Enterprise Session Border Controllers (E-SBC)

AudioCodes Mediant[™] Series

Interoperability Lab

Configuration Note

Microsoft[®] Lync[™] Server 2013 & Time Warner Cable Business Class SIP Trunk using Mediant E-SBC



Microsoft Partner







Version 6.8

February 2015

Document # LTRT-12370

Table of Contents

1	Introduction			
	1.1	Intended Audience	7	
	1.2	About AudioCodes E-SBC Product Series	7	
2	Component Information			
	2.1	AudioCodes E-SBC Version	9	
	2.2	TWCBC SIP Trunking Version		
	2.3	Microsoft Lync Server 2013 Version	9	
	2.4	Interoperability Test Topology		
		2.4.1 Environment Setup		
		2.4.2 Known Limitations		
3	Con	figuring Lync Server 2013	13	
	3.1	Configuring the E-SBC as an IP / PSTN Gateway	.13	
	3.2	Configuring the "Route" on Lync Server 2013	.21	
4	Con	figuring AudioCodes E-SBC	29	
	4.1	Step 1: IP Network Interfaces Configuration	.30	
		4.1.1 Step 1a: Configure VLANs		
		4.1.2 Step 1b: Configure Network Interfaces	.32	
		4.1.3 Step 1c: Configure the Native VLAN ID		
	4.2	Step 2: Enable the SBC Application		
	4.3	Step 3: Signaling Routing Domains Configuration		
		4.3.1 Step 3a: Configure Media Realms4.3.2 Step 3b: Configure SRDs		
		4.3.3 Step 3c: Configure SIP Signaling Interfaces		
	4.4	Step 4: Configure Proxy Sets		
	4.5	Step 5: Configure IP Groups	.43	
	4.6	Step 6: Configure IP Profiles	.45	
	4.7	Step 7: Configure Coders	.50	
	4.8	Step 8: SIP TLS Connection Configuration	.53	
		4.8.1 Step 8a: Configure the NTP Server Address		
	4.0	4.8.2 Step 8b: Configure a Certificate		
	4.9 4.10	Step 9: Configure SRTP		
	4.10	Step 11: Configure IP-to-IP Call Routing Rules		
		Step 12: Configure IP-to-IP Manipulation Rules		
		Step 13: Configure Message Manipulation Rules		
		Step 14: Configure Registration Accounts		
		Step 15: Miscellaneous Configuration		
		4.15.1 Step 15a: Configure Call Forking Mode		
		4.15.2 Step 15b: Configure SBC Session Refreshing Policy	.73	
		4.15.3 Step 15c: Loading Prerecorded Ring-Back Tone File	.74	
	4.16	Step 16: Reset the E-SBC	.75	
Α	Aud	ioCodes INI File	77	



This page is intentionally left blank.

Notice

This document describes how to connect the Microsoft Lync Server 2013 and Time Warner Cable Business Class (TWCBC) 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.

© Copyright 2015 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: February-19-2015

Trademarks

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

WEEE EU Directive

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

Customer Support

Customer technical support and 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 <u>www.audiocodes.com/support</u>.

Document Revision Record

LTRT	Description	
12370	Initial document release for Version 6.8.	

Documentation Feedback

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



This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between Time Warner Cable Business Class (TWCBC) SIP Trunk and Microsoft's Lync Server 2013 environment.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and TWCBC Partners who are responsible for installing and configuring TWCBC's SIP Trunk and Microsoft's Lync Server 2013 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.258.005
Protocol	SIP/UDP (to the TWCBC SIP Trunk)SIP/TCP or TLS (to the Lync FE Server)
Additional Notes	None

2.2 **TWCBC SIP Trunking Version**

Table 2-2: TWCBC Version

Vendor/Service Provider	TWCBC
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	

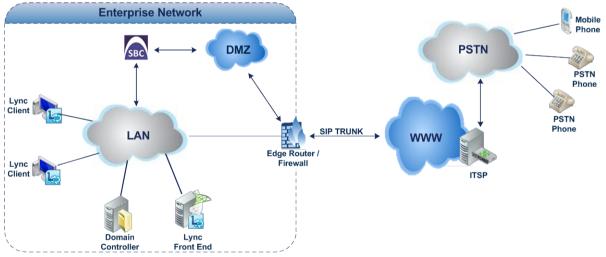
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and TWCBC SIP Trunk with Lync 2013 was done using the following topology setup:

- Enterprise deployed with Microsoft Lync Server 2013 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 TWCBC'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 Lync Server 2013 network in the Enterprise LAN and TWCBC's SIP Trunk located in the public network.

The figure below illustrates this 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	 Microsoft Lync Server 2013 environment is located on the Enterprise's LAN TWCBC SIP Trunk is located on the WAN
Signaling Transcoding	 Microsoft Lync Server 2013 operates with SIP-over-TLS transport type TWCBC SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	 Microsoft Lync Server 2013 supports G.711A-law and G.711U-law coders TWCBC SIP Trunk supports G.711U-law coder only
Media Transcoding	 Microsoft Lync Server 2013 operates with SRTP media type TWCBC SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Microsoft Lync Server 2013 and TWCBC's SIP Trunk.



This page is intentionally left blank.

3 Configuring Lync Server 2013

This chapter describes how to configure Microsoft Lync Server 2013 to operate with AudioCodes E-SBC.



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

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

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

- > To configure E-SBC as IP/PSTN Gateway and associate it with Mediation Server:
- On the server where the Topology Builder is installed, start the Lync Server 2013 Topology Builder (Windows Start menu > All Programs > Lync Server Topology Builder), as shown below:



Figure 3-1: Starting the Lync Server Topology Builder

AudioCodes

The following is displayed:

Figure 3-2: Topology Builder Dialog Box

🛃 Topology Builder 🛛 🔀
Welcome to Topology Builder. Select the source of the Lync Server 2010 (RC) topology document.
Download Topology from existing deployment. Retrieve a copy of the current topology from the Central Management Store database and save it as a local file. Use this option if you are editing an existing deployment.
Open Topology from a local file Open an existing Topology Builder file. Use this option if you have work in progress or if you have exported a topology from Planning Tool.
New Topology Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.
OK Cancel

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

Figure 3-3: Save Topology Dialog Box

🄀 Save Topology As			×
Administr	rator 👻 Documents	👻 🛃 Search	
🕘 Organize 👻 📗 Views	👻 📑 New Folder		0
Favorite Links Image: Desktop Computer Documents Pictures Music Recently Changed Searches Public	Name A	▼ Date modified ▼ Type 10/7/2010 5:53 PM TBXML File 10/12/2010 10:5 TBXML File	▼ Size ▼ Tag 101 KB 101 KB
	op2.tbxml ogy Builder files (*.tbxml)		×
Hide Folders		Save	Cancel

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

The Topology Builder screen with the downloaded Topology is displayed:

Figure 3-4: Downloaded Topology

Server 2013, Topology Builder						
<u>File Action H</u> elp						
Evic Server AudioCodes	SIP domain					
Lync Server 2010 Lync Server 2013 Standard Edition Front End Servers Enterprise Edition Front End pools Mediation pools Persistent Chat pools Edide pools	Default SIP domain: Additional supported SIP domains:	iLync15.local Not configured				
Trusted application servers	Simple URLs					
	Phone access URLs: Meeting URLs: Administrative access URL:	Active Simple URL Image: state of the stat	SIP domain iLync15.local			
	Central Management Serve	er				
	Central Management Server:	Active Front End	Site AudioCodes			

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

Figure 3-5: Choosing New IP/PSTN Gateway

KLync Server 2013, Topology Builder					
Ele Action Help					
🖃 🛃 Lync Server	The properties for this item are not available for editing.				
🖃 🔃 AudioCodes					
🕀 🚞 Lync Server 2010					
🖃 🚞 Lync Server 2013					
🕀 🛅 Standard Edition Front End Servers					
Enterprise Edition Front End pools					
Director pools					
🕀 🚞 Mediation pools					
Persistent Chat pools					
🚞 Edge pools					
Trusted application servers					
🖃 🚞 Shared Components					
🕀 🚞 SQL Server stores					
🕀 🚞 File stores					
PSTN gateway New IP/PSTN Gateway	V				
GW1.iLvn					
colt.ilync1 Tepefine a new IP/PS	TN gateway.				
Trunks Office Web Ar Help					
🕀 🚞 Branch sites					



The following is displayed:

Figure 3-6: Define the PSTN Gateway FQDN

🌄 Define N	iew IP/PSTN Gateway				×
5	Define the PSTN Gat	eway FQDN			
Define th	e fully qualified domain name (FQD	N) for the PSTN gate	eway.		
FQDN:*					
ITSP-GV	V.ilync15.local				
Help			<u>B</u> ack	Next	Cancel

Enter the Fully Qualified Domain Name (FQDN) of the E-SBC (e.g., ITSP-GW.ilync15.local). Update this FQDN in the relevant DNS record, and then click Next; the following is displayed:



🄀 Define New IP	/PSTN Gateway		×
See De	fine the IP address		
Enable IPv4)
Use all of	onfigured IP addresses.		
⊂ <u>L</u> imit se	vice usage to selected IP addresses.		
PSTN <u>I</u> P	address:		
C Enable IPv <u>6</u>			
	onfigured IP addresses.		
C Limit se	vice usage to selected IP addresses.		
PSTN <u>I</u> P	address:		
Help		<u>B</u> ack <u>N</u> ex	ct Cancel

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

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

Notes:

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

Figure 3-8: Define the Root Trunk

😓 Define New IP/PSTN Gateway	×
Define the root trunk	
Irunk name: *	
ITSP-GW.ilync15.local	
Listening port for IP/PSTN gateway: *	
5067	
SIP Transport Protocol:	
TLS	•
Associated Mediation Server:	
FE15.ilync15.local AudioCodes	▼
Associated Mediation Server port: *	
5067	
Help	Back Finish Cancel

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



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

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

le Action Help		
In Server AudioCodes	Trunk	
 Address Address Lync Server 2010 Lync Server 2013 Standard Edition Front End Servers Enterprise Edition Front End pools Director pools Mediation pools Persistent Chat pools Edge pools Trusted application servers Shared Components SQL Server stores File stores File stores GW1.Lync15.local Trunks Gotting Colligned Servers Trunks Gotting Colligned Servers Trunks Gotting Colligned Servers Trunks Gotting Colligned Servers Server Servers Trunks Gotting Colligned Servers Trunks Gotting Colligned Servers Server Servers 	Trunk name: PSTN gateway: Listening port: SIP Transport Protocol: Mediation Server: Mediation Server port:	ITSP-GW.ilync15.local ITSP-GW.ilync15.local (AudioCodes) 5067 TLS FE15.ilync15.local (AudioCodes) 5067

8. Publish the Topology: In the main tree, select the root node Lync Server, and then from the Action menu, choose Publish Topology, as shown below:



i o r	ync Server 2013, Topology Bullder					
File	Action Help					
	New Central Site					
	Edit Properties		main			
	New Topology					
	Open Topology		ult SIP domain:	iLync15	i.local	
	Download Topology		tional supported SIP	Not cor	nfigured	
			ains:		-	
	Save a copy of Topology As					
	Publish Topology					
	Install Database			1		
	Merge Office Communications Server 2007 R2 Top	ology[Pub	lish topology to the Centra	al Manag	ement store.	
	Remove Deployment					
	Help		e access URLs:	Active	Simple URL	
	File stores		,	7	https://dialin.iLync15.local	
	PSTN gateways	Маа	ting URLs:	<u> </u>		1
	GW1.iLync15.local	Piee	ung OKLS:	Active	Simple URL	SIP domain
	Colt.ilync15.local			 Image: A second s	https://meet.iLync15.local	iLync15.local
	ITSP-GW.ilync15.local		inistrative access	https://	/admin.iLync15.local	
	🖃 🧰 Trunks 🏹 Ofer	URL	:			
	2, colt.ilync15.local					
	C ITSP-GW.ilync15.local					
	Office Web Apps Servers	Centra	al Management Server			
	Branch sites		arrianogenene server			
		Cent	tral Management	Active	Front End	Site
		Serv		Acuve	FE15.ilync15.local	
				•	reisinyficisilocal	AudioCodes
1						

The following is displayed:

Figure 3-11: Publish the Topology

🔀 Publish Topology	×
Publish the topology	
 In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed: A validation check on the root node did not return any errors. A file share has been created for all file stores that you have configured in this topology. All simple URLs have been defined. For Enterprise Edition Front End pools and Persistent Chat pools and for Monitoring Servers and Archiving Servers: All SQL Server stores are installed and accessible remotely, and firewall exceptions for remote access to SQL Server are configured. For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed. You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role). If you are removing a Front End pool, all users, common area phones, analog devices, application contact objects, and conference directories have been removed from the pool. 	
Help Back Next Cancel	

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

Figure 3-12: Publishing in Progress

T¢	Publish Topology	×
	Publishing in progress	
	Please wait while Topology Builder tries to publish your topology.	
	Succeeded	
	Downloading topology	
	Succeeded	
	Downloading global simple URL settings	
	Succeeded	
	Updating role-based access control (RBAC) roles	
	Succeeded	
	Enabling topology	•
	<u>B</u> ack <u>N</u> ext Cancel	



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

Figure 3-13: Publishing Wizard Complete

🔀 Publish Topology		×
Publishing wizard complete		
Your topology was successfully published.		
 ✓ Publishing topology ✓ Downloading topology ✓ Downloading global simple URL settings ✓ Updating role-based access control (RBAC) roles ✓ Enabling topology 	Status Success Success Success Success Success	<u>V</u> iew Logs
To close the wizard, click Finish. Help	<u>B</u> ack <u>Finish</u>	Cancel

11. Click Finish.

3.2 Configuring the "Route" on Lync Server 2013

The procedure below describes how to configure a "Route" on the Lync Server 2013 and to associate it with the E-SBC PSTN gateway.

> To configure the "route" on Lync Server 2013:

 Start the Microsoft Lync Server 2013 Control Panel (Start > All Programs > Microsoft Lync Server 2013 > Lync Server Control Panel), as shown below:

Figure 3-14: Opening the Lync Server Control Panel

Search programs and files	Log off
▲ Back	
	Windows Security
	Run
	Help and Support
🕌 Startup	Administrative Tools
Microsoft SQL Server 2012	Devices and Printers
Microsoft Silverlight Microsoft SQL Server 2008	
25 Lync Server Topology Builder	Control Panel
🡼 Lync Server Management Shell	Network
Microsoft Lync Server 2013	FE15
鷆 Maintenance	
🚡 Administrative Tools	Documents
Accessories	Administrator
Windows Media Player Windows Update	
C Internet Explorer	
<i>ế</i> Internet Explorer (64-bit)	
💮 Default Programs	



2. You are prompted to enter your login credentials:

Figure 3-15: Lync Server Credentials

Windows Securit	ty	×
Connecting to Fi	E15.ilync15.local.	
	ILYNC15\administrator	
	🔀 Remember my credentials	
	Use another account	
		1
	OK Cancel	

3. Enter your domain username and password, and then click **OK**; the Microsoft Lync Server 2013 Control Panel is displayed:

N 🖏	crosoft Lync Server 2013	Control Panel	_ 🗆 ×
	nc Server 2013		Administrator Sign out
Ц	The Server 2015		5.0.8308.0 Privacy statement
	Home		
33	Users		
×	Topology	User Information	Resources
Ģ	IM and Presence Persistent Chat	Welcome, Administrator View your roles	Getting Started First Run Checklist
-			Using Control Panel Microsoft Lync Server 2013
6	Voice Routing	Top Actions	Using Office 365
S	Voice Features	Enable users for Lync Server	Getting Help
23	Response Groups	Edit or move users View topology status	Downloadable Documentation
₽	Conferencing	View Monitoring reports	Online Documentation on TechNet Library Lync Server Management Shell
6	Clients		Lync Server Management Shell Script Library Lync Server Resource Kit Tools
ħ	Federation and External Access		Community Forums
	Monitoring and Archiving		Blogs
9	Security		
9	Network Configuration		

Figure 3-16: Microsoft Lync Server 2013 Control Panel

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

Figure 3-17: Voice Routing Page

Min	crosoft Lync Server 2013	Contra	ol Panel									
Lyı	nc Server 2013										Administrator	
1										5.0	.8308.0 Privacy	statemen
	Home		Dial Plan	Voice Policy	Route	PSTN U	sage	Trunk Configuration	Test Voice Routing			
33	Users		Create voice	e routing te	st case info	rmation						~
M	Topology											
P	IM and Presence								Q			
9	Persistent Chat		🕂 New 🔻	🥖 Edit	 Action 	on 🔻	Comm	it 🔻				2
٢	Voice Routing		Name	-					Description			
C	Voice Features		💮 GI	obal Glo	oal Co	mmitted	1					
23	Response Groups		33 Ca	olt Use	r Coi	mmitted	2					
Ð	Conferencing											
e.	Clients											
1	Federation and External Access											
	Monitoring and Archiving											
	Security											
Ŷ	Network Configuration											

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

Figure 3-18: Route Tab

 Users Users Create voice routing test case information Topology IM and Presence Persistent Chat Voice Routing Voice Routing Voice Features CoolRoute Committed Internal, Local, Long Distance ^(\+10-9](10))s SBA001 Committed Internal, Local, Long Distance ^\+97235555 ColT Committed Internal, Local, Long Distance ^\++00972 ColT Committed Internal, Local, Long Distance ^\+00972 	Home	Dial Plan	Voice Policy	Route PST	N Usage Tr	unk Configuration	Test Voice Ro	uting	
 IM and Presence Persistent Chat Voice Routing Voice Reatures Voice Features Conferencing Conferencing Collints Federation and External Access Monitoring and Archiving Security Network 	Lusers	Create vo	ice routing test	case informati	on				~
 Persistent Chat Voice Routing Voice Features Voice Features LocalRoute Committed Internal, Local, Long Distance ^(+10-9](10))5 SBA001 Committed Internal, Local, Long Distance ^(+97235555) COLT Committed Internal, Local, Long Distance ^(+097235555) COLT Committed Internal, Local, Long Distance ^(+097235555) Conferencing Clients Federation and External Access Monitoring and Archiving Security Network 	Topology								
Voice Routing Voice Routing Name State Voice Features LocalRoute Committed Internal, Local, Long Distance Article State Conferencing CollT Committed Internal, Local, Long Distance Article State Conferencing CollT Committed Internal, Local, Long Distance Article State Conferencing CollT Committed Internal, Local, Long Distance Article State Monitoring and Archiving Security Network	IM and Presence					\$	Þ		
Voice Routing Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network	Persistent Chat	- New	🧷 Edit 🔻	The Move up	A Move de	wn Action V	Commit v		6
Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network	Voice Routing		-					Pattern to match	
Conferencing Colients	 Voice Features 	Loc	alRoute		Committed	Internal, Local, Lo	ng Distance	^(\+1[0-9]{10})\$	
Clients Clients Clients Constrained and External Access Monitoring and Archiving Security Network	Response Groups	SBA	001		Committed	Internal, Local, Lo	ng Distance	^\+972355555	
Federation and External Access Monitoring and Archiving Security Network	Conferencing	со	LT		Committed	Internal, Local, Lo	ng Distance	^\+00972	
External Access Monitoring and Archiving Security Network	Clients								
and Archiving Security Network		4							
Network									
	Security								



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

Figure 3-19: Adding New Voice Route

OK 🗙 Cancel		
lame:*		
SIP Trunk Route		
escription:		
- Build a Pattern to Match -		
Add the starting digits that you	want this route to handle, or create	
the expression manually by click	rine Edit	
are expression manually by circl	ang can.	
Starting digits for numbers that		
Starting digits for numbers that	you want to allow:	
Starting digits for numbers that	you want to allow:	
Starting digits for numbers that	you want to allow:	
Starting digits for numbers that	you want to allow:	
Starting digits for numbers that	you want to allow:	
Starting digits for numbers that * Match this pattern:*	you want to allow:	
Starting digits for numbers that	you want to allow:	

- 7. In the 'Name' field, enter a name for this route (e.g., SIP Trunk Route).
- 8. In the 'Starting digits for numbers that you want to allow' field, enter the starting digits you want this route to handle (e.g., * to match all numbers), and then click **Add**.

Figure 3-20: Adding New Trunk

	h.c	0.8308.0 Privacy s
Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
Users	Create voice routing test case information	
Гороlоду		
M and Presence	New Voice Route	
Persistent Chat	V K Cancel	0
Voice Routing	Exceptions	1
Voice Features	Remove	
Response Groups		
Conferencing	Match this pattern: *	_
Clients	*	
Federation and External Access	Edit Reset 🕐	
Monitoring and Archiving	Suppress caller ID	
Security	Alternate caller ID:	
Network Configuration	Associated trunks:	
	Add	
	Remove	

- 9. Associate the route with the E-SBC Trunk that you created:
 - **a.** Under the 'Associated Trunks' group, click **Add**; a list of all the deployed gateways is displayed:

Ž	erosone erne serrer eoro e						
Ly	nc Server 2013					Administrato 5.0.8308.0 Privao	or Sign out cy statement
	Home	Dial Plan Voice Pol	cy Route PSTN Usage	Trunk Configuration	Test Voice Routing		
33	Users	Create voice routing	test case information			_	~
N	Topology	Select	Trunk		0	22	
Ę	IM and Presence	New Vo			م		
P	Persistent Chat	10			~		0
C			Service PstnGateway:GA001.ilync15.loc	Site al SBA00:			•
L	Voice Features		PstnGateway:GW1.iLync15.local				
22	Response Groups		PstnGateway:SBA-GW.ilync15.ic		st.ilync15.local		
Ŗ	Conferencing		PstnGateway:colt.ilync15.local	Audio			
P	Clients		PstnGateway:ITSP-GW.ilync15.k	ocal AudioC	lodes		
1	Federation and External Access						
	Monitoring and Archiving	SL					
•	Security	AI					
9	Network Configuration	Assoc				-	
					OK Cancel		
				_	INCIDENCE.		
							-

Figure 3-21: List of Deployed Trunks

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

Figure 3-22: Selected E-SBC Trunk

	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
lome 🛛		
Isers	Create voice routing test case information	_
opology		
M and Presence	New Voice Route	
ersistent Chat	√ OK × Cancel	(
oice Routing	Exceptions	
oice Features	Remove	
esponse Groups		
onferencing	Match this pattern: *	
lients		
ederation and xternal Access	Edit Reset 🕐	
fonitoring nd Archiving	Suppress caller ID	
ecurity	Alternate caller ID:	
letwork onfiguration	Associated trunks:	
	PstnGateway:ITSP Add	
	Remove	



- **10.** Associate a PSTN Usage to this route:
 - a. Under the 'Associated PSTN Usages' group, click **Select** and then add the associated PSTN Usage.

erver 2013		Administrator 5.0.8308.0 Privacy
ie la	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
s	Create voice routing test case information	
blogy		
nd Presence	New Voice Route	
istent Chat	✓ OK × Cancel	(
e Routing		
e Features	Associated trunks:	
oonse Groups	PstoGateway:ITSP Add	
ferencing	Remove	
nts		
eration and rnal Access	Associated PSTN Usages	
itoring	Select Remove 🛧 🦊	
Archiving	PSTN usage record Associated voice policies	
irity	Internal Global	
vork	Local Global	
figuration	Long Distance Global	
	Translated number to test:	

Figure 3-23: Associating PSTN Usage to Route

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

Figure 3-24: Confirmation of New Voice Route

			٩	
🕈 New 🧪 Edit 🔻 🏠 Mov	e up 🔸 Move down	Action T Com	mit 🔻	0
Name	State	PSTN usage	Pattern to match	
SIP Trunk Route	1 Uncommitte	ed Local, Internal	۸/*	

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

Figure 3-25: Committing Voice Routes

🕈 New 🧪 Edit 🔻 👚 Mov	e up 🔸 Move down Action	Commit V	(
Name	State PST	IN usa Review uncommitted changes	
SIP Trunk Route	🕤 Uncommitted Loca		

The Uncommitted Voice Configuration Settings page appears:



outes				*
Identity	Action	New value (pattern to match)	Old value (pattern to match)	
SIP Trunk Route	Added	٨/*		

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

Figure 3-27: Confirmation of Successful Voice Routing Configuration

	rosoft Lync Server 2013 C	ontrol Panel						<u>- 0 ×</u>
Lyr	nc Server 2013						5.0	Administrator Sign out 18308.0 Privacy statement
合	Home							
22	Users	Create voice ro	outing test case info	rmation				~
M	Topology							
Ģ	IM and Presence				۶			
2	Persistent Chat	4 New	Edit 🔻 👚 Mov	eup 🐣 Mov	re down Action 🔻	Commit 🔻		0
12		Name		State	PSTN usage		Pattern to match	
8	Voice Features	LocalRout	te	Committe	d Internal, Loc	al, Long Distance	^(\+1[0-9](10])\$	
22,	Response Groups	SBA001	Microsoft Lyne	: Server 2013	Control Panel	() X	^\+972355555	
Ð	Conferencing	COLT			ice routing configu		^\+00972	
	Clients	SIP Trun	U Successiony	published vo	ice routing coningu		*	
	Federation and External Access					Close		
	Monitoring and Archiving							
-	Security							
	Network Configuration							



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

ync Server 2013					_			5.0.8308.0 Privacy stat
Home	Dial Plan	Voice Policy	Route PS1	IN Usage Trunk C	onfiguration	Test Voice Routing		
Users	Create	voice routing tes	t case informat	ion				
Topology								
IM and Presence					م			
Persistent Chat	4 Nev	V 🧪 Edit 🔻	1 Move up	🕂 Move down	Action ▼	Commit 🔻		
Voice Routing	N	lame		State	PSTN usage		Pattern to match	
- Voice Features	Ŀ	ocalRoute		Committed	Internal, Loca	al, Long Distance	^(\+1[0-9]{10})\$	
Response Groups	s	BA001		Committed	Internal, Loca	al, Long Distance	^\+972355555	
Conferencing	c	OLT		Committed	Internal, Loca	al, Long Distance	^\+00972	
Clients	S	IP Trunk Route		Committed	Internal, Loca	al, Long Distance	,*	
Federation and External Access	•							
Monitoring and Archiving								
Security								
Network Configuration								

Figure 3-28: Voice Routing Screen Displaying Committed Routes

AudioCodes

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Microsoft Lync Server 2013 and the TWCBC SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- E-SBC WAN interface TWCBC SIP Trunking environment
- E-SBC LAN interface Lync Server 2013 environment

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

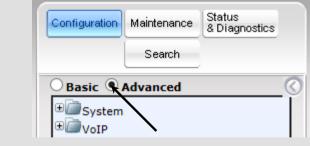
Notes:

- For implementing Microsoft Lync and TWCBC 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 Microsoft Lync environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Advanced-menu display mode. To do this, select the **Advanced** option, as shown below:



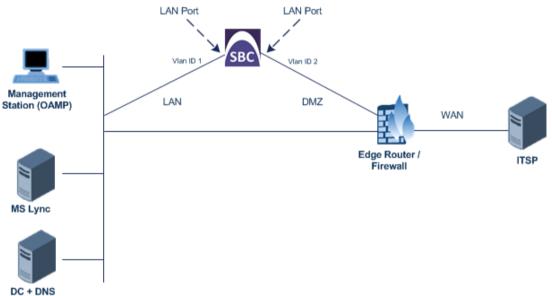
• When the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

4.1 Step 1: IP Network Interfaces Configuration

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

- E-SBC interfaces with the following IP entities:
 - Lync servers, located on the LAN
 - TWCBC 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 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 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 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 4-2: Configured VLAN IDs in Ethernet Device Table

Add +			
Index 4	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2
		e 1 of 1 🔛 🖬 Show 10 🗸 records pe	r page View 1 - 2 of

4.1.2 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:
- 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	195.189.192.158 (WAN IP address)
Prefix Length	25 (for 255.255.255.128)
Default 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 4-3: Configured Network Interfaces in IP Interfaces Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underly Devic
0 0	OAMP + Media + C	IPv4 Manual	10.15.17.77	16	10.15.0.1	Voice	10.15.25.1		vlan 1
1 1	Media + Control	IPv4 Manual	195.189.192.158	25	195.189.192.129	WANSP	80.179.52.100	80.179.55.100	vlan 2

4.1.3 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".

 Phys 	ical Ports Settin	igs					
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

Figure 4-4: Configured Port Native VLAN

4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

To enable the SBC application:

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

Figure 4-5: Enabling SBC Application

🗲 SAS Application	Disable	~	
🗲 SBC Application	Enable	~	
🗲 IP to IP Application	Disable	~	

- 2. From the 'SBC Application' drop-down list, select **Enable**.
- 3. Click Submit.
- Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.16 on page 75).

4.3 **Step 3: Signaling Routing Domains Configuration**

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

The SRD is composed of the following:

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

4.3.1 Step 3a: Configure Media Realms

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

- **To configure Media Realms:**
- Open the Media Realm Table page (Configuration tab > VolP menu > VolP 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 4-6: Configuring Media Realm for LAN

Index	þ	
Media Realm Name	MRLan	
IPv4 Interface Name	Voice	~
IPv6 Interface Name	None	~
Port Range Start	6000	
Number Of Media Session Legs	10	
Port Range End	6090	
Default Media Realm	Yes	~
QOE Profile	None	~
BW Profile	None	~

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 4-7: Configuring Media Realm for WAN

Index	1	
Media Realm Name	MRWan	
IPv4 Interface Name	WANSP	~
IPv6 Interface Name	None	~
Port Range Start	7000	
Number Of Media Session Legs	10	
Port Range End	-1	
Default Media Realm	No	~
QOE Profile	None	~
BW Profile	None	~

The configured Media Realms are shown in the figure below:

Figure 4-8: Configured Media Realms in Media Realm Table

Index (Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
0	MRLan	Voice	None
1	MRWan	WANSP	None

4.3.2 Step 3b: Configure SRDs

This step describes how to configure the SRDs.

To configure SRDs:

- 1. Open the SRD Settings page (Configuration tab > VoIP menu > VoIP Network > SRD Table).
- 2. Configure an SRD for the E-SBC's internal interface (toward Lync Server 2013):

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

Figure 4-9	: Configuring	LAN SRD
------------	---------------	---------

0
SRDLan
MRLan 🔻
Enable 🔻
NO
-1
Enable 🔻

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

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

Figure 4-10: Configuring WAN SRD

Edit Record #1	
Index	1
Name	SRDWan
Media Realm Name	MRWan 🔻
Media Anchoring	Enable 🔻
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable 🔻



The configured SRDs are shown in the figure below:

Figure 4-11: Configured SRDs in SRD Table

Index ·	Name	Media Realm Name	Media Anchoring
o s	SRDLan	MRLan	Enable
1 S	SRDWan	MRWan	Enable

4.3.3 Step 3c: Configure SIP Signaling Interfaces

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

To configure SIP Interfaces:

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

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

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	1
Interface Name	TWCBC (arbitrary descriptive name)
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TCP and TLS	0
SRD	1

The configured SIP Interfaces are shown in the figure below:

Figure 4-12: Configured SIP Interfaces in SIP Interface Table

Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
D.	Lync	Voice	SBC	0	0	5067	0
L	TWCBC	WANSP	SBC	5060	0	0	1

4.4 Step 4: Configure Proxy Sets

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

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

- Microsoft Lync Server 2013
- TWCBC SIP Trunk

These Proxy Sets will later be associated with IP Groups.

- **To configure Proxy Sets:**
- Open the Proxy Sets Table page (Configuration tab > VolP menu > VolP Network > Proxy Sets Table).
- 2. Configure a Proxy Set for Lync Server 2013:

Parameter	Value
Proxy Set ID	1
Proxy Address	FE15.ilync15.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
Proxy Redundancy Mode	Homing
SRD Index	0

	•					
\longrightarrow	Proxy Se	et II	D	1		~
			Proxy Address		Transport Type	
\rightarrow		1	FE15.ilync15.local:5067		TLS 🗸	←
		2			~	
		3			~	
		4			~	
		5			~	1
		6			~	
		7			~	
		8				
		9				-
		10				-
_						
	•			1		
→ _	Proxy Na			Lync		
→_			y Keep Alive	Using Opt	ions	<u> </u>
	Proxy Ke	eep	Alive Time	60		
	KeepAliv	e F	ailure responses			
	DNS Res	olv	e Method	Not Config	gured	\checkmark
\rightarrow	Proxy Lo	ad	Balancing Method	Round Ro	bin	~
\rightarrow	Is Proxy	Но	t Swap	Yes		\checkmark
\rightarrow	Proxy Re	edu	ndancy Mode	Homing		~
\rightarrow	SRD Ind	ex		0		
	Classifica	atio	n Input	IP only		~
	TLS Con	tex	t Index	-1		

Figure 4-13: Configuring Proxy Set for Microsoft Lync Server 2013

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

Parameter	Value
Proxy Set ID	2
Proxy Address	107.14.112.4 (TWCBC IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	TWCBC (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
SRD Index	1 (enables classification by Proxy Set for SRD of IP Group belonging to TWCBC SIP Trunk)



Proxy Set II)	2	•
	Proxy Addre	ess	Transport Type
1	107.14.112.4		UDP V
2			T
3			T
4			T
5			T
6			T
7			T
8			T
9			T
10			T
Proxy Name	5	ТWCBC	
-	y Keep Alive	Using Options	•
Proxy Keep		60	
	ailure responses		
DNS Resolv		Not Configured	Ŧ
Proxy Load	Balancing Method	Disable	•
Is Proxy Ho	t Swap	No	•
Proxy Redu	ndancy Mode	Not Configured	•
SRD Index		1	
Classificatio	n Input	IP only	•
TLS Contex	t Index	-1	

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

4. Reset the E-SBC with a burn to flash for these settings to take effect (see Section 4.16 on page 75).

4.5 Step 5: Configure IP Groups

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

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

- Lync Server 2013 (Mediation Server) located on the LAN
- TWCBC SIP Trunk located on the WAN
- To configure IP Groups:
- 1. Open the IP Group Table page (Configuration tab > VoIP menu > VoIP Network > IP Group Table).

Parameter	Value
Index	1
Туре	Server
Description	Lync (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	195.189.192.158 (according to ITSP requirement)
SRD	0
Media Realm Name	MRLan
IP Profile ID	1

2. Configure an IP Group for the Lync Server 2013 Mediation Server:

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

Parameter	Value
Index	2
Туре	Server
Description	TWCBC (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	195.189.192.158 (according to ITSP requirement)
SRD	1
Media Realm Name	MRWan
IP Profile ID	2



The configured IP Groups are shown in the figure below:

Figure 4-15: Configured IP Groups in IP Group Table

oup Table							
Туре	Description	Proxy Set ID	SIP Group Name	Contact User	SIP Re-Routing Mode	Always Use Route Table	SRD
Server	Lync	1	195.189.192.158			No	0
Server	TWCable	2	195.189.192.158			No	1
	Server	Server Lync	Server Lync 1	Server Lync 1 195.189.192.158	Type Description Proxy Set ID Name Contact Oser Gerver Lync 1 195.189.192.158 1	Type Description Proxy set ID Name Contact oser Mode Gerver Lync 1 195.189.192.158 1 </td <td>Type Description Proxy set ID Name Contact over Mode Route Table server Lync 1 195.189.192.158 No No</td>	Type Description Proxy set ID Name Contact over Mode Route Table server Lync 1 195.189.192.158 No No

4.6 Step 6: Configure IP Profiles

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

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

- Microsoft Lync Server 2013 to operate in secure mode using SRTP and TLS
- TWCBC SIP trunk 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 4.5 on page 43).

To configure IP Profiles:

- 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 4-16: Configuring IP Profile for Lync Server 2013 – Common Tab

Index	[1	
Profile Name	Lync	
Profile Preference	1	
Dynamic Jitter Buffer Minimum Delay [msec]	10	
Dynamic Jitter Buffer Optimization Factor	10	
RTP IP DiffServ	46	
Signaling DiffServ	40	
Silence Suppression	Disable	
RTP Redundancy Depth	0	
Echo Canceler	Line	
Disconnect on Broken Connection	Yes	
Input Gain (-32 to 31 dB)	0	
Voice Volume (-32 to 31 dB)	0	
Media IP Version Preference	Only IPv4	
Symmetric MKI	Enable	
MKI Size	1	
Reset SRTP Upon Re-key	Enable	
Generate SRTP keys mode	Always	

- Parameter Value SBC Media Security Behavior SRTP PRACK Mode **Optional** (required, as TWCBC SIP Trunk does not generate PRACK) **Supported** (required, as TWCBC SIP Trunk Session Expires Mode does not generate Session Expire Timer in incoming calls, so SBC will negotiate it with Lync Server) Remote Update Support Supported Only After Connect Remote Re-INVITE Supported Only With SDP Remote Delayed Offer Support Not Supported Remote REFER Behavior Handle Locally (required, as 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 By Media (required, as Lync Server 2013 does Remote Early Media RTP Detection not send RTP immediately to remote side Mode when it sends a SIP 18x response) Generate Always (required, as TWCBC SIP **RTCP Mode** Trunk does not send RTCP packets in hold call, and in this case, Microsoft Lync 2013 will terminate the call with network problems as the cause)
- 4. Click the **SBC** tab, and then configure the parameters as follows:

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

Figure 4-17: Configuring IP Profile for Lync Server 2013 – SBC Tab

> To configure an IP Profile for the TWCBC SIP Trunk:

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

Parameter	Value
Index	2
Profile Name	TWCBC (arbitrary descriptive name)

Figure 4-18: Configuring IP Profile for TWCBC SIP Trunk – Common Tab

Index	2
Profile Name	TWCBC
Profile Preference	1
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceler	Line
Disconnect on Broken Connection	No
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable 🔹
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required
Jitter Buffer Max Delay [msec]	300

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

Parameter	Value		
Index	2		
SBC Media Security Behavior	RTP		
Remote REFER Behavior	Handle Locally (E-SBC handles / terminates incoming REFER requests instead of forwarding them to SIP Trunk)		
Remote Multiple 18x	Not Supported (required, as TWCBC SIP Trunk does not support multiple 18x)		
Remote Can Play Ringback	No (required, as Lync Server 2013 does not provide a ring-back tone for incoming calls)		

Index	2	
Extension Coders Group ID	None	
Transcoding Mode	Only If Required	
Allowed Media Types		
Allowed Coders Group ID	None	
Allowed Video Coders Group ID	None	
Allowed Coders Mode	Restriction	
SBC Media Security Behavior	RTP	
RFC 2833 Behavior	As Is	
Alternative DTMF Method	As Is	
P-Asserted-Identity	As Is	
Diversion Mode	As Is	
History-Info Mode	As Is	
Fax Coders Group ID	None	
Fax Behavior	As Is	_
Fax Offer Mode	All coders	_
Fax Answer Mode	Single coder	_
PRACK Mode	Transparent	
Session Expires Mode	Transparent	
Remote Update Support	Supported	
Remote re-INVITE	Supported	
Remote Delayed Offer Support	Supported	
Remote REFER Behavior	Handle Locally	
Remote 3xx Behavior	Transparent	
Remote Multiple 18x	Not Supported	
Remote Early Media Response Type	Transparent	_
Remote Early Media	Supported	_
Enforce MKI Size	Don't enforce	_
Remote Early Media RTP Detection Mode	By Signaling	_
Remote RFC 3960 Gateway Model Support	Not Supported	
Remote Can Play Ringback	No	_
RFC 2833 DTMF Payload Type	0	_
User Registration Time		
-	0	
Reliable Held Tone Source	Yes	
Play Held Tone	No	
Remote Hold Format	Transparent	
Remote Replaces Behavior	Standard	
SDP Ptime Answer	Remote Answer	
Preferred PTime	0	
Use Silence Suppression	Transparent	
RTP Redundancy Behavior	AS IS	
Play RBT To Transferee	No	
RTCP Mode	Transparent	
Jitter Compensation	Disable	
Remote Renegotiate on Fax Detection	Transparent	
Remote Multiple Answers Mode	Disabled	
Keep VIA Headers	Not Configured	
Keep User-Agent Header	Not Configured	
User Behind NAT UDP Registration Time	-1	
User Behind NAT TCP Registration Time	-1	

Figure 4-19: Configuring IP Profile for TWCBC SIP Trunk – SBC Tab

4.7 Step 7: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Lync Server 2013 supports the G.711 coder while the network connection to TWCBC SIP Trunk <u>may</u> 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 TWCBC SIP Trunk.



Note: This step is required **only** if transcoding is required. In the tested configuration transcoding was not needed, so this step was skipped.

Note that the Coder Group ID for this entity should be assigned to its corresponding IP Profile in the previous step (see Section 4.6 on page 45).

- 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 Lync Server 2013:

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

Figure 4-20: Configuring Coder Group for Lync Server 2013

Coder Group ID				1 🔻			
Coder Nam	ie	Packetiza	tion Time	Rate		Payload Type	Silence Suppression
Coder Nam G.711U-law	re •	Packetiza 20	tion Time T	Rate	•	Payload Type	Silence Suppression Enable

3. Configure a Coder Group for <Vendor> SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	G.729

Figure 4-21: Configuring Coder Group for TWCBC SIP Trunk

•					
Coder Group ID 2					
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	
Coder Name	Fackedization fine	Kate	Fayload Type	Silence Suppression	
G.729	20 💌	8 💌	18	Disabled 💌	

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the TWCBC SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID should be assigned to the IP Profile belonging to the TWCBC SIP Trunk in the previous step (see Section 4.6 on page 45).

- > To set a preferred coder for the TWCBC 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.729

Figure 4-22: Configuring Allowed Coders Group for TWCBC SIP Trunk

▼		
Allowed Coders Group ID	2 💌	
	Coder Name	
	G.729	

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

Figure 4-23: SBC	Preferences Mode
------------------	------------------

Transcoding Mode	Only If Required	
No Answer Timeout [sec]	600	
GRUU Mode	As Proxy	~
Minimum Session-Expires [sec]	90	
BroadWorks Survivability Feature	Disable	~
BYE Authentication	Disable	~
User Registration Time [sec]	0	
Proxy Registration Time [sec]	0	
Survivability Registration Time [sec]	0	
Forking Handling Mode	Sequential	~
Unclassified Calls	Reject	~
Session-Expires [sec]	180	
Direct Media	Disable	~
Preferences Mode	Include Extensions	~
User Registration Grace Time [sec]	0	
Fax Detection Timeout [sec]	10	
RTCP Mode	Transparent	~
Max Forwards Limit	10	



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

4.8 Step 8: SIP TLS Connection Configuration

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

4.8.1 Step 8a: Configure the NTP Server Address

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

> To configure the NTP server address:

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

▼ NTP Settings	
NTP Server Address (IP or FQDN)	10.15.25.1
NTP UTC Offset	Hours: 3 Minutes: 0
NTP Updated Interval	Hours: 24 Minutes: 0
NTP Secondary Server Address (IP or FQDN)	
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

Figure 4-24: Configuring NTP Server Address

3. Click Submit.

4.8.2 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).
- 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 4-25: Certificate Signing Request – Creating CSR

Subject Name [CN]	
Subject Name [CN]	ITSP-GW.ilync15.local
Organizational Unit [OU] (optional)	
Company name [O] (optional)	
Locality or city name [L] (optional)	
State [ST] (optional)	
Country code [C] (optional)	
After creating the CSR, copy the text below (signing.	ncluding the BEGIN/END lines) and send it to your Certification Authority
BEGIN CERTIFICATE REQUEST	LmlseW5jMTUubG9jYWwwgZ8w



Note: The value entered in this field must be identical to the gateway name configured in the Topology Builder for Lync Server 2013 (see Section 3.1 on page 13.

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

Figure 4-26: Microsoft Certificate Services Web Page

Microsoft Certificate Services Demolab Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

7. Click Request a certificate.

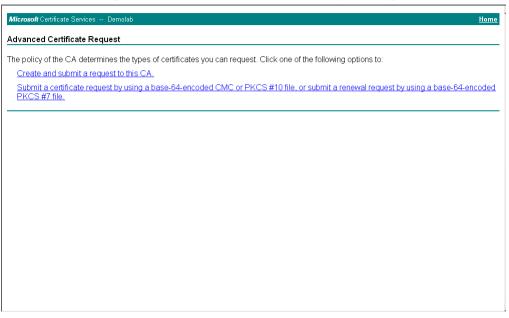
Figure 4-27: Request a Certificate Page

Microsoft Certificate Services Demolab		<u>H</u> t	ome
Request a Certificate			
Select the certificate type: Web Browser Certificate E-Mail Protection Certificate			
Or, submit an advanced certificate request.			



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





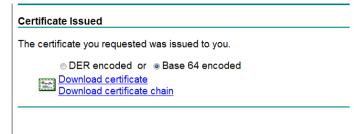
9. Click **Submit a certificate request ...**, and then click **Next**.



	Directory Certificate Services ~ Lync-DC-LYNC-CA ificate Request or Renewal Request	<u>Home</u>
	ved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal in external source (such as a Web server) in the Saved Request box.	request
Saved Request:		
certificate request (CMC or	A8jxeP85ymyfbknfx+zEusB8z8h4JgzbeNxwyKk1 rrfootrnsP0CAvEAAAAHAOCC3qGSHb3DeDBBNUA HnKHAkzeMg9gaagoLKmuch2Ba2m4gEcCAFTRack 9f3m8c4Bj81b+F5+YI+Ost57xT9D2XNg5Yp4G+OB vnduXOUUX6B=VBT71aC083HcA END CERTIFICATE REQUEST < m + Hate:	
Additional Attribu		
Attributes:	·	
	Submit >	

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

Figure 4-30: Certificate Issued Page



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

Figure 4-31: Download a CA Certificate, Certificate Chain, or CRL Page

Microsoft Certificate Services Demolab	<u>Home</u>
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
© DER © Base 64	
Download CA certificate Download CA certificate chain Download latest base CRL	
	[

- 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.

AudioCodes

- 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 4-32: Upload Device Certificate Files from your Computer Group

 Upload certificate files from your co 	mputer	
Private key pass-phrase (optional)		audc
Send Private Key file from your com The file must be in either PEM or PFX		
	Browse	Send File
Note: Replacing the private key is a physically-secure network link.		ended but if it's done, it should be over
Send Device Certificate file from yo	our computer to i	Alex alexies
Cond Davies Contificate file from w	our computer to l	ales destine

- 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 4-33: Importing Root Certificate into Trusted Certificates Store

Import New Certificate	×
D:\backup\warehouse\c Brows	e
	OK Cancel

- **21.** Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.
- **22.** Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 75).

4.9 Step 9: Configure SRTP

This step describes how to configure media security. If you configure the Microsoft Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for Lync Server 2013 when you configured an IP Profile for Lync Server 2013 (see Section 4.6 on page 45).

> 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 4-34: Configuring SRTP

-	General Media Security Settings		
• 🗲	Media Security	Enable	~
4	Aria Protocol Support	Disable	~
	Media Security Behavior	Mandatory	~
	Authentication On Transmitted RTP Packets	Active	~
	Encryption On Transmitted RTP Packets	Active	~
	Encryption On Transmitted RTCP Packets	Active	~
4	SRTP Tunneling Authentication for RTP	Disable	~
4	SRTP Tunneling Authentication for RTCP	Disable	~

3. Click Submit.

4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.16 on page 75).

4.10 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. In the tested configuration transcoding was not needed, so this step was skipped.

> To configure the maximum number of IP media channels:

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

Figure 4-35: Configuring Number of IP Media Channels

Number of Media Channels	30
Voice Streaming	Disable
NetAnn Announcement ID	annc
MSCML ID	ivr
Transcoding ID	trans

- 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 4.16 on page 75).

4.11 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 4.5 on page 43, IP Group 1 represents Lync Server 2013, and IP Group 2 represents TWCBC SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Lync Server 2013 (LAN) and TWCBC SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the LAN
- Calls from Lync Server 2013 to TWCBC SIP Trunk
- Calls from TWCBC SIP Trunk to Lync Server 2013
- **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 4-36: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab

Index	0
Route Name	OPTIONS termination
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS V
Message Condition	None 🗸
ReRoute IP Group ID	-1
Call Trigger	Any 🗸

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-37: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab

Index	0		
Destination Type	Dest Address	~	
Destination IP Group ID	-1		
Destination SRD ID	None	~	
Destination Address	internal		
Destination Port	0		
Destination Transport Type		~	
Alternative Route Options	Route Row	~	
Group Policy	None	~	
Cost Group	None	~	
Rules Set Id	-1		

6. Configure a rule to route calls from Lync Server 2013 to TWCBC SIP Trunk:

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

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

Figure 4-38: Configuring IP-to-IP Routing Rule for Lync to ITSP – Rule tab

Index	1
Route Name	Lync to ITSP
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None 🗸
ReRoute IP Group ID	-1
Call Trigger	Any 🗸

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	1

AudioCodes

Figure 4-39: Configuring IP-to-IP Routing Rule for Lync to ITSP – Action tab

Index	1
Destination Type	IP Group 🔻
Destination IP Group ID	2
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	T
Alternative Route Options	Route Row 🔻
Group Policy	None 🔻
Cost Group	None 🔻

- **To configure rule to route calls from TWCBC SIP Trunk to Lync Server 2013:**
- 1. Click Add.
- 2. Click the **Rule** tab, and then configure the parameters as follows:

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

Index	2	
Route Name	ITSP to Lync	
Source IP Group ID	2	
Source Username Prefix	×	
Source Host	×	
Destination Username Prefix	×	
Destination Host	*	
Request Type	All	~
Message Condition	None	~
ReRoute IP Group ID	-1	
Call Trigger	Any	~

Figure 4-40: Configuring IP-to-IP Routing Rule for ITSP to Lync – Rule tab

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

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

Figure 4-41: Configuring IP-to-IP Routing Rule for ITSP to Lync – Action tab

Index	2
Destination Type	IP Group 🔻
Destination IP Group ID	1
Destination SRD ID	0 🔻
Destination Address	
Destination Port	0
Destination Transport Type	T
Alternative Route Options	Route Row 🔻
Group Policy	None 🔻
Cost Group	None 🔻

The configured routing rules are shown in the figure below:

Figure 4-42: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

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



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

4.12 Step 12: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.5 on page 43, IP Group 1 represents Lync Server 2013, and IP Group 2 represents TWCBC SIP Trunk.



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

For this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from IP Group 2 (TWCBC SIP Trunk) to IP Group 1 (i.e., Lync Server 2013) for any destination username prefix.

To configure a number manipulation rule:

- 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 ID	2
Destination IP Group ID	1
Destination Username Prefix	* (asterisk sign)

Figure 4-43: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Index	1	
Manipulation Name		
Additional Manipulation	No	~
Source IP Group ID	2	
Destination IP Group ID	1	
Source Username Prefix	*	
Source Host	*	
Destination Username Prefix	*	
Destination Host	*	
Calling Name Prefix	*	
Message Condition	None	~
Request Type	All	~
ReRoute IP Group ID	-1	
Call Trigger	Any	~

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

Parameter	Value
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 4-44: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

Index	1
Manipulated Item	Destination URI V
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	
Privacy Restriction Mode	Transparent V

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., Lync Server 2013) and IP Group 2 (i.e., TWCBC SIP Trunk):

Figure 4-45: Example of Configured IP-to-IP Outbound Manipulation Rules

	Additional	Source IP	Destination	Source							
- Turno	Manipulatio	Group ID	IP Group ID	Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulatec Item	Prefix to Add	Suffix to Add
1	No	2	1	*	*	*	*	All	Destination	+	
1	No	1	2	*	*	+	*	All	Destination		
ſ	No	1	2	+	*	*	*	All	Source URI		
	I	No No No	No 1	No 1 2	No 1 2 *	NO 2 1 - - No 1 2 * *	No 1 2 * * +	NO 2 1 -	No 1 2 * + All	No 1 2 * * + All Destination	No 1 2 * * + All Destination

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.

4.13 Step 13: Configure Message Manipulation Rules

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

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

- **To configure SIP message manipulation rule:**
- 1. Open the Message Manipulations page (Configuration tab > VoIP menu > SIP Definitions > Msg Policy & Manipulation > Message Manipulations).
- 2. Add a manipulation rule to Index 0 for TWCBC's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the TWCBC SIP Trunk (IP Group 2). This removes the 'opaque' parameter from the SIP From Header.

Parameter	Value
Index	0
Manipulation Name	Remove opaque
Manipulation Set ID	4
Message Type	any.request
Action Subject	header.from.url.param.ms-opaque
Action Type	Remove

Figure 4-46: Configuring SIP Message Manipulation Rule 0 (for TWCBC's SIP Trunk)

Index	0
Manipulation Name	Remove opaque
Manipulation Set ID	4
Message Type	any.request
Condition	
Action Subject	header.from.url.param.
Action Type	Rem ove 🔻
Action Value	
Row Role	Use Current Condit 🔻

3. Add a manipulation rule to Index 1 for TWCBC's SIP Trunk (Manipulation Set ID 4). This rule applies to messages sent to the TWCBC SIP Trunk (IP Group 2). This replaces the host part of the Referred-By Header with the value from the From Header.

Parameter	Value
Index	1
Manipulation Name	Host of Referred-by
Manipulation Set ID	4
Condition	header.referred-by exists
Action Subject	header.referred-by.url.host
Action Type	Modify
Action Value	header.from.url.host

Figure 4-47: Configuring SIP Message Manipulation Rule 1 (for TWCBC's SIP Trunk)

Index	1
Manipulation Name	Host of Referred-by
Manipulation Set ID	4
Message Type	any.request
Condition	header.referred-by exis
Action Subject	header.referred-by.url.h
Action Type	Modify 🔻
Action Value	header.from.url.host
Row Role	Use Current Condit 🔻

Figure 4-48: Configured SIP Message Manipulation Rules

Name	Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
e opaque	4	any.request		header.from.url.param.	Remove	
Referred-by	4	any.request	header.referred-by exists	header.referred-by.url.	Modify	header.from.ur
		e opaque 4 Referred-by 4				

The table displayed below includes SIP message manipulation rules which are bound together by commonality via the Manipulation Set IDs (Manipulation Set ID 4), which are executed for messages sent to and from the TWCBC SIP Trunk (IP Group 2). These rules are specifically required to enable proper interworking between TWCBC SIP Trunk and Lync Server 2013. 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 sent to the TWCBC SIP Trunk (IP Group 2). This removes the 'opaque' parameter from the SIP From Header.	-
1	This rule applies to messages sent to the TWCBC SIP Trunk (IP Group 2). This replaces the host part of the Referred-By Header with the value from the From Header.	-

- 4. Assign Manipulation Set ID 4 to IP Group 2:
 - 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 4-49: Assigning Manipulation Set 4 to IP Group 2

ndex	2
Classify By Proxy Set	Enable 🗸
1ax. Number of Registered Users	-1
nbound Message Manipulation Set	-1
Outbound Message Manipulation Set	4
Registration Mode	User Initiates Registra 🗸
Authentication Mode	User Authenticates 🗸
Authentication Method List	
SBC Client Forking Mode	Sequential V
Source URI Input	Not Configured 🗸
Destination URI Input	Not Configured 🗸
Jsername	
Password	

e. Click Submit.

4.14 Step 14: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the TWCBC SIP Trunk on behalf of Lync Server 2013. The TWCBC SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is Lync Server 2013 (IP Group 1) and the Serving IP Group is TWCBC SIP Trunk (IP Group 2).

> To configure a registration account:

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

Figure 4-50: Configuring SIP Registration Account

Index	Served Trunk Group	Served IP Group	Serving IP Group	User Name	Password	Host Name	Register	Contact User	Applica Typ
0	-1	1	2	19199732120	*	107.14.112.4	Regular	19199732120	SBC

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

Parameter	Value
Served IP Group	1 (Lync Server 2013)
Serving IP Group	2 (TWCBC SIP Trunk)
Username	As provided by TWCBC
Password	As provided by TWCBC
Host Name	107.14.112.4 (As provided by TWCBC)
Register	Regular
Contact User	19199732120 (trunk main line)
Application Type	SBC

4. Click Apply.

4.15 Step 15: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

4.15.1 Step 15a: Configure Call Forking Mode

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

> To configure call forking:

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

Figure 4-51: Configuring Forking Mode

▼		
Transcoding Mode	Only If Required	~
No Answer Timeout [sec]	600	
GRUU Mode	As Proxy	~
Minimum Session-Expires [sec]	90	
BroadWorks Survivability Feature	Disable	~
BYE Authentication	Disable	~
User Registration Time [sec]	0	
Proxy Registration Time [sec]	0	
Survivability Registration Time [sec]	0	
Forking Handling Mode	Sequential	~
Unclassified Calls	Reject	~
Session-Expires [sec]	180	
Direct Media	Disable	~
Preferences Mode	Include Extensions	~
User Registration Grace Time [sec]	0	
Fax Detection Timeout [sec]	10	
RTCP Mode	Transparent	~
Max Forwards Limit	10	

3. Click Submit.

4.15.2 Step 15b: Configure SBC Session Refreshing Policy

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

> To configure SBC Session Refreshing Policy:

- 1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., <u>http://10.15.17.77/AdminPage</u>).
- 2. In the left pane of the page that opens, click *ini* Parameters.

Figure 4-52: Configuring SBC Session Refreshing Policy in AdminPage

→	Parameter Name: Enter Value: 1 Apply New Va SBCSESSIONREFRESHINGPOLICY	lue		
	Output Window			
	Parameter Name: SBCSESSIONREFRESHINGPOLICY Parameter New Value: 1 Parameter Description:Defines whether Remote or SBC should be refresher when SBC terminates the Session Expire refreshing			

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

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

4. Click the Apply New Value button.

4.15.3 Step 15c: Loading Prerecorded Ring-Back Tone File

This step shows how to load a pre-recorded ring-back PRT tone file.

Notes:

- Playing tones from the PRT file does not require DSP resources.
- For SBC calls, the PRT file supports only calls that use the G.711 coder.
- For SBC calls, the PRT file supports only the ring-back and hold tones.

The pre-recorded tones are prepared offline using third-party recording utilities and combined into a single file, using the AudioCodes DConvert utility (refer to the *DConvert Utility User's Guide* for more information).

The raw data files must be recorded with the following characteristics:

- Coders: G.711 A-law or G.711 μ-law
- Rate: 8 kHz
- Resolution: 8-bit
- **Channels:** mono
- To load a pre-recorded file to the device using the Web interface:
- Open the Load Auxiliary Files page (Maintenance tab > Software Update menu > Load Auxiliary Files).

INI file (incremental) Choose File No file chosen	Load File
CAS file Choose File No file chosen	Load File
✓ Call Progress Tones file Choose File No file chosen	Load File
Prerecorded Tones file Choose File No file chosen	Load File
Dial Plan file Choose File No file chosen	Load File
User Info file Choose File No file chosen	Load File

Figure 4-53: Load Auxiliary Files

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

4.16 Step 16: 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).

✓ Reset Configuration				
Reset Board	Reset			
Burn To FLASH	Yes			
Graceful Option	No			
LOCK / UNLOCK Lock LOCK				
Graceful Option	No			
Gateway Operational State	UNLOCKED			
▼ Save Configuration				
Burn To FLASH	BURN			

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



This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 29, 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.258.005
;DSP Software Version: 5014AE3_R => 680.28
;Board IP Address: 10.15.17.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
               Flash size: 64M Core speed: 300Mhz
;Ram size: 369M
;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
```

AudioCodes

```
NTPServerIP = '10.15.25.1'
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_qwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value
[BSP Params]
PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
[Analog Params]
[ControlProtocols Params]
AdminStateLockControl = 0
[MGCP Params]
[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
[PSTN Params]
[SS7 Params]
[Voice Engine Params]
PrerecordedTonesFileName = 'RingingTonePRT-G711U.dat'
;Offline: initial val of PrerecordedTonesFileName param is '' (new val is
'RingingTonePRT-G711U.dat')
ENABLEMEDIASECURITY = 1
SRTPTxPacketMKISize = 1
CallProgressTonesFilename = 'usa_tones_13.dat'
[WEB Params]
UseRProductName = 'Mediant 800 E-SBC'
WebLogoText = 'TWCBC'
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
```

```
[SIP Params]
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCPREFERENCESMODE = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SBCSESSIONREFRESHINGPOLICY = 1
[SCTP Params]
[IPsec Params]
[Audio Staging Params]
[SNMP Params]
[ PhysicalPortsTable ]
FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan,
PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription,
PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 2, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 2, 4, "User Port #3", "GROUP_2",
"Redundant";
PhysicalPortsTable 4 = "FE_5_1", 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_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.17.77, 16, 10.15.0.1, "Voice",
10.15.25.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.158, 25, 195.189.192.129, "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_BlockUnReqUsers, SRD_MaxNumOfReqUsers,
SRD_EnableUnAuthenticatedRegistrations;
SRD 0 = "SRDLan", "MRLan", 0, 0, -1, 1;
SRD 1 = "SRDWan", "MRWan", 0, 0, -1, 1;
[ \SRD ]
[ ProxyIp ]
FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType,
ProxyIp_ProxySetId;
ProxyIp 0 = "FE15.ilync15.local:5067", 2, 1;
ProxyIp 1 = "107.14.112.4", -1, 2;
[ \ProxyIp ]
[ IpProfile ]
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile MediaIPVersionPreference, IpProfile TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
```

```
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay, IpProfile_SBCRemoteMultipleAnswersMode,
IpProfile SBCKeepVIAHeaders, IpProfile SBCKeepUserAgentHeader,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime;
IpProfile 1 = "Lync", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
0, 300, 0, -1, -1, -1, -1;
IpProfile 2 = "TWCBC", 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, 2,
0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 3, 0, 0, 0,
0, 0, 300, 0, -1, -1, -1, -1;
[ \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, 0, "-1", -1, -1, "";
ProxySet 1 = "Lync", 1, 60, 1, 1, 0, 0, "-1", 1, -1, "";
ProxySet 2 = "TWCBC", 1, 60, 0, 0, 1, 0, "-1", -1, -1, "";
[ \ProxySet ]
[ IPGroup ]
FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description,
IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser,
IPGroup_EnableSurvivability, IPGroup_ServingIPGroup,
IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers,
IPGroup InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
```

```
IPGroup_MsqManUserDef2, IPGroup_SIPConnect,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 1 = 0, "Lync", 1, "195.189.192.158", "", 0, -1, -1, 0, -1, 0,
"MRLan", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", ", "", 0, "", ", 0, 0;
IPGroup 2 = 0, "TWCBC", 2, "195.189.192.158", "", 0, -1, -1, 0, -1, 1,
"MRWan", 1, 2, -1, -1, 4, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "",
"", "", 0, "", "", 0, 0;
[ \IPGroup ]
[ Account ]
FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup,
Account_ServingIPGroup, Account_Username, Account_Password,
Account_HostName, Account_Register, Account_ContactUser,
Account_ApplicationType;
Account 0 = -1, 1, 2, "19199732120", "$1$eCgYCQhISkZG4fTm6uu0tr75sLo=",
"107.14.112.4", 1, "19199732120", 2;
[ \Account ]
[ IP2IPRouting ]
FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType,
IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID,
IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting DestSRDID, IP2IPRouting DestAddress, IP2IPRouting DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 0 = "OPTIONS termination", 1, "*", "*", "*", "*", 6, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "Lync to TWCBC", 1, "*", "*", "*", "*", 0, "", -1, 0, -
1, 0, 2, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "TWCBC to Lync", 2, "*", "*", "*", "*", 0, "", -1, 0, -
1, 0, 1, "0", "", 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 0 = "Lync", "Voice", 2, 0, 0, 5067, 0, "", "", -1, 0, 500, -
1;
SIPInterface 1 = "TWCBC", "WANSP", 2, 5060, 0, 0, 1, "", "", -1, 0, 500,
-1;
[ \SIPInterface ]
[ IPOutboundManipulation ]
FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "Add +1", 0, 1, 2, "*", "*", "732", "*", "*",
"", 0, -1, 0, 1, 0, 0, 255, "+", "", 0;
[ \IPOutboundManipulation ]
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 1, "";
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 1, "";
[ \CodersGroup0 ]
[ MessageManipulations ]
FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations MessageType, MessageManipulations Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Remove opaque", 4, "any.request", "",
"header.from.url.param.opaque", 1, "", 0;
```

```
MessageManipulations 1 = "Host of Referred-by", 4, "any.request",
"header.referred-by exists", "header.referred-by.url.host", 2,
"header.from.url.host", 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 ]
```



Configuration Note



www.audiocodes.com