# Ribbon SBC Core R11.0 Interop with Zoom Phone Local Survivability : Interoperability Guide

## Table of Contents

# Interoperable Vendors

# Copyright

# Document Overview

This document outlines the configuration best practices for the Ribbon solution covering the Ribbon SBC Core when deployed with Zoom Phone Local Survivability (ZPLS).

## About Ribbon SBC Core

A Session Border Controller (SBC) is a network element deployed to protect SIP-based Voice over Internet Protocol (VoIP) networks. Early deployments of SBCs were focused on the borders between two service provider networks in a peering environment. This role has now expanded to include significant deployments between a service provider's access network and a backbone network to provide service to residential and/or enterprise customers.

The SBC Core (SBC 5K, 7K, SWe) addresses the next-generation needs of SIP communications by delivering embedded media transcoding, robust security, and advanced call routing in a high-performance, small form-factor device enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP Trunking, secure Unified Communications, and Voice over IP (VoIP).

The SBC Core provides a reliable, scalable platform for IP interconnect to deliver security, session control, bandwidth management, advanced media services, and integrated billing/reporting tools in an SBC appliance. This versatile series of SBCs can be deployed as peering SBCs, access SBCs, or enterprise SBCs (eSBCs). The SBC product family is tested for interoperability and performance against a variety of third-party products and call flow configurations in the customer networks.

⚠ SBC 5x10, 5400, 7000 and SWe are represented as SBC Core in the subsequent sections.

## About Zoom Phone Local Survivability (ZPLS)

Zoom Phone is a cloud-based service that is dependent on IP connectivity to Zooms datacenters. Customers that are using the Zoom Phone solution at corporate locations are encouraged to deploy redundant and reliable internet connectivity with sufficient bandwidth at each corporate office as a base requirement.

For certain business locations maintaining telephony service in the event of an outage is critical. Zoom can offer a survivability solution of basic telephony services in order to provide an additional layer of protection to ensure business continuity. An outage can be the result of an internet service failure at a business location or a failure in multiple Zoom datacenters that prevent client devices from reaching Zoom Phone components.

The Zoom Phone Local Survivability (ZPLS) module leverages the platform and Operating System (OS) provided by the Zoom Node and is distributed as a Linux-based appliance that is spun up on an on-premises VMware ESXi host. The ZPLS module does not affect the phone service during normal operations. Phone clients and devices in survivable Phone Sites register to the corresponding ZPLS module and are able to maintain a subset of Phone features when connectivity to Zoom Phone is lost. When connectivity to the Zoom Phone cloud returns, clients and devices re-register back to the cloud. During the outage, neither the administrator nor the end user is required to take any action to enable survivability. The failover and fallback process is seamless and automatic.

The interoperability compliance testing focuses on verifying inbound and outbound call flows between the Ribbon SBCCore& ZPLS.

This guide contains the following configuration sections:

- Section A: Ribbon SBC CoreConfiguration
  - Captures general SBC Core configurations for deploying SBC with ZPLS.
- Section B: Zoom Phone Local Survivability Configuration
  - Captures the Zoom Phone Local Survivability configuration.

## Non-Goals

It is not the goal of this guide to provide detailed configurations that will meet the requirements of every customer. Usethis guide as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

## Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring both the Ribbon SBCs and the third-party product.

To perform this interop, you need to:

- use the graphical user interface (GUI) or command line interface (CLI) of the Ribbon product.
- understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- have SIP/RTP/SRTP to complete the configuration and for troubleshooting.

**Note**
This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided AS IS. Users must take full responsibility for the application of the specifications and information in this guide.

## Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBCCore.
- Public IP Addresses.
- Zoom Go account - a special type of account where the Zoom user can be configured for ZPLS.
- TLS Certificatesfor Ribbon SBCCoresigned by one of the Zoom approved CA vendors.

## Product and Device Details

The sample configuration in this document uses the following equipment and software:

**Table 1:** Requirements

| | Appliance/Application/Tool | Software Version |
|---|---|---|
| **Ribbon Communications** | SBC SWe Core | V11.00.00-R001 |
| **Zoom** | Zoom Phone Local Survivability (ZPLS) | 1.8.0.73 |
| | Zoom Client | 5.11.10 (8200) |
| **PSTN Phone** | Jitsi | 2.10.5550 |

**Note**

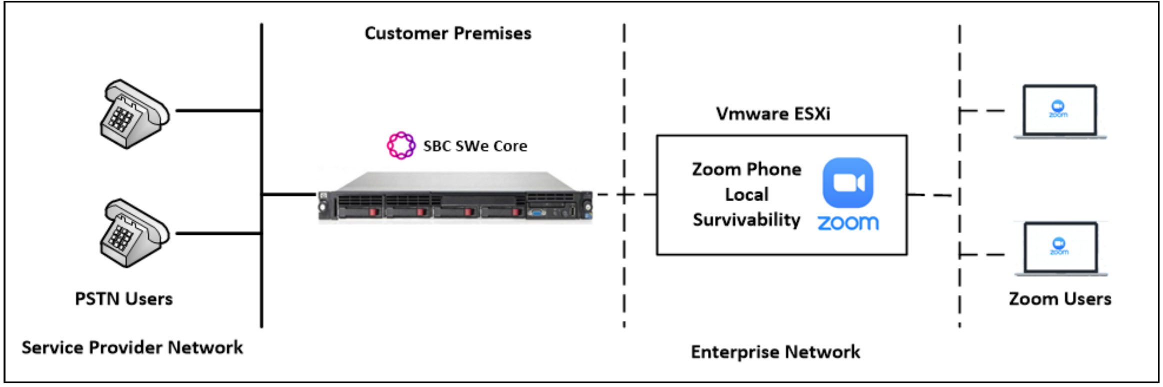
- ZPLS version is 1.8.0.73 or later.
- Zoom Client version is 5.11.10 (8200) or later.
- Jitsi version is 2.10.5550 or later

# Network Topology Diagram

This section covers the Ribbon SBC SWe Core deployment topology and the Interoperability Test Lab Topology.

## Deployment Topology

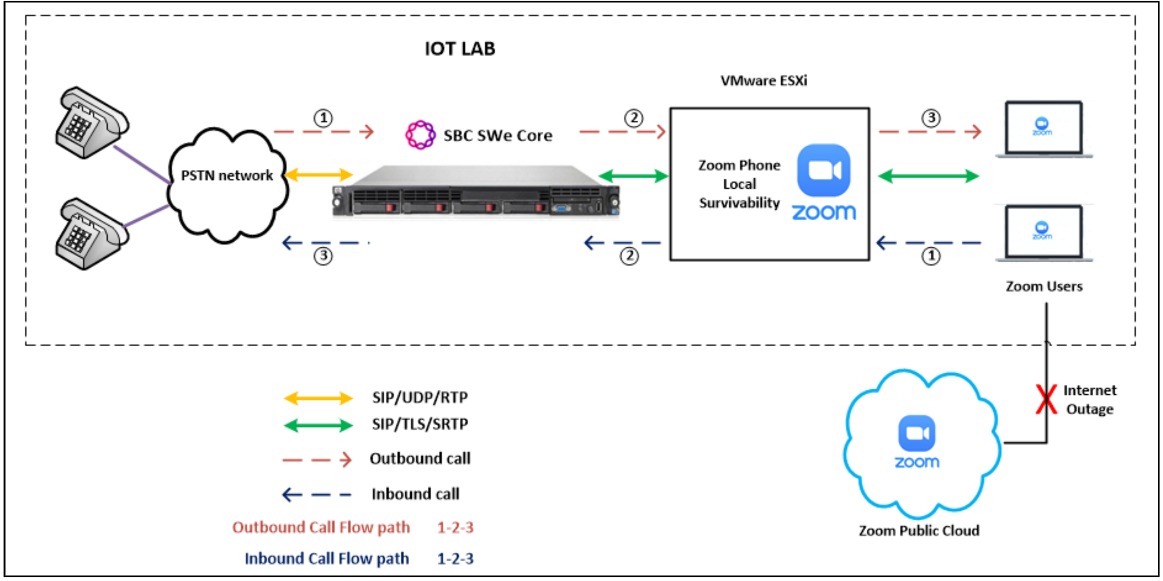
**Figure 1:** Ribbon SBC SWe Core Deployment Topology



## Interoperability Test Lab Topology

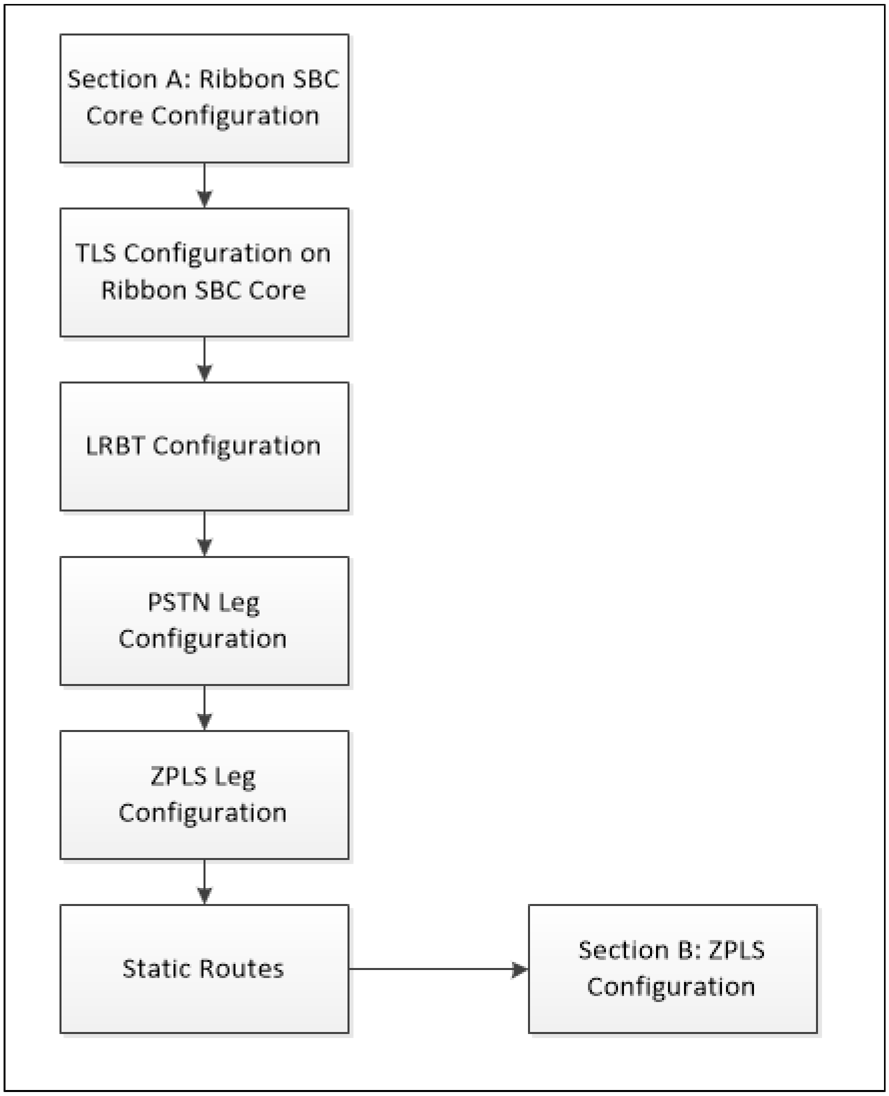
The following lab topology diagram shows connectivity between Ribbon SBC SWe Core on virtual platform and Zoom Phone Local Survivability.

**Figure 2:** SBC SWe Core and ZPLS interoperability Test Lab Topology



# Document Workflow

The sections in this document follow the sequence below. The reader is advised to complete each section for successful configuration.


Section A: Ribbon SBC Core Configuration
TLS Configuration on Ribbon SBC Core
LRBT Configuration
PSTN Leg Configuration
ZPLS Leg Configuration
Static Routes
Section B: ZPLS Configuration

# Section A: Ribbon SBC Core Configuration

The following SBC Core configurations are included in this section:

Network and Connectivity

Static Routes

TLS Configuration on Ribbon SBC Core

LRBT Configuration

PSTN Leg Configuration

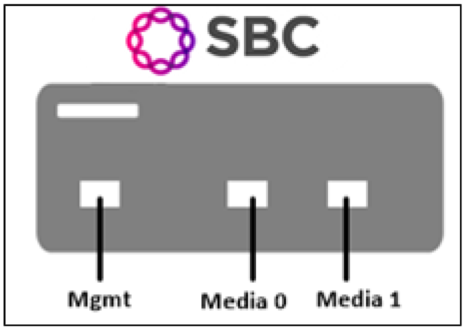
ZPLS Leg Configuration

- SBC Core can connect to the network as mentioned inNetwork and Connectivity.
- ZPLS prefers transport as TLS. Establishing a TLS connection between SBC SWe Core and ZPLS is covered under TLS Configuration on Ribbon SBC Core.
- SBC Core specific configuration related to PSTN Leg is covered under PSTN Leg Configuration.
- SBC Core specific configuration related to ZPLS Leg is covered under ZPLSLeg Configuration.

## Network and Connectivity

A Ribbon SBC is as shown below:

**Figure 3:** Ribbon SBC



**Mgmt**is an RJ45 port and is the management interface of the SBC.

**Media 0/Media1**depicted as pkt0/pkt1 are RJ45 OR optical SFP ports. Media 0 and Media 1 are used in the current deployment and the same interfaces can be used in SBC Core 5K and 7K (appliance based). Typically, on 5K/7K these ports would be optical SFPs.

For the SBC SWe (virtualized platform), the logical pkt0/pkt1 interface must be mapped to a physical port.

## Static Routes

Static routes are used to create communication to remote networks. In a production environment, static routes are mainly configured for routing from a specific network to a network that can only be accessed through one point or one interface (single path access or default route).

**Tip**

- For smaller networks with just one or two routes, configuring static routing is preferable. This is more efficient since a link is not wasted by exchanging dynamic routing information.
- For networks that have a LAN-side Gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with Voice VLAN towards SBC Core, static routing configurations are not required.

Add the static route once the PSTN Leg and ZPLS Leg configurations are done on the SBC.

### Static route towards PSTN

```
set addressContext default staticRoute 0.0.0.0 0 10.54.X.X LIF1 PKT0_V4 preference 100
commit
```

### Static route towards ZPLS

```
set addressContext default staticRoute 0.0.0.0 0 172.16.X.X LIF2 PKT1_V4 preference 100
commit
```

## TLS Configuration on Ribbon SBC Core

**Prerequisites:**

- For the TLS to work, a trusted CA (Certificate Authority) is needed. In this scenario, GoDaddy is used as a Trusted CA.
- Digicert Global Root CA and Digicert Global G2 is also required for TLS handshake.
- ZPLS is enabled with TLS/SRTP by default.

**Generate a CSRwith OpenSSL**

```
# To create a Certificate Signing Request (CSR) and key file for a Subject Alternative Name (SAN) certificate with
multiple subject alternate names, complete the following procedure:

Create an OpenSSL configuration file (text file) on the local computer by editing the fields to the company
requirements.

Note 1: In the example used in this article, the configuration file is req.conf.

Note 2: req_extensions will put the subject alternative names in a CSR, whereas x509_extensions would be used when
creating an actual certificate file.

[req]
        distinguished_name = req_distinguished_name
        req_extensions = v3_req
        prompt = no
        [req_distinguished_name]
        C = US
        ST = VA
        L = SomeCity
        O = MyCompany
        OU = MyDivision
        CN = www.company.com
        [v3_req]
        keyUsage = keyEncipherment, dataEncipherment
        extendedKeyUsage = serverAuth
        subjectAltName = @alt_names
        [alt_names]
        DNS.1 = www.company.com
        DNS.2 = company.com
        DNS.3 = www.company.net
        DNS.4 = company.net

Make sure there are no whitespaces at the end of the lines.

#Run the following commands to create the Certificate Signing Request (CSR) and a new Key file:
openssl req -new -out company_san.csr -newkey rsa:2048 -nodes -sha256 -keyout company_san.key.temp -config req.conf

#Run the following command to verify the Certificate Signing Request:
openssl req -text -noout -verify -in company_san.csr

#After receiving the CSR with the above information, provide it to CA (Certificate Authority). You will then
receive the proper CA signed certificate in .crt format that is convertable into other formats using openssl.

#By default, you should receive two or more certificates from CA (depanding upon your CA). One is the SBC
certificate, and the other is CA's root and intermediate certificate.

#Upload the certificates to the SBC at /opt/sonus/external and convert them into an SBC-readable format, i.e. SBC
certificate is in .pem or .p12 format and root certificate is in .cer or .der.

#Convert .crt to .pem USING OPENSSL for SBC certificate.
openssl x509 -in sbc_cert.crt -out sbc_cert.der -outform DER
openssl x509 -in sbc_cert.der -inform DER -out sbc_cert.pem -outform PEM

#After generating sbc_cert.pem file, convert it to .p12 format using the command below and the location of the
certificate key.
openssl pkcs12 -export -out sbc1_cert.p12 -in sbc_cert.pem -inkey /opt/sonus/company_san.key.temp

#CONVERTING CRT to CER USING OPENSSL for CA's root and intermediate certificate.
openssl x509 -in root_cert.crt -out root_cert.cer -outform DER

After converting all these certificates, upload them on SBC at /opt/sonus/external location.
```

## Import the Required Certificates into SBC

```
#Import Public CA Root Certificate into database.
set system security pki certificate CA_ROOT_CERT type remote fileName root_cert.cer state enabled

#Import Public CA Certified SBC Server Certificate into database.
set system security pki certificate SBC_CERT filename sbc1_cert.p12 passPhrase <Password defined during CSR
generation> state enabled type local

#Import Public Digicert Global Root CA Certificate into database.
set system security pki certificate DIGI_ROOT type remote fileName DigiCertGlobalRootCA.crt state enabled

#Import Public Digicert Global G2 Certificate into database.
set system security pki certificate DIGI_ROOT_G2 type remote fileName DigiCertGlobalRootG2.pem state enabled
```

#### TLS Profile

A TLS Profile is required for the TLS handshake between SWe Core and ZPLS. This profile defines cipher suites supported by SWe Core. Create the TLS profile as mentioned below:

```
set profiles security tlsProfile TLS_PROF clientCertName SBC_CERT serverCertName SBC_CERT cipherSuite1
tls_ecdhe_rsa_with_aes_256_cbc_sha384 cipherSuite2 tls_ecdhe_rsa_with_aes_128_cbc_sha authClient true allowedRoles
clientandserver acceptableCertValidationErrors invalidPurpose
set profiles security tlsProfile TLS_PROF v1_1 enable
set profiles security tlsProfile TLS_PROF v1_0 disable
set profiles security tlsProfile TLS_PROF v1_2 enable
commit
```

Attach the TLS Profile to the SIP Signaling Port that will be created later in ZPLS Leg Configuration.

```
set addressContext default zone ZOOM sipSigPort 7 state disabled mode outOfService
commit
set addressContext default zone ZOOM sipSigPort 7 tlsProfileName TLS_PROF
commit
set addressContext default zone ZOOM sipSigPort 7 state enabled mode inService
commit
```

## LRBT (Local Ring Back Tone) Configuration

This section contains the general SBC configurations.

#### DSP Resource Allocation

This configuration only applies if the SBC has been deployed with (hardware) DSP resources. If it has not, executing this configuration step has no negative impact. Do not attempt transcoding, so that the lack of compression resources will not impact the overall SBC configuration in this document.

```
set system mediaProfile compression 75 tone 25
commit
```

This configuration is not required for SBC SWe 7.2 release onwards.

#### Local Ringback Tone (LRBT) Profile

- Create a Local Ringback Tone (LRBT) profile that is attached to both PSTN and Zoom leg.
- Enable Dynamic LRBT.

```
set profiles media toneAndAnnouncementProfile LRBT_PROF
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone signalingTonePackageState enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone precedence lower
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone makeInbandToneAvailable enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags useThisLrbtForEgress enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags useThisLrbtForIngress enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags dynamicLRBT enable
commit
```

## PSTN Leg Configuration

Create profiles with a specific set of characteristics corresponding to PSTN. This includes configuration of the following entities on PSTN leg:

Codec Entry

Packet Service Profile

IP Signaling Profile

IP Interface Group

Zone

SIP Signaling Port

IP Peer

SIP Trunk Group

Routing Label

Call Routing

### Codec Entry

Codec entry allows you to specify the codec used for the call.Create the codec entry for G711Ulaw codec with packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711ULAW codec g711
set profiles media codecEntry G711ULAW law ULaw
set profiles media codecEntry G711ULAW packetSize 20
set profiles media codecEntry G711ULAW dtmf relay rfc2833
commit
```

### Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the PSTN leg. The PSP is attached to sipTrunkGroup created later in this section.

```
set profiles media packetServiceProfile PSTN_PSP codec codecEntry1 G711ULAW
set profiles media packetServiceProfile PSTN_PSP rtcpOptions rtcp enable
commit
```

### IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards PSTN.

```
set profiles signaling ipSignalingProfile PSTN_IPSP
set profiles signaling ipSignalingProfile PSTN_IPSP egressIpAttributes flags disable2806Compliance enable
commit
```

### IP Interface Group

Create an IP interface group.

Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards PSTN (example pkt0 IP), and "Y" with its prefix length. Provide ceName used during an SBC deployment.

Here the ceName is "ZPLS1".

```
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 ceName ZPLS1 portName pkt0
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 mode inService state enabled
commit
```

### Zone

Create the Zone towards PSTN and specify the id of the Zone.

This Zone groups the set of objects used for the communication towards PSTN.

```
set addressContext default zone PSTN id 2
commit
```

### SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

Replace "x.x.x.x" with SIP Signaling Port IP of SBC towards PSTN.

```
set addressContext default zone PSTN sipSigPort 3 ipInterfaceGroupName LIF1
set addressContext default zone PSTN sipSigPort 3 ipAddressV4 x.x.x.x
set addressContext default zone PSTN sipSigPort 3 portNumber 5060
set addressContext default zone PSTN sipSigPort 3 transportProtocolsAllowed sip-udp
set addressContext default zone PSTN sipSigPort 3 mode inService
set addressContext default zone PSTN sipSigPort 3 state enabled
commit
```

### IP Peer

Create an IP Peer with the signaling IP address of the PSTN (Service Provider) and assign it to the PSTN Zone.

Replace "x.x.x.x" with the PSTN IP.

```
set addressContext default zone PSTN ipPeer PSTN_IPP ipAddress x.x.x.x
set addressContext default zone PSTN ipPeer PSTN_IPP ipPort 5060
commit
```

### SIP Trunk Group

Create a SIP Trunk Group towards the PSTN and assign corresponding profiles like LRBT, PSP, IPSP created in earlier steps.

You must configure Trunk Group names using capital letters.

```
set addressContext default zone PSTN sipTrunkGroup PSTN_TG media mediaIpInterfaceGroupName LIF1
set addressContext default zone PSTN sipTrunkGroup PSTN_TG mode inService state enabled
commit

set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy signaling ipSignalingProfile PSTN_IPSP
set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy media packetServiceProfile PSTN_PSP
set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy media toneAndAnnouncementProfile LRBT_PROF
set addressContext default zone PSTN sipTrunkGroup PSTN_TG ingressIpPrefix 0.0.0.0 0
commit
```

### Routing Label

Create a Routing Label with a single Routing Label Route to bind the the PSTN Trunk Group with the PSTN IP Peer.

```
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 trunkGroup PSTN_TG
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 ipPeer PSTN_IPP
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 inService inService
commit
```

### Call Routing

This entry is used to route all the calls coming from PSTN towards ZOOM endpoints.

> Provide ceName used during an SBC deployment. "ZPLS1" is the ceName.

```
set global callRouting route trunkGroup PSTN_TG ZPLS1 standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel ZOOM_RL
commit
```

## ZPLS Leg Configuration

Create profiles with a specific set of characteristics corresponding to Zoom. This includes configuration of the following entities on ZPLS leg:

Codec Entry

Packet Service Profile

IP Signaling Profile

IP Interface Group

Zone

SIP Signaling Port

IP Peer

SIP Trunk Group

Routing Label

Call Routing

### Codec Entry

Codec entry allows you to specify the codec used for the call.Create the codec entry for G711Ulaw codec with packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711_Zoom codec g711
set profiles media codecEntry G711_Zoom law ULaw
set profiles media codecEntry G711_Zoom packetSize 20
set profiles media codecEntry G711_Zoom dtmf relay rfc2833
commit
```

## Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the ZPLS leg. The PSP is attached to the sipTrunkGroup that is created later in this section.

Since there is an SRTP between the SBC Core and Zoom, you must create a crypto suite profile.

```
set profiles security cryptoSuiteProfile CRYPT_PROF entry 1 cryptoSuite AES-CM-128-HMAC-SHA1-80
```

The Crypto Suite profile is attached to the ZOOM_PSP.

```
set profiles media packetServiceProfile ZOOM_PSP codec codecEntry1 G711_Zoom
set profiles media packetServiceProfile ZOOM_PSP rtcpOptions rtcp enable
set profiles media packetServiceProfile ZOOM_PSP secureRtpRtcp cryptoSuiteProfile CRYPT_PROF
set profiles media packetServiceProfile ZOOM_PSP secureRtpRtcp flags allowFallback enable
set profiles media packetServiceProfile ZOOM_PSP secureRtpRtcp flags enableSrtp enable
commit
```

## IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards Zoom.

- The SBC Core to Zoom transport type is TLS and therefore enables the same transport type in ZOOM_IPSP.
- ZPLS expects the transport type in Contact header, hence the flag "includeTransportTypeInContactHeader" need to be enabled.

```
set profiles signaling ipSignalingProfile ZOOM_IPSP
set profiles signaling ipSignalingProfile ZOOM_IPSP egressIpAttributes flags disable2806Compliance enable
set profiles signaling ipSignalingProfile ZOOM_IPSP egressIpAttributes numberGlobalizationProfile DEFAULT_IP
set profiles signaling ipSignalingProfile ZOOM_IPSP egressIpAttributes transport type1 tlsOverTcp
set profiles signaling ipSignalingProfile ZOOM_IPSP commonIpAttributes flags includeTransportTypeInContactHeader
enable
commit
```

## IP Interface Group

Create an IP interface group.

Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards ZOOM (example pkt1 IP), and "Y" with its prefix length. Provide the ceName used during an SBC deployment.

Here the ceName is "ZPLS1".

```
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ceName ZPLS1 portName pkt1
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 mode inService state enabled
commit
```

## Zone

Create a Zone towards Zoom and specify the id of the zone.

This Zone groups the set of objects used for communication towards Zoom.

```
set addressContext default zone ZOOM id 6
commit
```

## SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

Replace "x.x.x.x" with the SIP Signaling Port IP address of the SBC towards ZPLS.

```
set addressContext default zone ZOOM sipSigPort 7 ipInterfaceGroupName LIF2
set addressContext default zone ZOOM sipSigPort 7 ipAddressV4 x.x.x.x
set addressContext default zone ZOOM sipSigPort 7 portNumber 5060
set addressContext default zone ZOOM sipSigPort 7 tlsProfileName TLS_PROF
set addressContext default zone ZOOM sipSigPort 7 transportProtocolsAllowed sip-tls-tcp
set addressContext default zone ZOOM sipSigPort 7 mode inService
set addressContext default zone ZOOM sipSigPort 7 state enabled
commit
```

You created the TLS profile inTLS Profile.

There are a few areas that result in a TLS negotiation issue. One area involves assigning the incorrect port.Ensure the following are accomplished:

- Zoom listens on port number 5061 (default setting).
- Configureport number 5060 on Zoom IP-Peer since Ribbon SBC Coreincrements the port by 1 when the transport protocol is TLS.

## IP Peer

Create an IP Peer with the signaling IP address of ZOOM and assign it to the ZOOM Zone.

Replace "x.x.x.x" with the Zoom SIP signaling IP.

```
set addressContext default zone ZOOM ipPeer ZOOM_IPP ipAddress x.x.x.x
set addressContext default zone ZOOM ipPeer ZOOM_IPP ipPort 5060
commit
```

### Path Check Profile

Create a path check profile that attaches to the Zoom side.

```
set profiles services pathCheckProfile ZOOM_OPTIONS protocol sipOptions sendInterval 20 replyTimeoutCount 1
recoveryCount 1
set profiles services pathCheckProfile ZOOM_OPTIONS transportPreference preference1 tls-tcp
commit
```

## SIP Trunk Group

Create a SIP Trunk Group towards ZPLS and assign corresponding profiles like LRBT, PSP, IPSP that were created in earlier steps.

You must configure Trunk Group names using capital letters.

```
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG media mediaIpInterfaceGroupName LIF2
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG mode inService state enabled
commit

set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG policy signaling ipSignalingProfile ZOOM_IPSP
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG policy media packetServiceProfile ZOOM_PSP
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG policy media toneAndAnnouncementProfile LRBT_PROF
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG ingressIpPrefix 0.0.0.0 0
commit
```

### Routing Label

Create a Routing Label with a single Routing Label Route to bind the ZOOM Trunk Group with the ZOOM IP Peer.

```
set global callRouting routingLabel ZOOM_RL routingLabelRoute 1 trunkGroup ZOOM_TG
set global callRouting routingLabel ZOOM_RL routingLabelRoute 1 ipPeer ZOOM_IPP
set global callRouting routingLabel ZOOM_RL routingLabelRoute 1 inService inService
commit
```

### Call Routing

This entry is used to route all the calls coming from Zoom towards PSTN endpoints.

> Provide the ceName used during an SBC deployment. "ZPLS1" is the ceName.

```
set global callRouting route trunkGroup ZOOM_TG ZPLS1 standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel PSTN_RL
commit
```

## Section B: Zoom Phone Local Survivability Configuration

For configuring both Zoom Phone System and Zoom Phone local Survivability, refer to the following link:

https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin.

## Supplementary Services and Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

| Sr. No. | Supplementary Features/Services | Coverage |
|---|---|---|
| 1 | Internal Extension Dialing | ✓ |
| 2 | Dial By Name | ✓ |
| 3 | Dial From Call History | ✓ |
| 4 | OPTIONS ping (SBC to ZPLS) | ✓ |
| 5 | OPTIONS ping (ZPLS to SBC) | ✓ |
| 6 | Basic Call from PSTN to Zoom | ✓ |
| 7 | Basic Call from Zoom to PSTN | ✓ |
| 8 | Call Hold & Call Resume | ✓ |
| 9 | Mute/Unmute | ✓ |
| 10 | DTMF (RFC 2833) | ✓ |

| | | |
|---|---|---|
| 11 | Blind/Unattended Transfer | ✓ |
| 12 | Consultative/Attended Transfer | ✓ |
| 13 | Call Park & Retrieve | ✓ |
| 14 | Adhoc 3-Party Conference | ✓ |

**Legend**

| | |
|---|---|
| ✓ | Supported |
| ✗ | Not Supported |
| **N/A** | Not Applicable |

# Support

For any support related queries about this guide, contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website:https://ribboncommunications.com/services/ribbon-support-portal

# References

For detailed information about Ribbon products & solutions, go to:

https://ribboncommunications.com/products

For information about Zoom products & solutions, go to:

https://zoom.us

# Conclusion

This Interoperability Guide describes a successful configuration of the Zoom Phone Local Survivability interoperability with Ribbon SBC Core.

All features and capabilities tested are detailed within this document - any limitations, notes, or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there may be additional configuration changes required to suit the exact deployment environment.