Ribbon G5 Line Access Gateway R4.7 Interop with Zoom : Interoperability Guide

Table of Contents

Interoperable Vendors

ZOOM

Copyright

Document Overview

This document outlines the configuration best practices for the Ribbon solution covering the Ribbon G5 Line Access Gateway when deployed with Zoom.

The Ribbon G5 system is a Line Access Gateway (LAG) that provides high-density, low cost Plain Old Telephone Server (POTS) subscriber interfaces over copper pairs. The G5 system provides telephony interfaces to subscribers connected directly to the G5.

This guide contains the following configuration sections:

- Section A: Zoom Configuration
    - Captures the Zoom configuration.

- Section B: Ribbon G5 Configuration
    - Captures general G5 configurations for deploying with Zoom.

Non-Goals

It is not the goal of this guide to provide detailed configurations that will meet the requirements of every customer. Use this guide as a starting point and build the Ribbon G5 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 G5 and the third-party product.

To perform this interop, you need

- to use graphical user interface (GUI) or command line interface (CLI) of the Ribbon product
- to understand the basic concepts of TCP/UDP/TLS and IP/Routing
- to 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 G5 Line Access Gateway (LAG)
- Public IP Addresses
- Zoom Go account - a special type of Zoom account that has the option of Phone System Management
- TLS Certificates for Ribbon SBC Core signed by one of Zoom's approved CA vendors

Product and Device Details

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

Table 1: Requirements

	Equipment/Device	Software Version
Ribbon Communications	Ribbon G5 LAG	4.7.07
Zoom	Zoom Desktop app	5.9.3(3169)
	Zoom Mobile app	5.9.3(4247)

> ⓘ **Note**
>
> - Zoom Desktop app version is 5.9.3 (3169) or later.
> - Zoom Mobile app version is 5.9.3 (4247) or later.

Network Topology Diagram

This section covers the Ribbon G5 LAG deployment topology and the Interoperability Test Lab Topology.

Ribbon G5 Deployment Topology

Figure 1: Ribbon G5 Deployment Topology
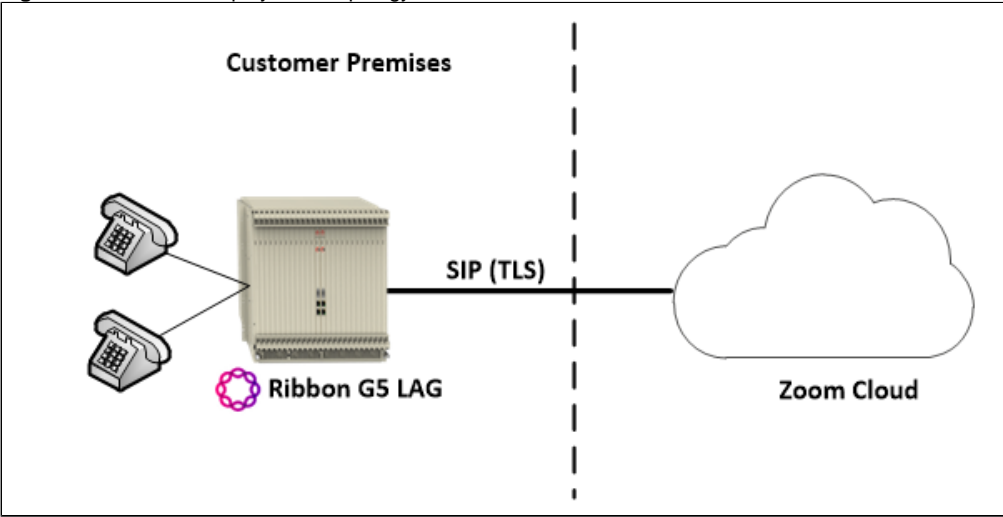
Interoperability Test Lab Topology

The following lab topology diagram shows connectivity between Zoom and Ribbon G5 LAG.

Figure 2: Interoperability Test Lab Topology

IOT lab

Zoom Desktop App

Polycom VVX 300

Internet

Zoom Cloud
162.12.X.X

Public network (internet)

IOT lab

Ribbon G5 LAG

115.110.X.X

① ② ③
③ ② ①

SIP TLS SRTP
Inbound call
Outbound call
IOT lab

Inbound Call Flow path   1-2-3
Outbound Call Flow path   1-2-3

Section A: Zoom Configuration

This section provides instructions on how to configure a SIP Endpoint in a Zoom Web Portal (does not include steps for configuring Vendor Endpoint specifically).

To register a SIP Endpoint to Zoom Phone, start by creating a new common area phone in the Zoom web portal. See the Zoom support site for more information.

1. **Sign in** to the Zoom web portal.
2. Click **Phone system management** > Users & Rooms.
3. Click the **Common Area Phones or Phones & Devices** tab.
4. Click **Add** and enter the following information:
    a. **Site** (only visible if you have multiple sites): Select the site you want the device to belong to.
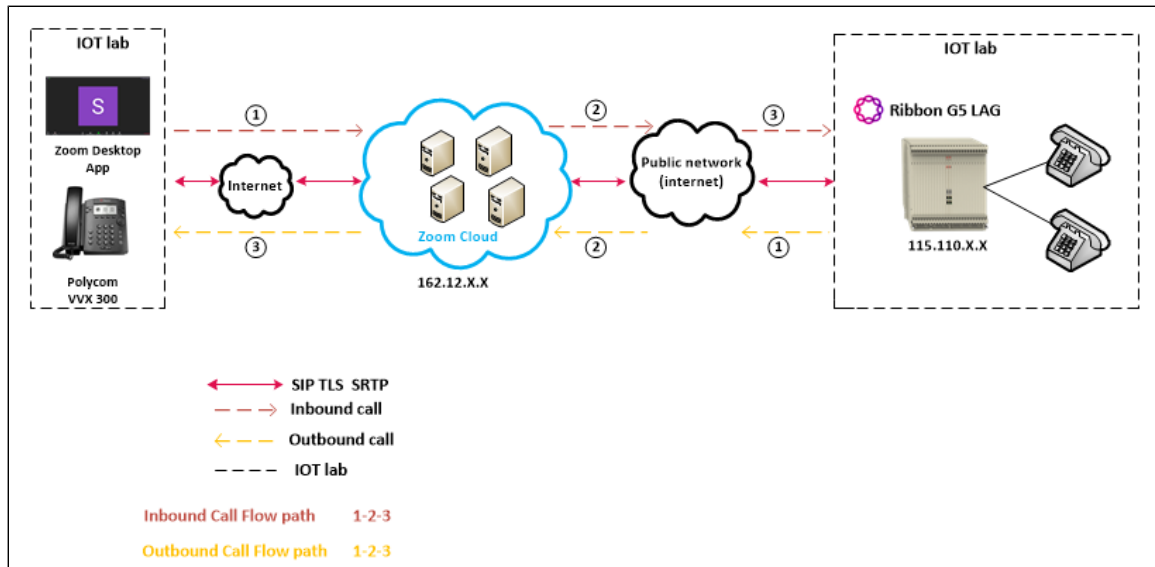   b. **Display Name**: Enter a display name to identify the device.
    c. **Description (Optional)**: Enter a description to help you identify the location of the device.
    d. **Extension Numbe**r: Enter an extension number to assign to the device.
    e. **MAC Address**: Enter the 12-digit MAC address of the Endpoint. The MAC can be found on the product label.
    f. **Device Type**: Select **Other**.
    g. **Emergency Address** (only visible if you don't have multiple sites): Select an emergency address to assign to the desk phone. If you selected a site for a common area phone, the site's emergency address will be applied to the phone.
    h. Click **Save.**
    i. Click **Provision** to view the SIP credentials. You will need this information to complete the provisioning.

⚠️ By default, support for a generic SIP profile is not enabled. If you don't have the **Other** option, contact your Zoom sales representative.

Section B: Ribbon G5 Configuration

This section provides instructions on how to configure a Vendor's SIP Endpoint (does not include steps for configuring in Zoom Web Portal).

The Ribbon G5 system is a Line Access Gateway (LAG) that provides high-density, low cost Plain Old Telephone System (POTS) subscriber interfaces over copper pairs. The G5 system provides telephony interfaces to subscribers connected directly to the G5.

The G5 shelf is a single 23" wide, 10 rack unit (RU) high shelf. The shelf includes a chassis, backplane, optional fan module, and 26 card slots which can be equipped as follows:

- Universal Slots:
    - 24 slots which support a variety of card types for services, subscribers, and network connections.
    - The Universal Slots (which are indicated by grey card guides on the chassis) house the POTS-32 cards.
    - The POTS-32 card provides standard POTS telephony service for up to 32 subscribers.
- Controller/Trunk (CT) Slots:
    - 2 slots which provide redundancy and support the main coordinating processor on the G5 system, as well as a variety of other central or common functions.
    - The Controller/Trunk Slots (which are indicated by red card guides on the chassis) house the CTG (Controller Trunk Gateway) cards.
    - The CTG cards provide VoIP north-bound interface capability.

1. G5 SIP using the CTG Cards

The Controller Trunk Gateway card, referred to as the CTG card, also implements the common control mechanism for providing narrowband services. When you install two CTG cards, one is active and the other is standby in a 1:1 redundant pair.

Figure 3: G5 SIP using the CTG cards
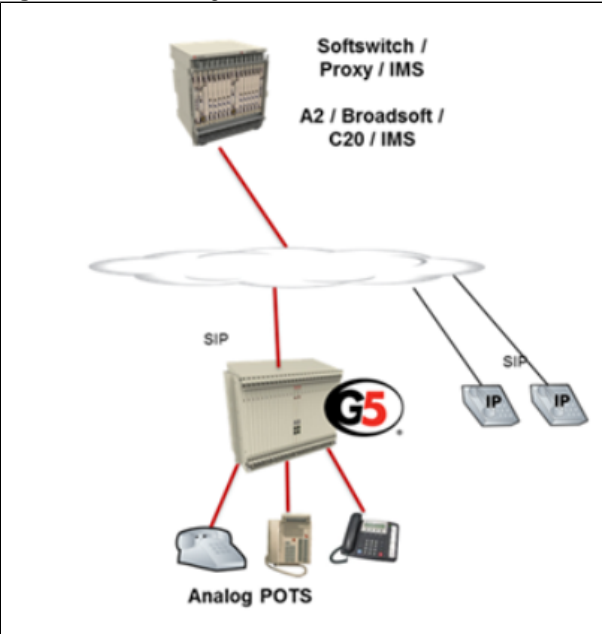
The G5 uses Transaction Language 1 (TL1) protocol for provisioning and commissioning. TL1 is used in the input and output messages that pass between the Operating System (OS) and Network Element (NE). TL1 is defined in the Telecordia Technologies (formally Bellcore) Generic Requirements document GR-831-CORE.

The TL1 language consists of a set of messages. The TL1 messages follow a fixed structure and all commands must conform to that structure. TL1 commands for the G5 conform to the following syntax: a:b:c:d::[p];

The table below describes the TL1 command syntax:

TL1 Command Syntax	
Parameter	Description
a	TL1 Command Code
b	Target Identifier (TID) or System Identifier (SID) – Unique name assigned to each system when it is installed. The recommended value is the Common Language Location Identifier (CLLI) for the system. The TID can have a maximum of 20 ASCII characters. A null TID (that is, successive colons) can be used when the OS communicates directly with the Network Element.

c	Access Identifier (AID) or User Identifier (UID) – Represents code used to identify specific components within the 5000LF (that is, shelf - slot)
d	Correlation Tag (CTAG) – Unique identifier assigned to each input command by the user. When the 5000LF system responds to a command, it includes the command's CTAG in the reply. Valid CTAG values can be up to 6 characters or decimal numerals with an optional non-trailing ".". Note: CTAG is required when inputting a command and the same value is displayed in the output. The same CTAG value does not have to be used with each command input.
p	Parameter (Payload) block – The TID(SID), AID (UID), and CTAG route and control the TL1 command, while the optional parameter block provides any information required to complete the action requested by the command.
;	Terminates each command. Note: A command is immediately processed when a semicolon (;) is typed; there is no need to press ENTER.

2. Connecting a PC/Laptop to a G5 System

Each CTG card has two Ethernet connectors and one RS-232 serial port connector on the faceplate of the card to connect to external equipment. The Ethernet connector labeled "CRAFT" is a 10/100BaseT connector and the Ethernet connector labeled "NETWORK" is a 10/100/1000BaseT connector.

The G5 System has two administrative software interfaces: a TL1 interface and a Web-based interface. This method will focus on the primary interface, which is the TL1 interface.

1. Using an RS-232 cable connected between the console terminal on the Laptop/PC and the DB9 serial port on the front of the active CTT/CTG card, access the Terminal Emulation Program (that is, Tera Term).

[Start] > [Programs] > [Tera Term] > [Tera Term]

> ⚠
> 1. The active CTT or CTG card will have its STATUS LED on the front of the card illuminated (Green).
> 2. If required, disconnect the Ethernet cables from the NETWORK or CRAFT port connectors on the front of both of the CTT cards.

2. Open the console connection and set up the serial port connection with the following parameters:

Setup > Serial Port (Tera Term)

Bit per Second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow Control: None

> ⚠ If Tera Term is not available, use another terminal emulation program such as Putty or Secure CRT.

3. Click OK.

```
cttf50001lf login:
```

4. Enter the following at the Linux login prompt and press Enter.

```
cttf50001lf login: tl1s

password: tl1s
```

⚠️ TL1S in lowercase - case sensitive.

5. Press the semicolon (;) key a few times to verify that the system is responding.

⚠️ If you are connected to the active CTT/CTG card, the [ ] prompt will be displayed. If the [*] prompt is displayed, you are connected to the standby CTT/CTG card and the console cable needs to be switched.

6. Log into the TL1 interface with the default username/password (SUPERUSER/ADMIN.5).

```
[ ] ACT-USER:: SUPERUSER:<ctag>::ADMIN.5;

Example Observation:

[] ACT-USER::SUPERUSER:9::*******;

  5000LF 10-11-19 00:37:31
M 9 COMPLD
  "SUPERUSER:2010-11-18,23-42-16,0,NO,"
  /* WARNING: AUTHORIZED USE ONLY. VIOLATORS WILL BE PROSECUTED! */
```

⚠️
    1. When logging onto the G5, the password will be masked with asterisks (***) as shown in the example observation above.

    2. Commands to log in should be entered using lower-case because the password is lowercase by default.

7. Proceed to Procedure 2.

Accessing the TL1 interface via Ethernet Port

8. Connect a straight-thru Ethernet cable between an Ethernet port on the Laptop/PC and the CRAFT port on the front of the active CTT card.

⚠️ The active CTT card will have its STATUS LED on the front of the card illuminated (Green).

9. Navigate to the TCP/IP settings on the Laptop/PC and change the network settings to a value within the same subnet as the default settings on the G5.

Example Network Settings for Laptop/PC:

IP Address: 192.168.1.12

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

⚠️ The 5000LF has the following default network settings:

    IP Address: 192.168.1.11

    Subnet Mask: 255.255.255.0

    Gateway: 192.168.1.254

10. Using your terminal emulation program, establish a ssh session with the G5 using the default IP Address and TL1 interface listening port.

HostName (or IP Address): [192.168.1.11]

```
ssh tl1s@192.168.1.11
```

11. Press the semicolon (;) key a few times to verify that the system is responding.

⚠ The [ ] prompt will be displayed indicating a connection to the active CTT card.

12. Log into the TL1 interface with the default username/password (SUPERUSER/ADMIN.5).

```
[ ] ACT-USER:: SUPERUSER:<ctag>::ADMIN.5;

Example Observation:
[] ACT-USER::SUPERUSER:9::*******;

   5000LF 10-11-19 00:37:31
M 9 COMPLD
   "SUPERUSER:2010-11-18,23-42-16,0,NO,"
   /* WARNING: AUTHORIZED USE ONLY. VIOLATORS WILL BE PROSECUTED! */
```

⚠
1. For the CTAG value, enter a desired value. For example, a CTAG entry of 9 has been used in the example observation. The same CTAG value does not have to be used with each command input. Reference Table 3 of this Interoperability Guide. The CTAG is not included in the specbook.
2. When logging onto the G5, the password will be masked with asterisks (***) as shown in the example observation above.

End of procedure. Continue to "G5 Initial Provisioning".

3. Performing G5 Initial Provisioning Procedure

Perform the following procedure for initial provisioning.

1. Using your web browser, log into the G5 Web interface with default credentials.

- Use URL http://<G5 IP Address>
- Username = admin
- Password = 4on1o5W [that's a one]
- Select OK

2. Create a new folder titled "g5lag" and transfer the new G5 SIP load from an FTP server. Move the folder to the C directory on the laptop. Record the path name for use in step 7.

3. If using the laptop as an FTP server, obtain the IP address of the network. From the Windows(R) "cmd" prompt, enter ipconfig. Record the IPv4 Address for use in step 7.

```
C:\Windows\system32\cmd.exe

   Connection-specific DNS Suffix  . : genband.com
   Link-local IPv6 Address . . . . . : fe80::69f8:28a2:78d4:194c%12
   IPv4 Address. . . . . . . . . . . : 172.16.28.72
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.16.28.1
```

4. Click on the SOFTWARE link under Update in the upper left hand corner of the Web page.

Figure 4: Software Update

5. Enter the following required information to download the software:

- FTP Server IP address = <172.16.28.72> [Note: This is the IP address of the laptop used for the FTP Server.]
- Path name of image file = </g5lag/3.1.00.83/3.1.00.83.tgz> [Note: This is the path to the folder on the C drive.]
- User Name = <ftp User Name>
- Password = <ftp User Password>
- Confirm password = <ftp User Password> or
- Check the Anonymous FTP box for anonymous login.
- Click the Update button.

Figure 5: FTP server

6. When the Software download on the system completes, a window asking to select the **Swap** button will appear:

Figure 6: Swap button
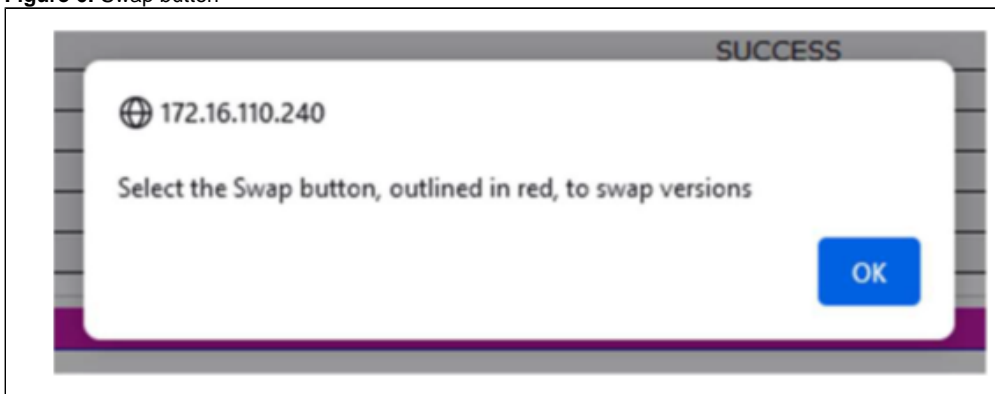
Select OK.

Figure 7: Swap
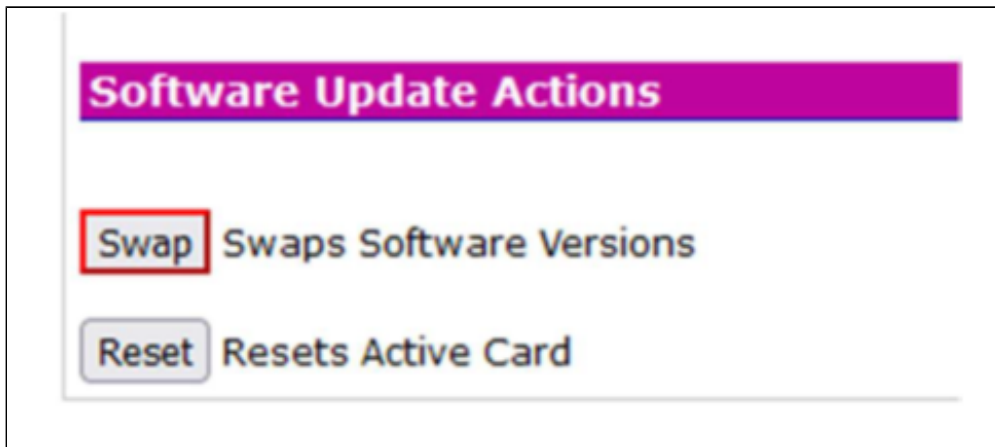
> ⚠ When you select the **Swap**, button the active CTG card loads the new software and the standby CTG card reboots.
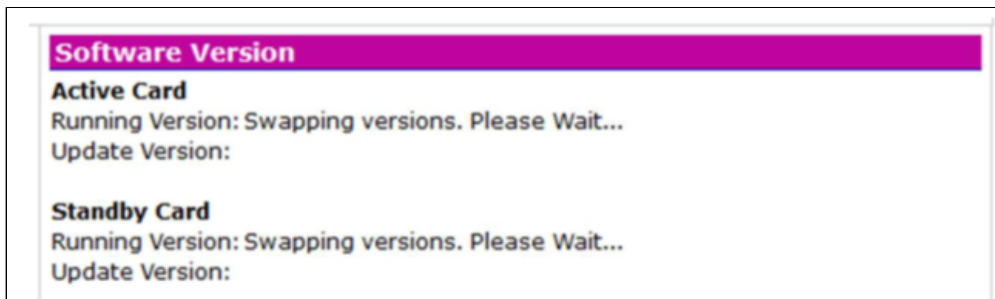
7. After the Standby CTG card reboots, a window asking to click the Reset to complete the Update appears:

Figure 8: Reset
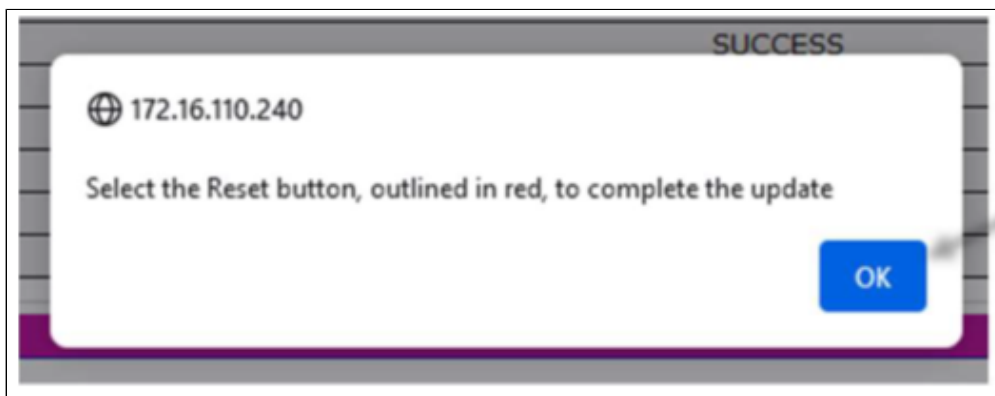
Select OK, then select the Reset button.

Software Update Actions

Swap — Swaps Software Versions

Reset — Resets Active Card

After the Active CTG reboots, log into the GUI once again as in step 1 and verify the Software Running Version for both the Active and the Standby match and are correct version as loaded. (Example: running version 4.7.07.00 and Update version is 4.6.25.00.)
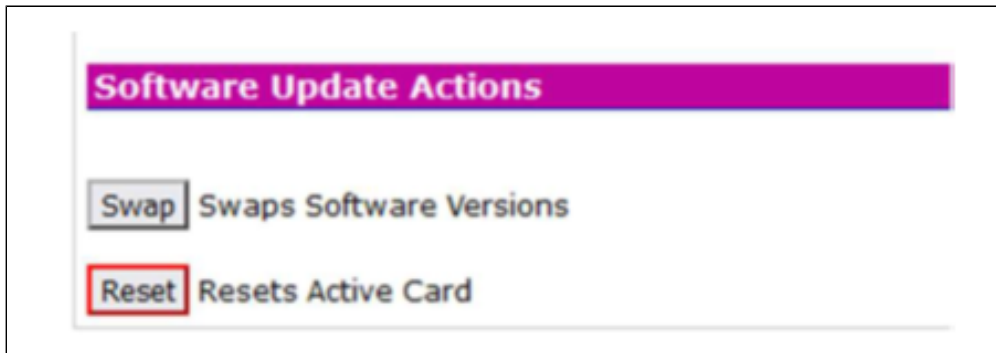
Figure 9: software update

Software Version

Active Card
Running Version: 4.7.03.00
Update Version: 4.6.25.00

Standby Card
Running Version: 4.7.03.00
Update Version: 4.6.25.00
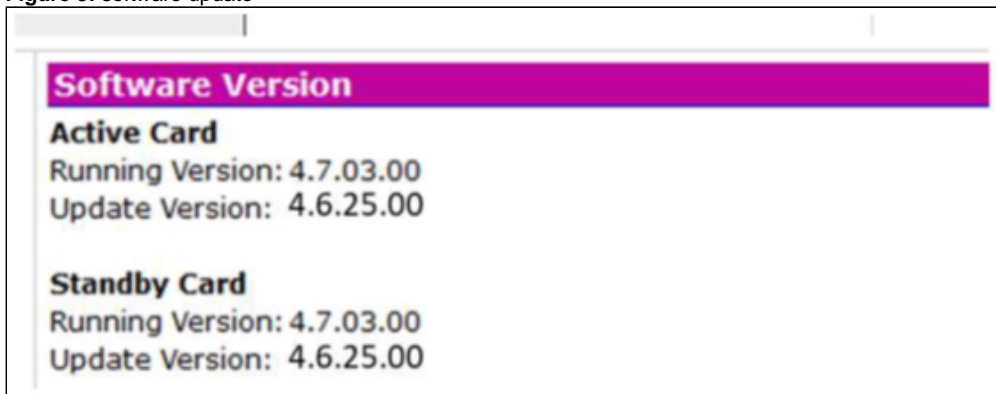
> ⚠ After the CTs are updated, the POTS cards will automatically update individually to the new load. This can take a few minutes to complete.

Exit the Web interface by closing the browser session.

8. Log back into the G5 as SUPERUSER.

```
[  ] ACT-USER:: SUPERUSER:<ctag>::ADMIN.5;
```

9. Enter the following at the Linux login prompt and press Enter.

```
cttf50000lf login: tl1s
password: tl1s
```

> ⚠ tl1s in lowercase - case sensitive

10. Log back into the G5 as SUPERUSER.

```
[  ] ACT-USER:: SUPERUSER:<ctag>::ADMIN.5;
```

11. After the CTG and POTS cards are updated, issue a RTRV-EQPT command and verify that all of the cards in the system are in service (IS) and that the software is displayed correctly.

- ```
       Enter: RTRV-EQPT:::9;
  ```

The correct software load should be displayed for each card in the equipment list. In this example, "AP=3.1.00.07" should appear in the card information for CTA, CTB, and the POTS cards.

12. Set the system date and time via NTP Server. Note: Proceed to the next step if the NTP Server is not available. Reference the Network Engineering Specbook for Site Requirements.

```
[G5] ED-DAT:::<ctag>:::SOURCE=<NTP>, TZ=<timezone>, NTP1=<NTP1 IP Addr>, NTP2=<NTP2 IP Addr>, NTP3=<NTP3 IP Addr>,
NTP4=<NTP4 IP Addr>;
```

⚠️
    1. If source = NTP, up to four (4) NTP servers may be configured for a G5; NTP1 is required and NTP2 through NTP4 are optional. If NTP2 through NTP4 are not required, enter 127.0.0.1 for their IP Addresses to disable those options.
    2. Enter the timezone based on site location; the default timezone value is MT (US/Mountain).

```
Example:
ED-DAT:::9:::SOURCE=NTP,TZ=CT,NTP1=132.163.96.5,NTP2=216.239.35.4,NTP3=127.0.0.1,NTP4=127.0.0.1;
```

13. Use the following command to enter DATE & TIME manually, if an NTP Server is not available.

```
[G5] ED-DAT:::9:::SOURCE=MANUAL,DATE=<TBD>,TIME=<TBD>;
```

14. Set the System Identification (SID) for the G5.

```
[G5] SET-SID:::<ctag>::<SID>;

Example:
SET-SID:::9::"Zoom-G5";
```

15. If SIP TLS and SRTP is to be enabled, load the customer provided SSL certificate .tar file. The customer provided certificate file is required for this step.

```
[G5] COPY-RFILE:::9:::TYPE=SIPTLS,IPADDR=<IP Address>, UID="FTP User ID",PID =<FTP User ID>,SRC="<certificate
filename.tar>;

Example:

COPY-RFILE:::9:::TYPE=SIPTLS,IPADDR=192.168.1.75,UID="ftpuser",PID="ftpuser",SRC="zoomcerts.tar";
```

⚠️ The .md5 file is downloaded after the .tar file and the md5sum of the .tar file is computed and checked against the contents of the .md5 file.

16. ED-SIP. The Edit SIP (ED-SIP) command allows for modifying the parameter settings of the SIP DEFLT profile. Reference the Network Engineering Specbook for Site Requirements.

⚠️ If the system will use the optional TLS/SRTP, use the command to set SSPORT=5061, and PROXY CERT, SSL CERT and SSLKEY to the customer provided certificates and key.

```
[G5] ED-SIP:[<tid>]:<aid>:<ctag>:::[SSIP=<ssip>][,SSPORT=<ssport>][,PROXYIP=<proxyip>]
[,PROXYPORT=<proxyport>]
[,IPPORT=<ipport>][,SOFTSWITCH=<softswitch>][,UAINFO=<uainfo>],[REGREFRESH=<regrefresh>]
[,DISABLEDNS=<disabledns>][,TL[PRACK=<prack>],[TLS=<tls>],[PROXYCERT=<proxycert>],
[SSLCERT=<sslcert>],[SSLKEY=<sslkey>];


For example:

ED-SIP::DEFLT:9:::SSIP="10000500.zoom.us",SSPORT=5091,PROXYIP=192.204.13.6,PROXYPORT=5091,SECPROXYIP=192.204.13.8,
SECPROXYPORT=5091,IPPORT=5070,SOFTSWITCH="G5Profile",UAINFO="G5Profile",REGREFRESH=3600,DISABLEDNS=Y, PRACK=Y,
TCP=N,TLS=Y,MULTIPORT=N:;
```

17. ED-SIP. Use the Edit SIP command to configure the certificate to be used for TLS.

```
ED-SIP::DEFLT:9:::TLS=Y,PROXYCERT="DigiCertGlobalRootCA.crt",SSLCERT="",SSLKEY="";
```

18. ED-DSP. Use the Edit DSP (ED-DSP) command to configure the bearer IP. Use ED-DSP to modify the parameters of the DSP DEFLT profile.

```
[G5] ED-DSP:[<tid>]:<aid>:<ctag>:::[IPADDR=<ipaddr>,][STARTPORT=<startport>];


For example:
ED-DSP::DEFLT:9:::IPADDR=192.168.1.12,DSPBIP=192.168.1.13,STARTPORT=6000;
```

19. ED-MEDIA. Use the Edit Media (ED-MEDIA) command to modify the parameter settings of a Media Profile. i.e Codecs, Packet Rate, etc.

```
[G5] ED-MEDIA::SIPMEDIA:6:::CODECS=G711;


For example:
ED-MEDIA::DEFLT:9:::CODECS=G711&G729,PACKETRATE=20,VAD=N,COMFORTNOISE=Y,
ECHOCANCEL=Y,DTMFMODE=RFC4733,PTYPE=DYN101,FAXMODE=PASSTHRU,
PASSTHRUCODEC=G711,SRTP=Y;
```

20. Provision a SIP Interface Group. Use the Enter Interface Group (ENT-IG) command to create a network-facing GR-303 or VoIP interface group on a CT card.

```
For example:
ENT-IG::1-CT-IG-10:9:::IFTYPE=SIP;
```

> ⚠ This example is only applicable if there is a HOTLINE service profile added in the Custom Engineering Section of the G5 Specbook

21. Bring the POTS card into service.

```
[G5] ENT-EQPT: [<tid>]:<aid>:<ctag>::<type>:[DESC=<desc>]:[<pst>];


For example:
ENT-EQPT::1-2:9::POTS::IS;
```

22. ENT-T0. Use the Enter T0 (ENT-T0) command to create a SIP Subscriber Identity on a POTS line. (Refer to Appendix F for SIP scripting.)

```
For example:
ENT-T0::1-2-1:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
ENT-T0::1-2-2:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
ENT-T0::1-2-3:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
ENT-T0::1-2-4:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
ENT-T0::1-2-5:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
ENT-T0::1-2-6:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
ENT-T0::1-2-7:9:::POTSLINETYPE=LS,POTSLINEIMP=900,RTLP=-6;
```

> ⚠️ The SIP subscriber identity is also added in the EXPERiUS (A2) Provisioning Client.

23. ENT-CRS-T0. SIP Profile and T0 Termination (Subscriber Line) Association. You can accomplish this assignment (that is, "cross-connecting") using the ENT-CRS-T0 command and by designating the <b1> "FROM" AID of the command to be the SIP VoIP IG to which the termination is to be associated. The <b2> "TO" AID of the ENT-CRS-T0 command will indicate the access-facing T0 termination. You can assign a group of terminations to the SIP VoIP IG using the double ampersand (&&) range notation in the <b2> "TO" AID of the ENT-CRS-T0 command.

```
For example:
ENT-CRS-T0::1-CT-IG-10,1-2-1:9;
ENT-CRS-T0::1-CT-IG-10,1-2-2:9;
ENT-CRS-T0::1-CT-IG-10,1-2-3:9;
ENT-CRS-T0::1-CT-IG-10,1-2-4:9;
ENT-CRS-T0::1-CT-IG-10,1-2-5:9;
ENT-CRS-T0::1-CT-IG-10,1-2-6:9;
ENT-CRS-T0::1-CT-IG-10,1-2-7:9;

To check the cross-connects:
[G5] RTRV-CRS-T0::1-1-ALL:9;
```

> ⚠️ The following SpecBook example identifies the <b1> "FROM" AID and the <b2> "TO" AID. This is an example only; refer to the Project SpecBook for actual site configuration.

Figure 10: IG

Interface Group (IG) for SIP (Note IG # range)	VoIP IG <b1> AID format is: <shelf>-<slot>-IG-<IG#> shelf is always 1, slot is CT, IG is 10 to 99	POTS-32 Shelf-Slot-Port <b2> AID format is: <shelf>-<slot>-<port> where shelf is always 1, slot is 1-24, port is 1-32 OR port is ALL
10	1-CT-IG-20	1-1-ALL

24. The Allow Switch Duplex Equipment (ALW-SWDX-EQPT) command enables the automatic or manual protection switching of the redundant controller card. Note: When this command is executed, the standby CT automatically resets.

```
For example:
[G5] ALW-SWDX-EQPT::1-CT:9;
```

25. ENT-DIALRULE. Create a dial rule. The Enter Dial Rule (ENT-DIALRULE) command allows for creating a sequence of characters that describes a dial rule. The format must follow the digit map syntax rules of RFC 3525. Reference the Network Engineering Specbook to determine if applicable.

```
[G5] ENT-DIALRULE:[<tid>]:<aid>:<ctag>::<dialrule>[:DESC=<desc>];

For example:
ENT-DIALRULE::STAR7:9::*XXXXXXXXX:DESC="STAR 7";
ENT-DIALRULE::STAR10:9::*XXXXXXXXXXXX:DESC="STAR 10";
```

26. Modify the DEFLT dial plan (digit map). The Edit Dial Plan (ED-DIALPLAN) command allows for modifying the DEFLT dial plan. A dial plan is made up of one or more dial rules. Reference the Network Engineering Specbook to determine if applicable.

```
[G5] ED-DIALPLAN:[<tid>]:<aid>:<ctag>::<dialplan>[:DESC=<desc>];

For example:
ED-DIALPLAN::DEFLT:ctag::STAR&STAR7&STAR10&POUND&SPECIAL&LOCALOP&LONGOP&
7DIGIT&
LONGDIST&10DIGIT&INTL&ROUTINE&PRIORITY&IMMEDIATE&FLASH&FLASHOVR:DESC="North American Dial Plan";
```

27. ED-SNMP-TRAP. Configure the SNMP Traps. The G5 LAG will now support SNMP 'traps' to communicate alarm events to an SNMP listener (or GENView). Note: SNMP can be configured later if the information is not available at the time of commissioning.

```
[G5] ED-SNMP-TRAP:[<tid>]::<ctag>:::[IPADDR=<ipaddr>][,IPPORT=<ipport>],
[COMMUNITY=<community>][,VERSION=<version>][,PID=<PID>];

For example:
[G5] ED-SNMP-TRAP:::9:::IPADDR=172.25.99.24,COMMUNITY="public",VERSION="2C";
```

⚠️ Version 2C is the only SNMP trap version available in G5 SIP Release 3.0.

28. ED-SNMP-AGENT. Referring to the Network Engineering Specbook, review the setting for SNMP AGENT (default is disabled). To set SNMP-TRAP-AGENT enabled enter the following:

```
[G5] ED-SNMP-AGENT:[<tid>]::<ctag>:::ENABLED=Y,IPPORT=161, READ=g5snmpRD,WRITE=g5snmpWR;

For example:
[G5] ED-SNMP-AGENT:::9:::ENABLED=Y,IPPORT=161,READ="g5snmpRD",WRITE="g5snmpWR";

   G5 15-12-21 11:09:21
M 9 COMPLD
   "ENABLED=Y,IPPORT=161,READ=\"g5snmpRD\",WRITE=\"g5snmpWR\",";
```

⚠️ SNMP can be configured later if the information is not available at the time of commissioning.

29. Referring to the Network Engineering Specbook, change the IP address parameters on the G5 from their default values to their new values.

```
[G5] ED-IP:::<ctag>::::IPADDR=<IP Address>, NETMASK=<netmask>, GATEWAY=<Gateway IP Address>;

For example:
ED-IP:::9:::IPADDR=192.168.1.11,NETMASK=255.255.255.0,GATEWAY=192.168.1.1;
```

⚠️ When you enter this command, the system automatically resets the network interface, and connectivity to the TL1 interface will be lost.

30. To reset the shelf, re-enter the tl1s/tl1s user credentials and log back in with the ACT-USER command.

```
[G5] ACT-USER::SUPERUSER:9::ADMIN.5;
```

31. Enter the following command to reset the shelf:

```
INIT-SYS:::9::0;
Y;
```

32. After the shelf has rebooted, establish an ssh connection to the G5 using a laptop connected to the Customer network. Use the IP address entered in step 29.

```
ssh tl1s@<IP Address>
password: tl1s
```

33. Log back into the G5.

```
[ G5] ACT-USER:: SUPERUSER:<ctag>::ADMIN.5;
```

34. RTRV-SHELF (Retrieve Shelf Information)

The RTRV-SHELF command provides EEPROM information about the backplane of the specified G5 shelf. Note: The AID of the shelf must be 1-CT.

```
RTRV-SHELF (Retrieve Shelf Information)
The RTRV-SHELF command provides EEPROM information about the backplane of the specified G5 shelf. Note: The AID of
the shelf must be 1-CT.

[ G5] RTRV-SHELF:[<tid>]:<aid>:<ctag>;

Example:
[DLLSTXWHRPA03308A05C] RTRV-SHELF::1-CT:123;
    DLLSTXWHRPA03308A05C 16-05-13 10:28:51
M 123 COMPLD
    "1-CT::NAME=G5 LAG,HW=B0,FRU=GBVW00TN B0,SN=KAU142601051,CLEI=SLMHS00DRA,FMANAME=0.0,FMAHW=0.0,FMAFRU=0.0,
FMASN=0.0,FMACLEI=0.0:"
;
```

⚠ If the system returns "0.0" values for NAME, FRU, SN, or CLEI contact your next level of support.

```
Example:
[DLLSTXWHRPA03307A05B] RTRV-SHELF::1-CT:123;

    DLLSTXWHRPA03307A05B 16-05-13 10:28:48
M 123 COMPLD
    "1-CT::NAME=0.0,HW=0.0,FRU=0.0,SN=0.0,CLEI=0.0,FMANAME=0.0,FMAHW=0.0,FMAFRU=0.0,
FMASN=0.0,FMACLEI=0.0:"
;
```

35. Log off the system.

```
[G5] CANC-USER::SUPERUSER:<ctag>;
```

4. Backing up the G5 Configuration

This section describes the command used for creating a backup of the provisioned database. Once the backup is complete, you can store the archive to a (*.tar) file that can be stored to or retrieved from an FTP server.

1. If required, log back into the system via either the Ethernet Port (Telnet) or Serial Port method used in Procedure 1.

2. Verify that the customer has a valid FTP server available for storing the backup files.

⚠ The Installation laptop may be used as the FTP server, but the backup file will need to be sent to the location specified by the customer.

3. Back up the database files.

```
[5000LF] COPY-RFILE:::<CTAG>:::TYPE=BACKUPDB,UID=<"FTP Server UserID">,PID=<"FTP Server Password">,IPADDR=<FTP
Server IP Address>,DEST="<FTP Server directory location>";

Ex. [5000LF] COPY-RFILE:::9:::TYPE=BACKUPDB,UID="admin",PID="password",
IPADDR=10.123.2.1,DEST="/database/5000lf";
```

> ⚠
> 1. The UID and PID parameters consist of ASCII characters that must be enclosed in double quotes. The maximum number of characters is 32 (excluding the double quotes).
> 2. The DEST parameter consists of ASCII characters that must be enclosed in double quotes. The maximum number of characters is 80 (excluding the double quotes).
> 3. The DEST parameter must specify the full path of the storage directory on the FTP server. If the DEST parameter is not specified, the database files will be copied to the home directory of the User ID (UID) on the FTP server.

4. The archived database files are stored in a single tar file (*.tar) along with a checksum file (*.md5) for validation purposes. The files are successfully copied to the FTP server when the COMPLD response is displayed.

The files are in the following format: <SID>_<Serial Number>_DB_<Date>_<Time>.tar or .md5.

```
Example: 5000LF_55_DB_20110401_170025.tar and 5000LF_55_DB_20110401_170025.md5
```

Caveats

This section provides instructions on how to resolve common issues. Below are examples of how to format etc. (if applicable).

SIP Registration Status = "Rejected by Server"

Definition: The server received the register request from the endpoint and responds with an unauthorized message.

- Ensure the SIP credentials (extensions, authentication ID, password) are correct.
- Under Basic Settings > SIP, click on the blue circular arrows to the right of the Password field. If the Password is not what it should be, the web browser is probably auto-filling the password field. If so, any change on a page containing a password could be filled in with an undesired string.

SIP Registration Status = "No reply from Server"

Definition: The device is not able to communicate across the network to the phone server.

- Double check that the "SIP Domain(Proxy Server)" fields, under Basic Settings > SIP tab, are filled out correctly with the address of your server and port number.
- Ensure the firewall (if present) is not blocking the incoming packets from the server.
- Ensure TLS is configured for SIP Transportation Method (Advanced Settings > Advanced SIP).

Supplementary Services and Features Coverage

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

Sr. No.	Supplementary Features and Services	Coverage
1	Basic Registration over TLS	✔
2	Basic Call Setup	✔
3	Basic Call Termination	✔
4	Call Hold/Resume	✔
5	Call Transfer - Blind (Cold transfer)	✔
6	Call Transfer - Consult (Warm transfer)	✔
7	Conference	✔
8	Group Call Pickup	✔
9	Call Park	✔

Legend

✔	Supported
✘	Not Supported
N/A	Not Applicable

Support

For any support related queries about this guide, please 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 and solutions, please visit:

https://ribboncommunications.com/products

For detailed information about Zoom products and solutions, please visit:

https://zoom.us/

Conclusion

This Interoperability Guide describes a successful configuration covering Zoom interop involving the Ribbon G5 LAG. All the necessary features and serviceability aspects stand covered as per the details provided in this interoperability document.

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.