATE-----
```

5. Copy the Certificate from the line **"----BEGIN CERTIFICATE" to "END CERTIFICATE REQUEST----**" to a text file (such as Notepad), save it to a folder on your computer, and then send it to SAP Contact Center for loading to their system.

3.8.2 Step 8b: Import Trusted Root Certificate

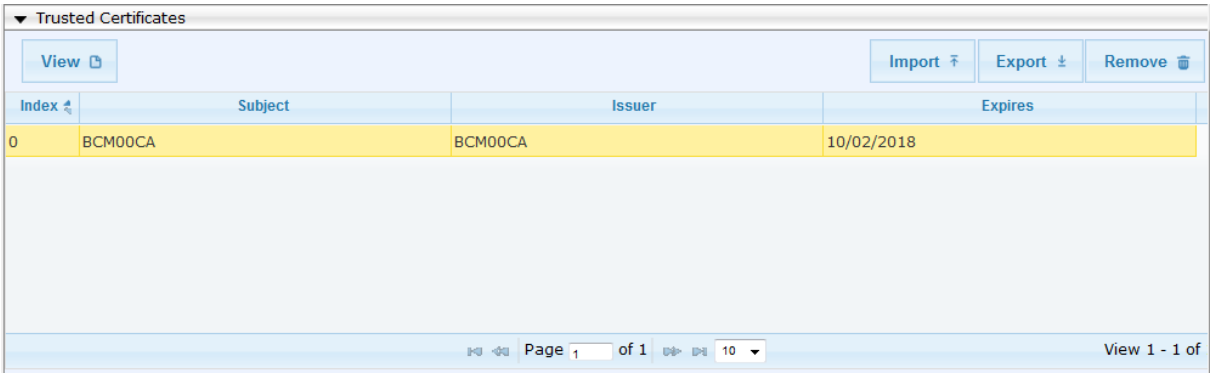
This section shows how to import a trusted root certificate.

➢ **To import a trusted root certificate:**

1. In the SBC's Web interface, return to the TLS Contexts page and then click the **Context Trusted-Roots** button.
2. Import to the device the 'Trusted Root Certificate' that was received from SAP Contact Center CA.

Note: The device supports Base-64 encoded x.509 (.CER) certificate format.

Figure 3-21: Certificates Page (Import Certificate)



3. Reset the SBC with a burn to flash for your settings to take effect (see Section 3.12 on page 48).

3.9 Step 9: Configure IP-to-IP Call Routing Rules

This step shows how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The 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 26, IP Group 1 represents SAP Contact Center, and IP Group 2 represents Colt SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between SAP Contact Center (LAN) and Colt SIP Trunk (WAN):

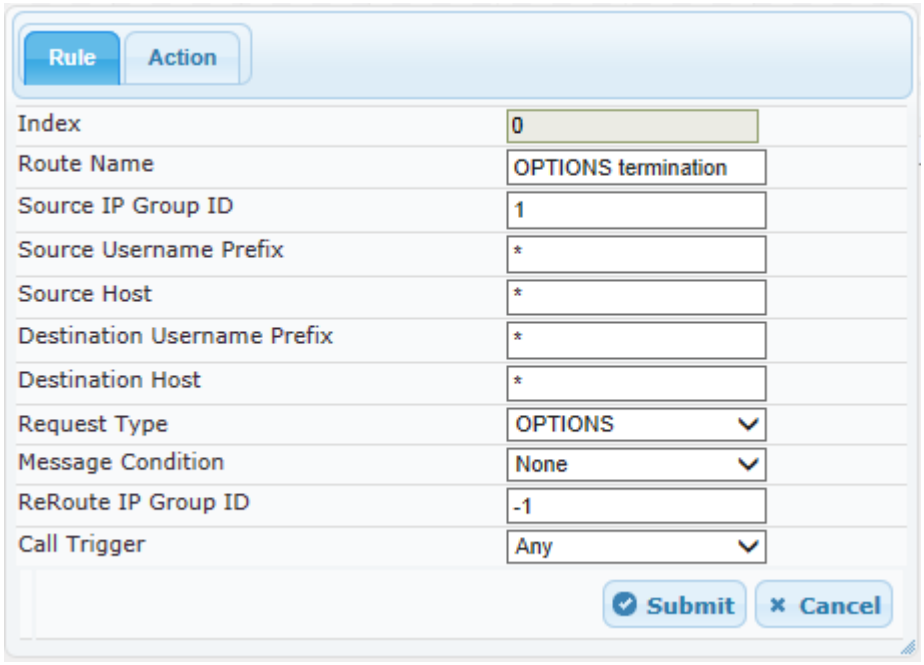
- Terminate SIP OPTIONS messages on the SBC that are received from the LAN
- Calls from SAP Contact Center to Colt SIP Trunk
- Calls from Colt SIP Trunk to SAP Contact Center

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

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

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

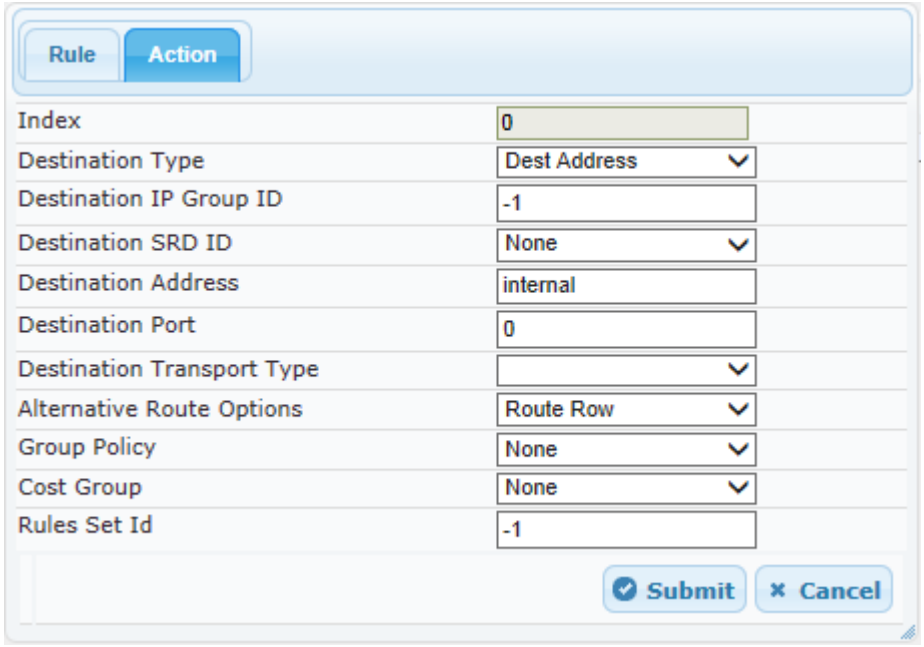
Figure 3-22: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



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

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

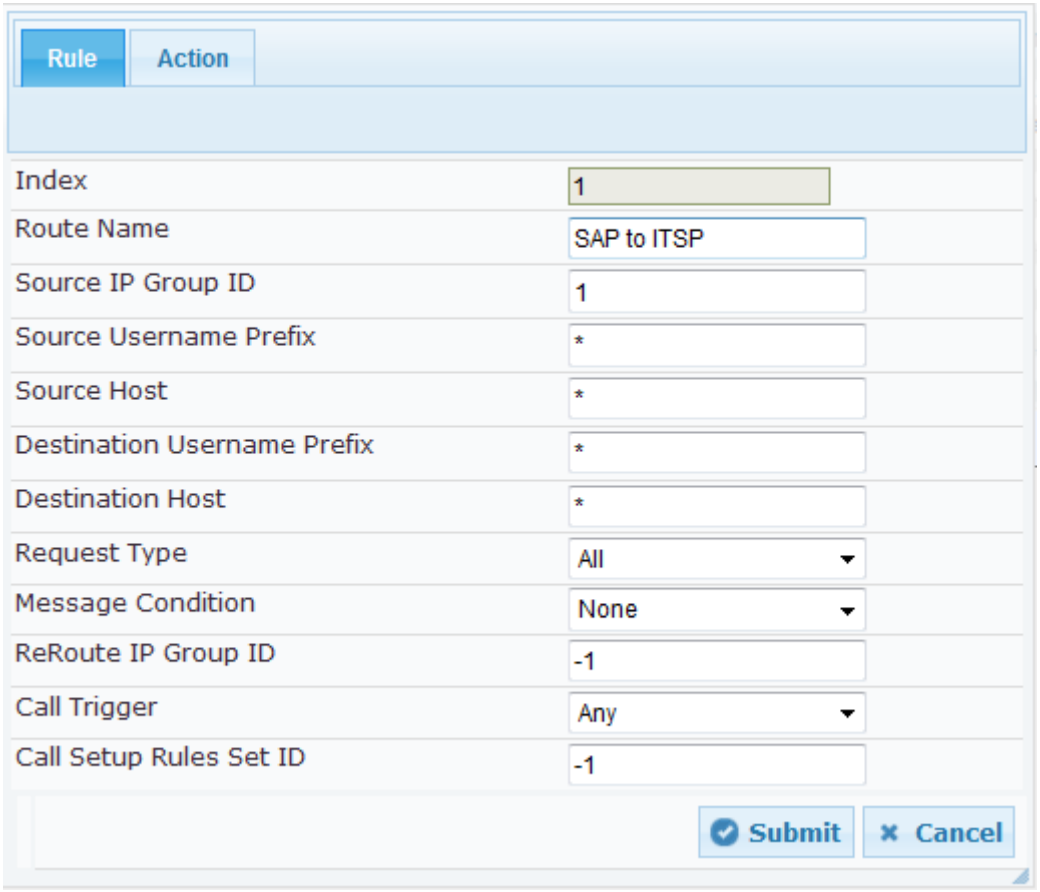
Figure 3-23: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



4. Configure a rule to route calls from SAP Contact Center to Colt SIP Trunk:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

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

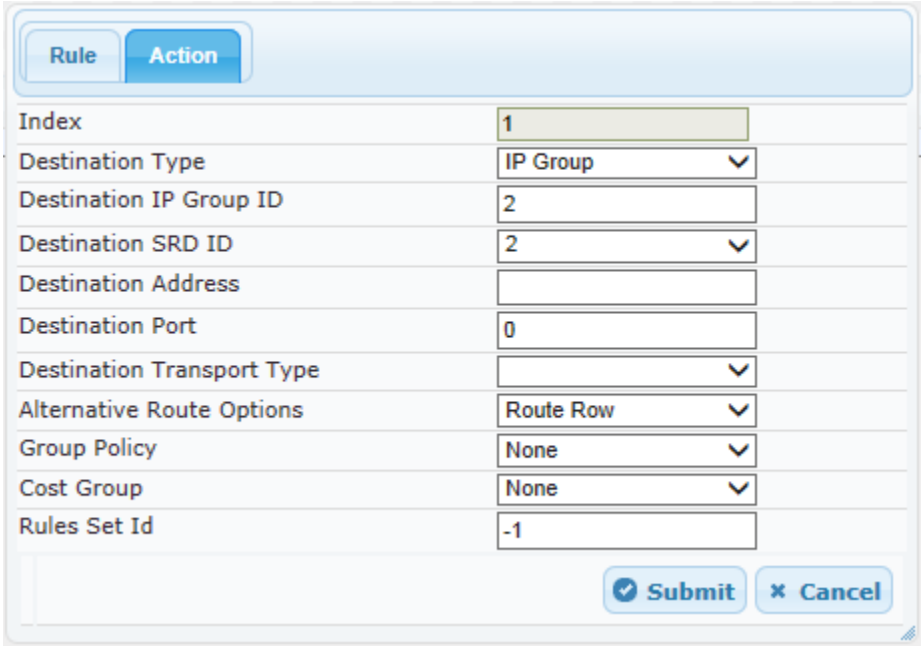
Figure 3-24: Configuring IP-to-IP Routing Rule for SAP to ITSP – Rule tab



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

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

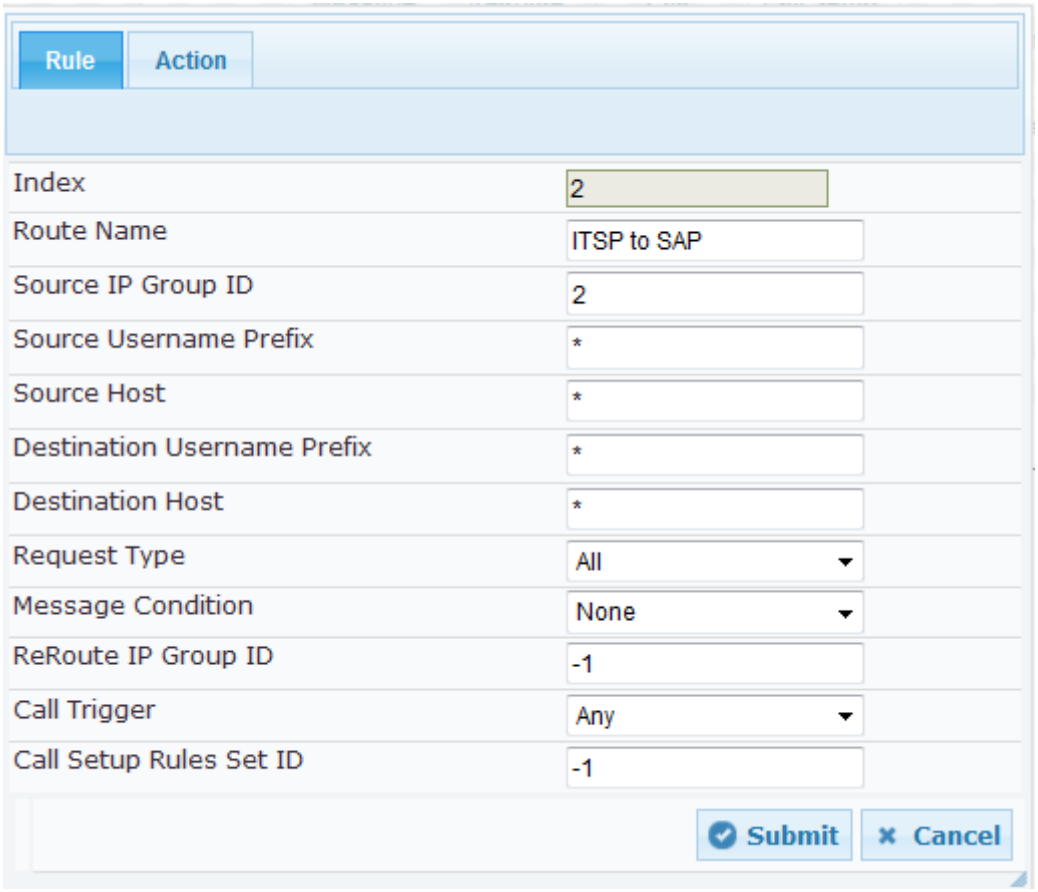
Figure 3-25: Configuring IP-to-IP Routing Rule for SAP to ITSP – Action tab



6. Configure a rule to route calls from Colt SIP Trunk to SAP Contact Center:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

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

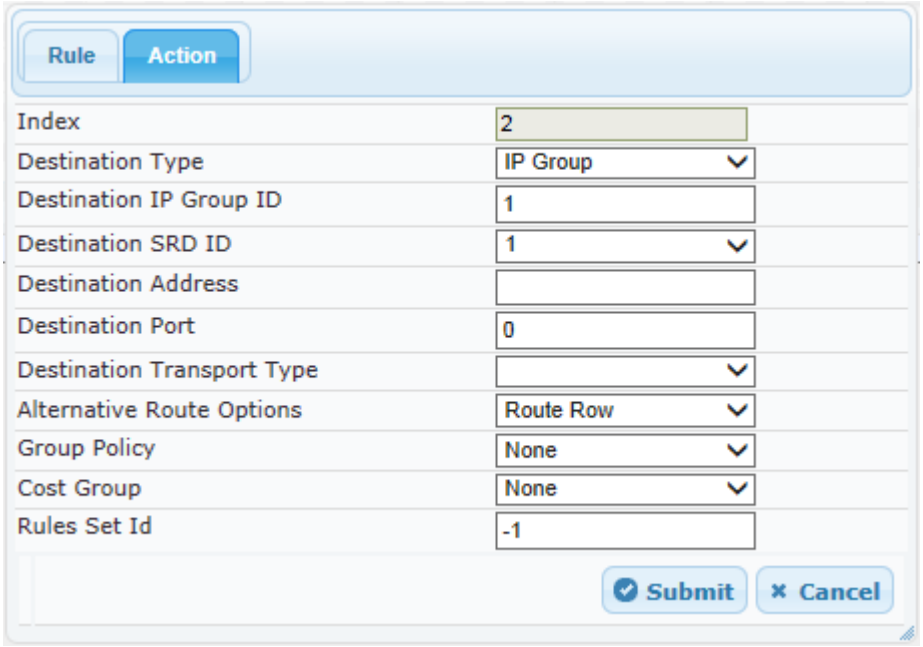
Figure 3-26: Configuring IP-to-IP Routing Rule for ITSP to SAP – Rule tab



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

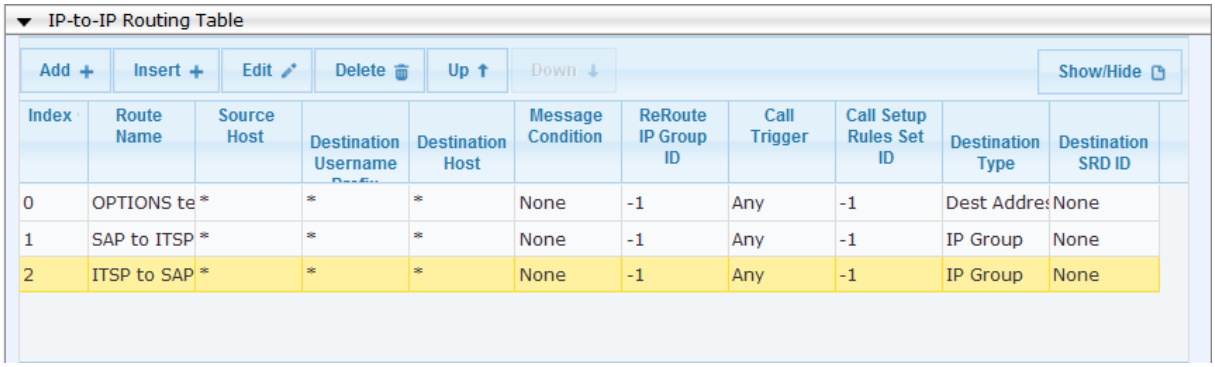
Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 3-27: Configuring IP-to-IP Routing Rule for ITSP to SAP – Action tab



The configured routing rules are shown in the figure below:

Figure 3-28: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



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

3.10 Step 10: Configure IP-to-IP Manipulation Rules

This step shows how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The device supports SIP URI user part (source and destination) manipulations for inbound and outbound routing. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.5 on page 26, IP Group 1 represents SAP Contact Center, and IP Group 2 represents Colt SIP Trunk.

Note: The following manipulation rules are only examples. Adapt the manipulation table according to your environment dial plan.

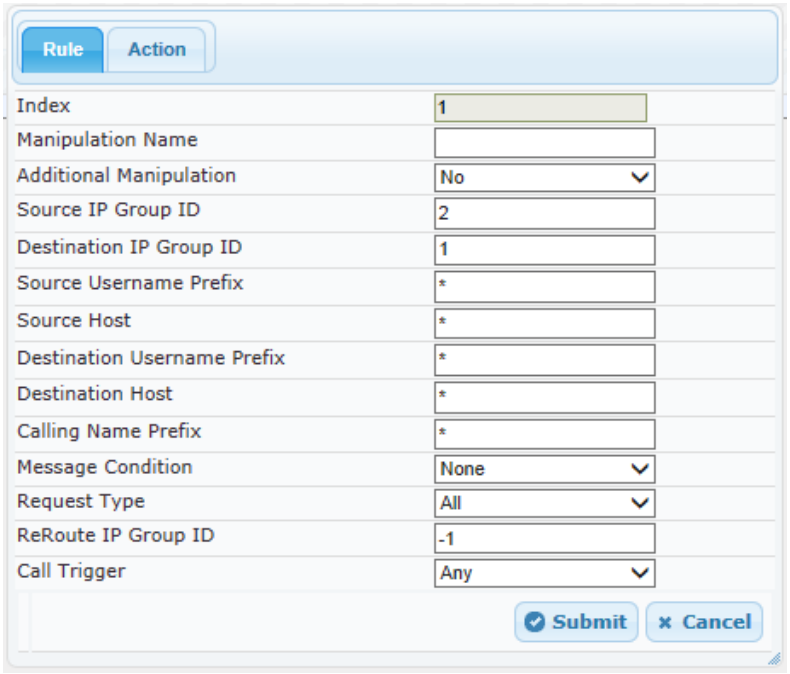
For this interoperability test topology, a manipulation is configured to leave 4 digits from the destination number for calls from IP Group 2 (Colt SIP Trunk) to IP Group 1 (i.e., SAP Contact Center) for any destination username prefix.

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

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

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

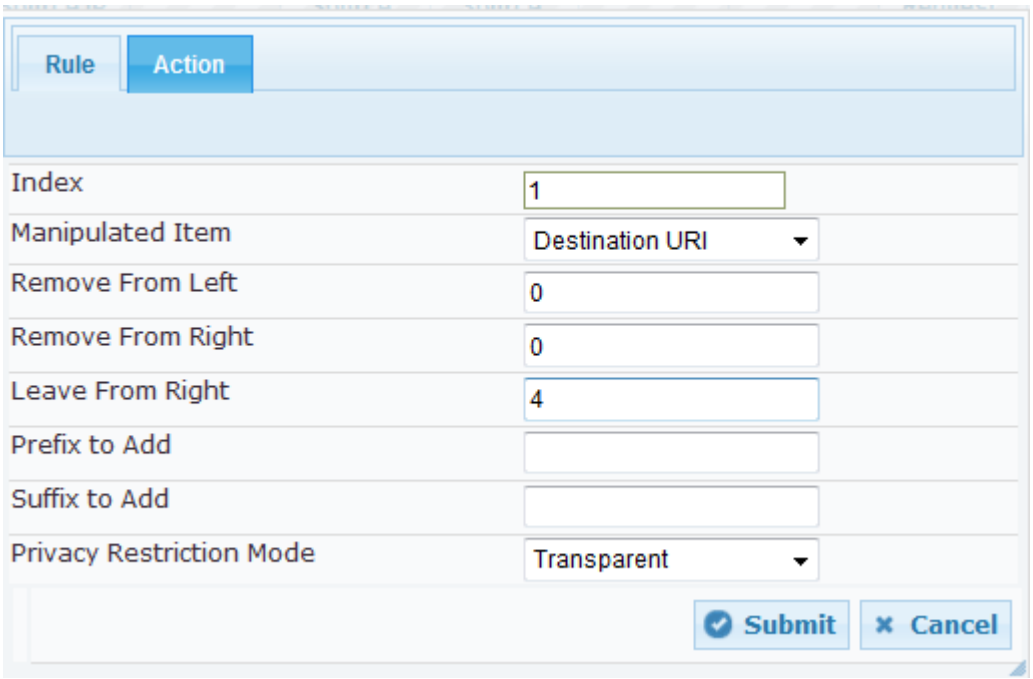
Figure 3-29: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Value
Manipulated Item	**Destination URI**
Leave From Right	**4**

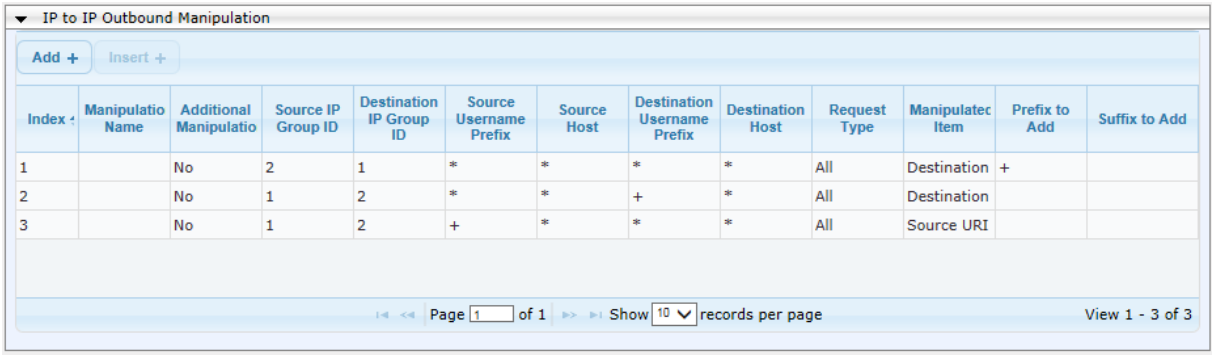
Figure 3-30: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



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., SAP Contact Center) and IP Group 2 (i.e., Colt SIP Trunk):

Figure 3-31: Example of Configured IP-to-IP Outbound Manipulation Rules



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

3.11 Step 11: Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

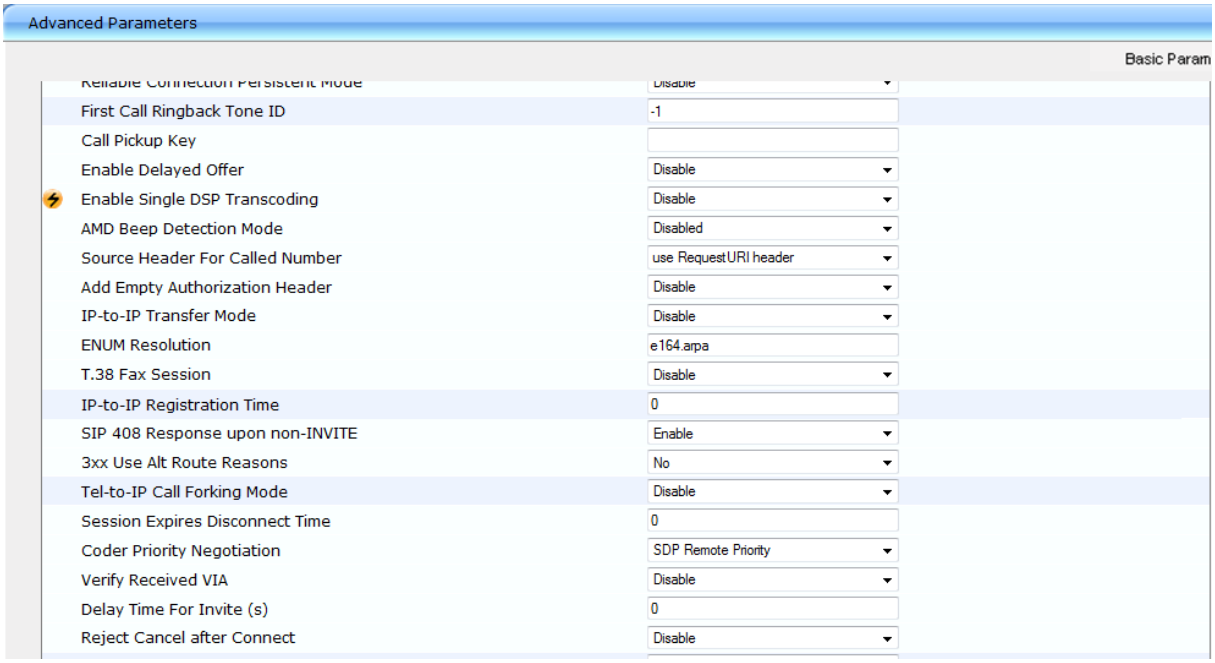
3.11.1 Step 11a: Configure Session Expires Disconnect Time

Session Expires Disconnect Time defines a session expiry timeout. The device disconnects the session (sends a SIP BYE) if the refresher did not send a refresh request before one-third (1/3) of the session expiry timeout, or before the time configured by this parameter (the minimum of the two).

➢ **To configure the Session Expires Disconnect Time:**

1. Open the **Advanced Parameters** page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).

Figure 3-32: Configuring Session Expires Disconnect Time



2. Configure the 'Session Expires Disconnect Time' parameter value to 0.

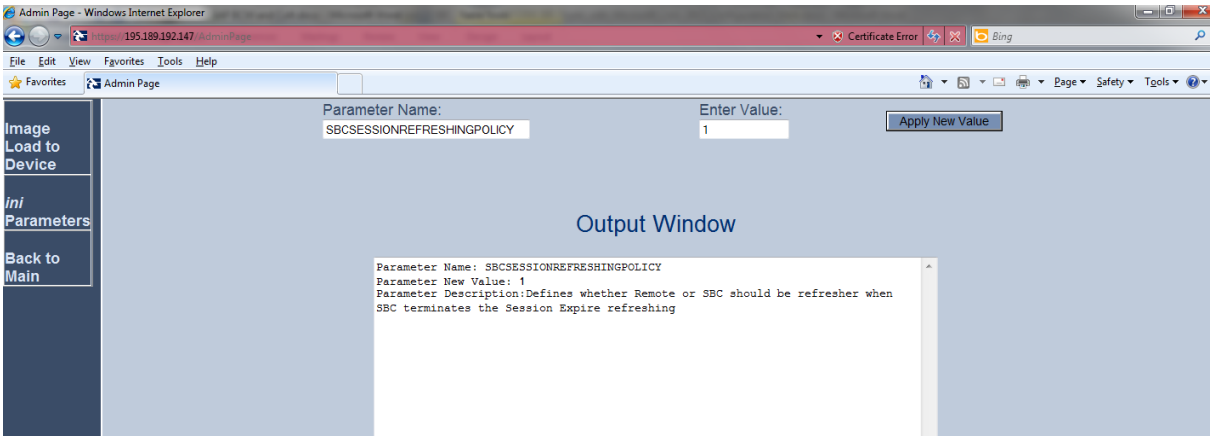
3.11.2 Step 11b: Configure Session Refresher Policy

The following parameter defines whether Remote or SBC will be the refresher when the SBC terminates the Session Expire refreshing. In this example, the refresher must be the SBC.

➢ **To configure the Session Refresher parameter:**

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

Figure 3-33: Configuring SBC Session Refreshing Policy



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

Parameter	Value
SBCSessionRefreshingPolicy	**1** (This enables SBC to be the refresher in the session expire refresh)

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

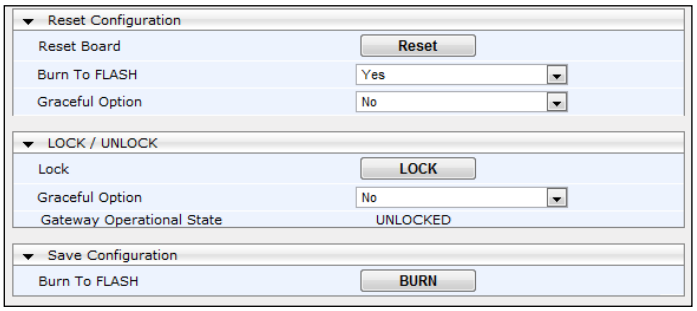
3.12 Step 12: Reset the SBC

After finishing configuring the SBC as shown in this section, save ("burn") the configuration to the 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 3-34: Resetting the SBC



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

A AudioCodes *ini* File

This appendix shows the *ini* configuration file of the SBC, corresponding to the Web-based configuration described in Section 3 on page 13.

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

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

;Board: Mediant 4000
;Board Type: 70
;Serial Number: 4773101
;Slot Number: 1
;Software Version: 6.80A.218.002
;DSP Software Version: 5039AE3_R => 680.22
;Board IP Address: 195.189.192.147
;Board Subnet Mask: 255.255.255.128
;Board Default Gateway: 195.189.192.129
;Ram size: 2048M Flash size: 252M
;Num of DSP Cores: 24 Num DSP Channels: 30
;Num of physical LAN ports: 8
;Profile: NONE
;Key features:;Board Type: Mediant 4000 ;DATA features: ;DSP Voice
features: IpmDetector ;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 ;Channel Type: DspCh=30 ;HA ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Control Protocols:
MSFT CLI EMS SBC-SIGNALING=1416 MGCP SIP TPNCP SBC=4000 ;Default
features:;Coders: G711 G726;

;------ Mediant 4000 HW components------
;
; Slot # : LAN Ports : DSP's # : Module type
;---------------------------------------------
;1 |0 |0 |Empty |
;2 |0 |0 |Empty |
;3 & 4 |1 - 8 |4 |CSM |
;5 |0 |0 |Empty |
;6 |0 |0 |Empty |
;7 |0 |0 |Empty |
;8 |0 |0 |Empty |


;MAC Addresses in use:
;---------------------------
;GROUP_1 - 00:90:8f:48:d4:f0
;GROUP_2 - 00:90:8f:48:d4:f0
;GROUP_3 - 00:90:8f:48:d4:ee
;GROUP_4 - 00:90:8f:48:d4:ee
;---------------------------------------------
```

```
[SYSTEM Params]



;ISPRACKREQUIRED is hidden but has non-default value
USEGATEWAYNAMEFOROPTIONS = 2
ENABLESBCAPPLICATION = 1
SESSIONEXPIRESDISCONNECTTIME = 0
SBCSESSIONREFRESHINGPOLICY = 1

[IPsec Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 1, 4, "LAN Port#1", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 1, 4, "LAN Port#2", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_3", 1, 2, 4, "WAN Port#1", "GROUP_2", "Active";
PhysicalPortsTable 3 = "GE_4", 1, 2, 4, "WAN Port#2", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "GE_5", 1, 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "GE_6", 1, 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "GE_7", 1, 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "GE_8", 1, 1, 4, "User Port #7", "GROUP_4",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode,
EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_1", "GE_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_3", "GE_4";
EtherGroupTable 2 = "GROUP_3", 2, "GE_5", "GE_6";
EtherGroupTable 3 = "GROUP_4", 2, "GE_7", "GE_8";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "", "";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 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, 195.189.192.147, 25, 195.189.192.129, 2, "ITSP",
80.179.52.100, 80.179.55.100, "vlan 2";
InterfaceTable 1 = 5, 10, 192.168.0.3, 24, 192.168.0.1, 1, "SAP", 0.0.0.0,
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 = "MRSAP", "SAP", "", 6000, 10, 6045, 1, "", "";
CpMediaRealm 1 = "MRITSP", "ITSP", "", 8000, 10, 8045, 0, "", "";

[ \CpMediaRealm ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SDRSAP", "MRSAP", 0, 0, -1, 1;
SRD 2 = "SDRITSP", "MRITSP", 0, 0, -1, 1;

[ \SRD ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "x.x.x.x:5060", 0, 1;
```

```
ProxyIp 1 = "217.110.230.98:5060", 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 = "SAP", 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, 0, 0, 0,
0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 3, 0, 2, 1, 0, 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, 0, 0, 0,
300;
IpProfile 2 = "Colt", 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, 0, 0, 0,
0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 2, 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, 0, 0, 0,
300;

[ \IpProfile ]
```

```
[ ProxySet ]

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

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_RoutingMode,
IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet,
IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet,
IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile, IPGroup_BWProfile,
IPGroup_MediaEnhancementProfile, IPGroup_AlwaysUseSourceAddr,
IPGroup_MsgManUserDef1, IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "SAP", 1, "195.189.192.147", "", 0, -1, -1, 0, -1, 1,
"MRSAP", 1, 1, -1, -1, 0, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "",
"", "", 0, "", "";
IPGroup 2 = 0, "ITSP", 2, "217.110.230.98", "", 0, -1, -1, 0, -1, 2,
"MRITSP", 1, 2, -1, -1, -1, 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 = "SAP to ITSP ", 1, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 2, "", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "ITSP to SAP ", 2, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 1, "", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]
[ TLSContexts ]
```

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

[ \TLSContexts ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType;
SIPInterface 1 = "SAPSIP", "SAP", 2, 5060, 5060, 5061, 1, "", "", -1, 0,
500;
SIPInterface 2 = "ITSPSIP", "ITSP", 2, 5060, 0, 0, 2, "", "", -1, 0, 500;

[ \SIPInterface ]


[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]


[ ResourcePriorityNetworkDomains ]

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

[ \ResourcePriorityNetworkDomains ]
```

Reader's Notes

AudioCodes

Configuration Note

www.audiocodes.com