ORACLE
COMMUNICATIONS

ORACLE

Oracle Enterprise Session Border Controller and Microsoft Skype for Business for Video calls

Technical Application Note

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Intended Audience

This document is intended for use by Oracle personnel, third party Systems Integrators, and end users of the Oracle Enterprise Session Border Controller (E-SBC). It assumes that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller – Acme Packet 4600 / Acme Packet 3820.

Document Overview

Oracle Communications provides session based products that help internetwork SIP based communications in multivendor environments. This document discusses the configuration and implementation of Oracle's Enterprise Session Border Controller and Skype for Business Video Interop Server for seamless audio or video connectivity between Microsoft Skype for Business endpoints and Polycom Group Series 500 and/or sip endpoints such as Bria 4.

It should be noted that the E-SBC configuration provided in this guide focuses strictly on the Skype for Business (SFB) Server associated parameters. Many E-SBC users may have additional configuration requirements that are specific to other applications. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

For additional information on Skype for Business Server, please visit http://www.skype.com/en/business/.

Introduction

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise SBC and the Skype for Business Server. There will be steps that require navigating Microsoft Windows Server as well as the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Requirements

- Fully functioning Skype for Business Server deployment, including Active Directory and DNS
- A Video Interop Server to enable video calling
- Microsoft Skype for Business 2015 – Version 6.0.93190.0
- Skype for Business 2016 client, Version 16.0.4288.1000
- Oracle Enterprise Session Border Controller AP 3820 and AP 4600 running Net-Net OS ECZ730m1p1.32.bz.
    a. **Note:** the configuration running on the SBC is backward/forward compatible with any release in the 7.3.0 stream
    b. **Note:** the same configuration & software can be loaded on any SBC flavor such as 1100, 4500, 6300 and achieve same results.
- Functioning implementation of Polycom Real Presence UC environment including Group Series 500
- A soft client with H.264 video support like Counterpath Bria 4.

VIS server and Codec Support

The Video Interop Server (VIS) is a new server role in Skype for Business that enables video interoperability between third party video conferencing systems and SFB deployment.

- It enables successful video calls between third party systems and SFB by transcoding between several flavors of H.264 formats used by video systems.
- VIS does not support transcoding of RTV codec. So only Lync 2013, SFB clients and any other endpoint that supports Microsoft's H.264 SVC codec can participate in the call.
- A video SIP trunk is configured between the SBC and VIS to route the calls.

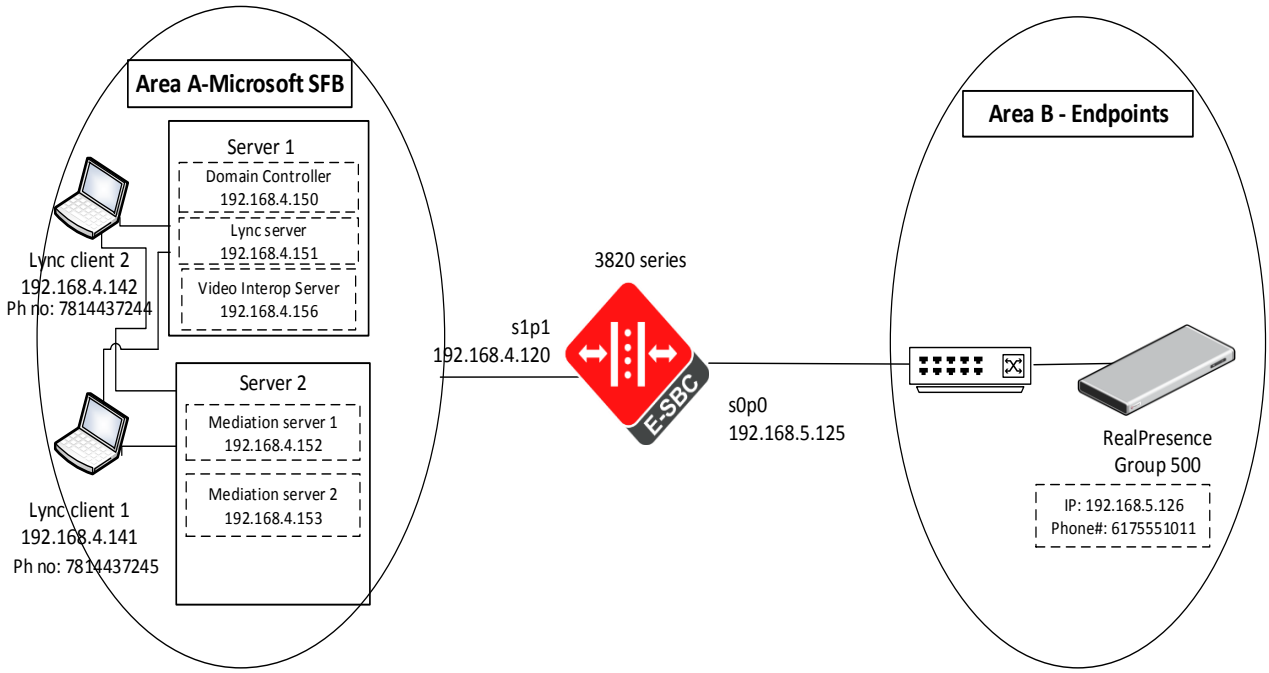
VIS Limitation

As of today, only inbound calls into VIS server is allowed – no outbound calls are allowed. Read more here - https://technet.microsoft.com/en-us/library/ms.lync.plan.videointerop.aspx

For the purpose of this testing, peer to peer video calling was tested with calls being made from Polycom/Bria end points to the SFB client.

Lab Architecture and Configuration

The following diagram, illustrates the lab environment created to facilitate the video testing (IP addressing/Port below is only a reference; they can change per your network specification).



Area A represents the customer's on premise infrastructure, which includes the Active Directory, DNS and Skype for Business Server systems. Area B represents the endpoints we have configured for video calling (like Polycom RP Group 500 and Bria 4). It is necessary that the Skype for Business deployment include a functioning Video Interop Server for the video calls to be successful. The configuration, validation and troubleshooting of the areas A and B is the focus of this document and will be described in two phases:

- Phase 1 – Configure the Skype for Business Server
- Phase 2 – Configure the SBC

Phase 1 – Configuring the Skype for Business server

The enterprise will have a fully functioning Skype for Business Server infrastructure with Video Interop Server deployed. If there is no VIS present for this purpose, one will have to be deployed.

There are two parts for configuring SFB Server to operate with the Oracle SBC:

- Adding the SBC as a video gateway to the SFB Server infrastructure
- Configure the VIS with appropriate settings for the video trunk.

To add the video gateway, we will need:

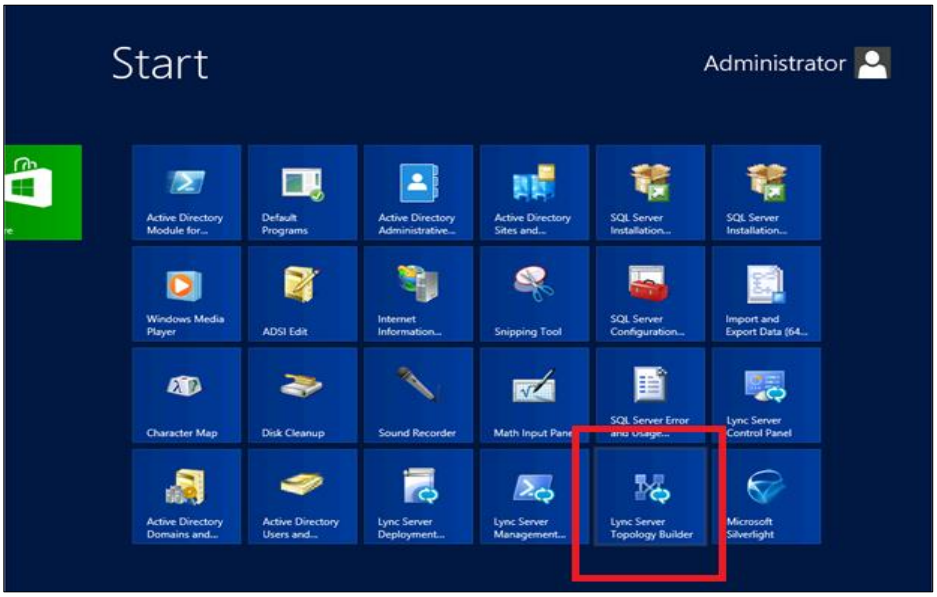
- FQDN of the SBC being used as the video gateway
- Rights to administer Lync Server Topology Builder
- Access to the Lync Server Topology Builder

Note: This section of the Application note only walks you through adding Oracle E-SBC to Microsoft's Skype for Business config, the assumption is that Microsoft's Skype for Business application is already installed and 100% functional.

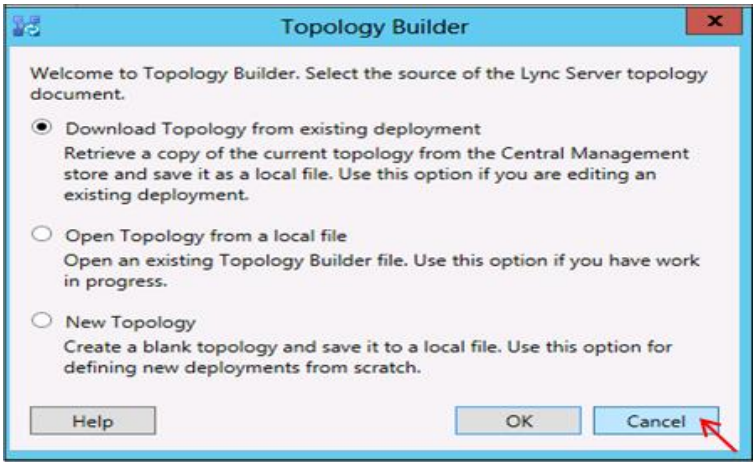
Adding the SBC as a video gateway

The following process details the steps to add the SBC as the PSTN gateway

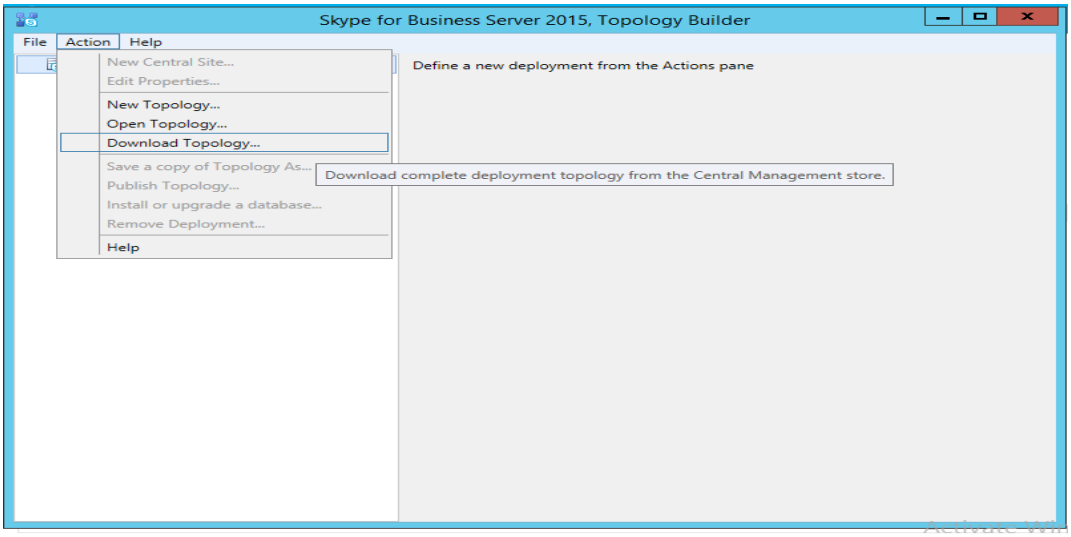
1. On the server where the Topology Builder is located, start the console.
2. From the **Start** bar, select **Lync Server Topology Builder**.



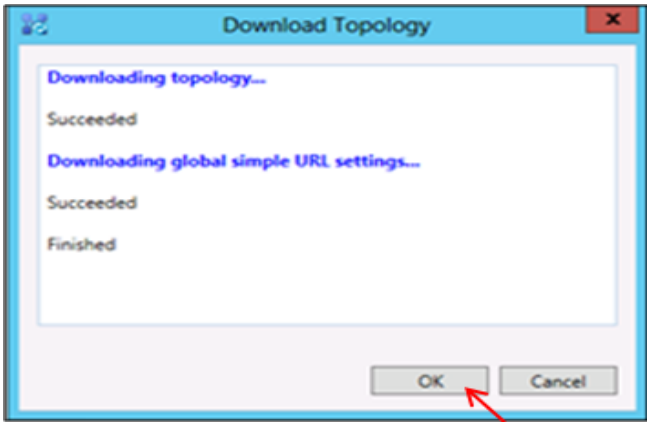
3. The opening screen of the Topology builder will be displayed. Click on the **Cancel** button.



4. The Topology Builder window will now be displayed. Click on **Action** and select **Download Topology**.

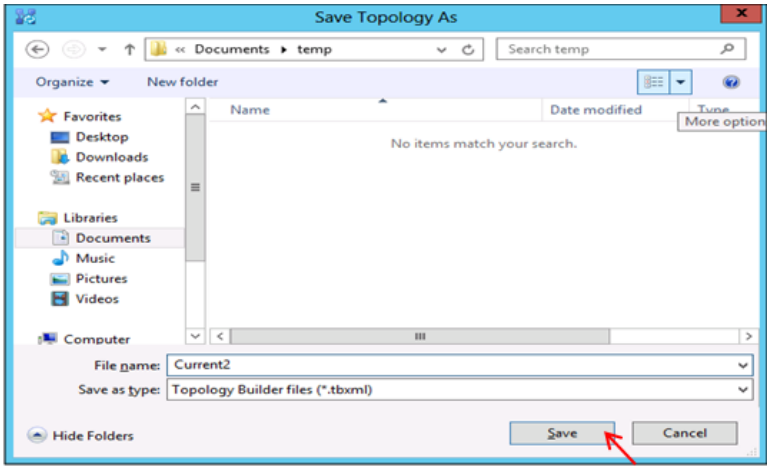


5. You will then see a screen showing that you have successfully imported the topology. Click the **Ok** button.

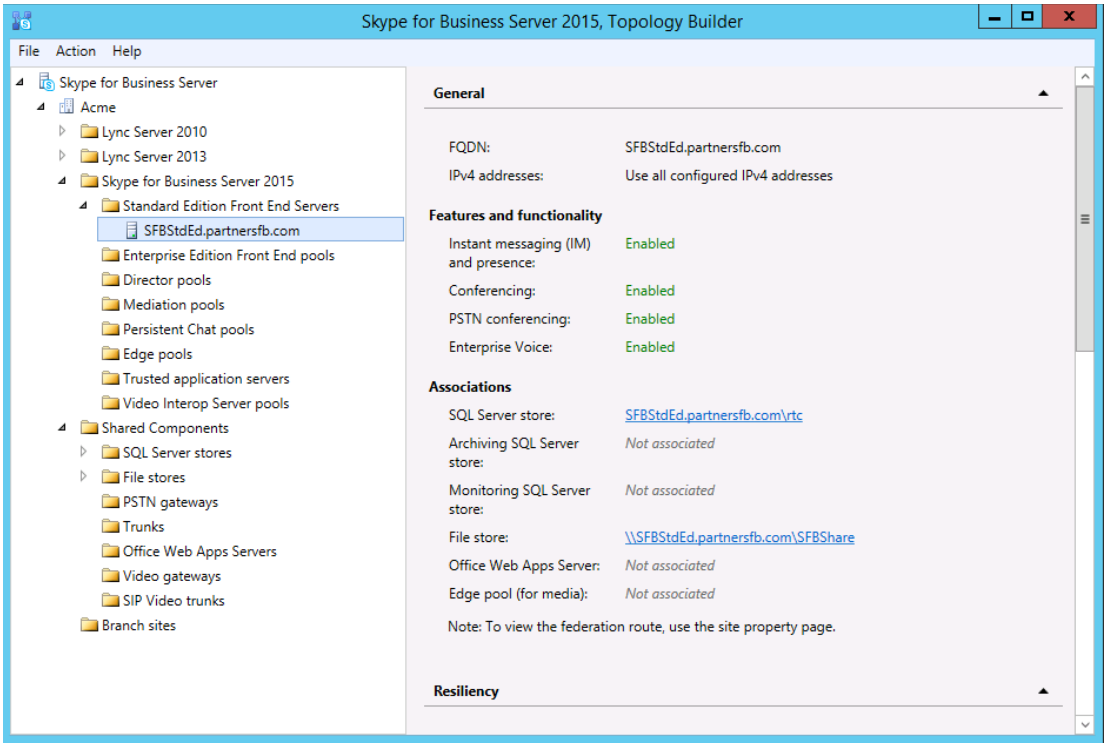


6. Next you will be prompted to save the topology which you have imported. You should revision the name or number of the topology according to the standards used within the enterprise. Click the **Save** button

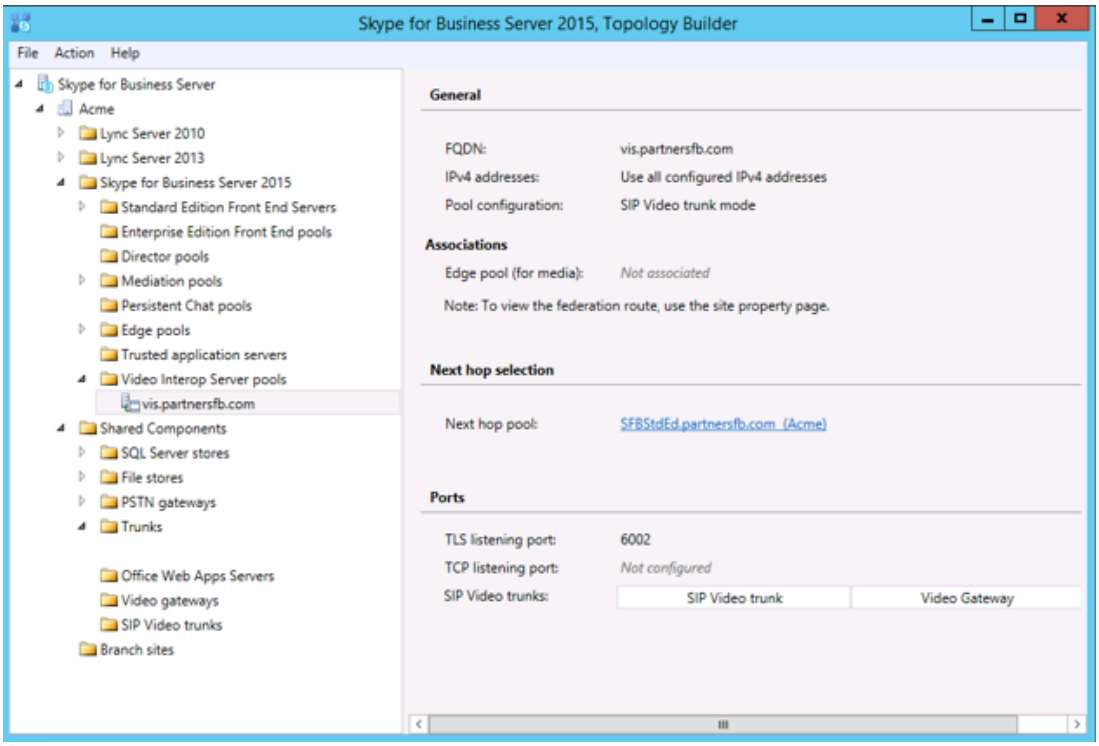
   Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make during this installation



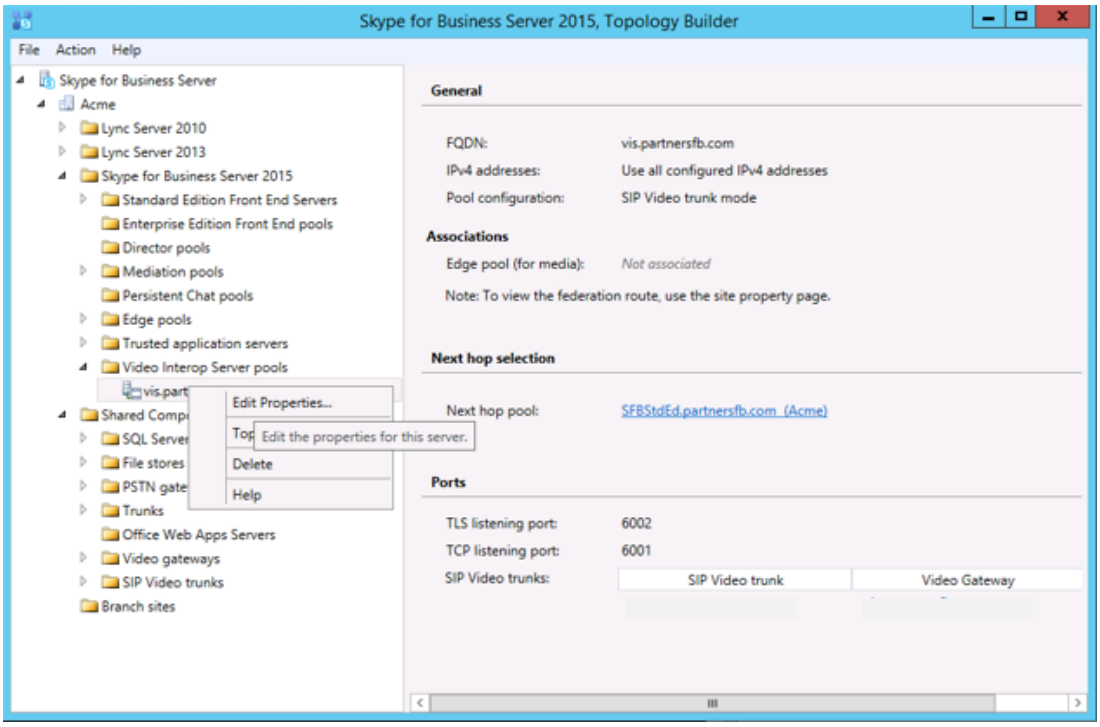
7. You will now see the topology builder screen with the enterprise's topology imported.



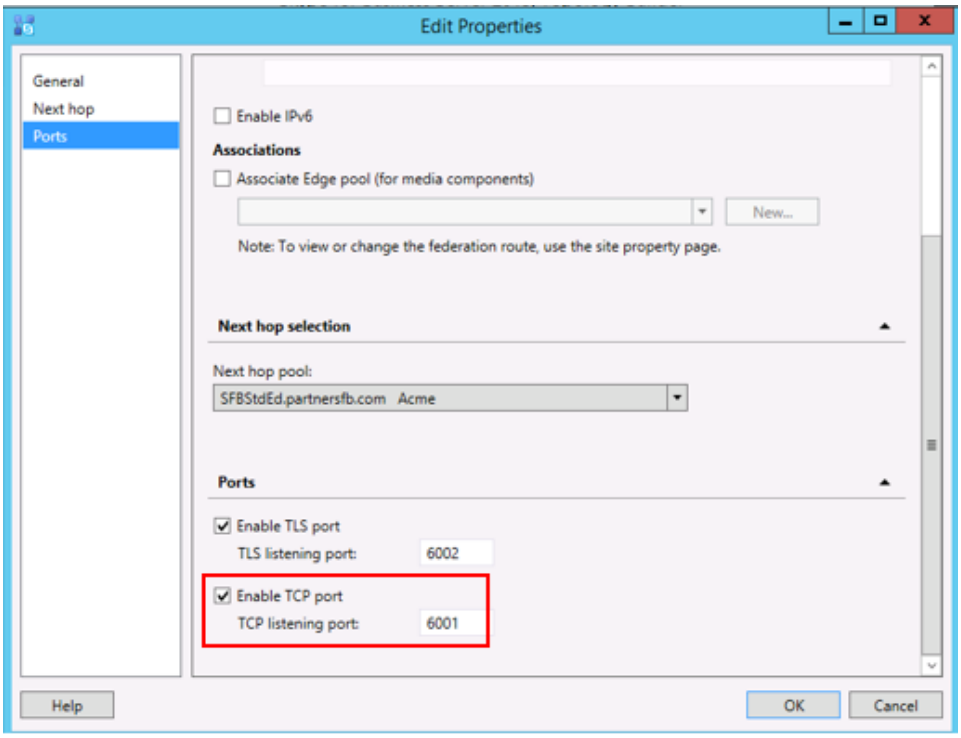
8. Before proceeding further, ensure that the VIS is deployed by expanding the **Video Interop Server pools**.



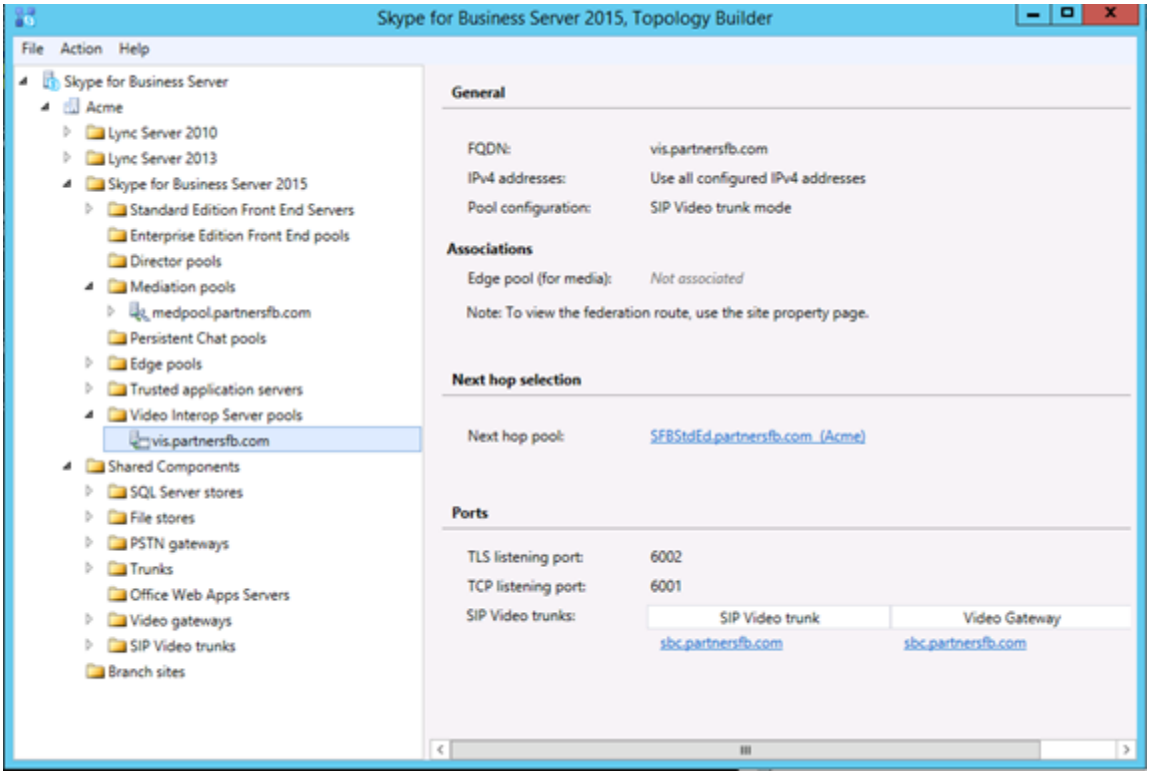
9. When you add the VIS, the TCP port is disabled by default. To enable the TCP port, right-click the VIS pool and click on **Edit Properties**.



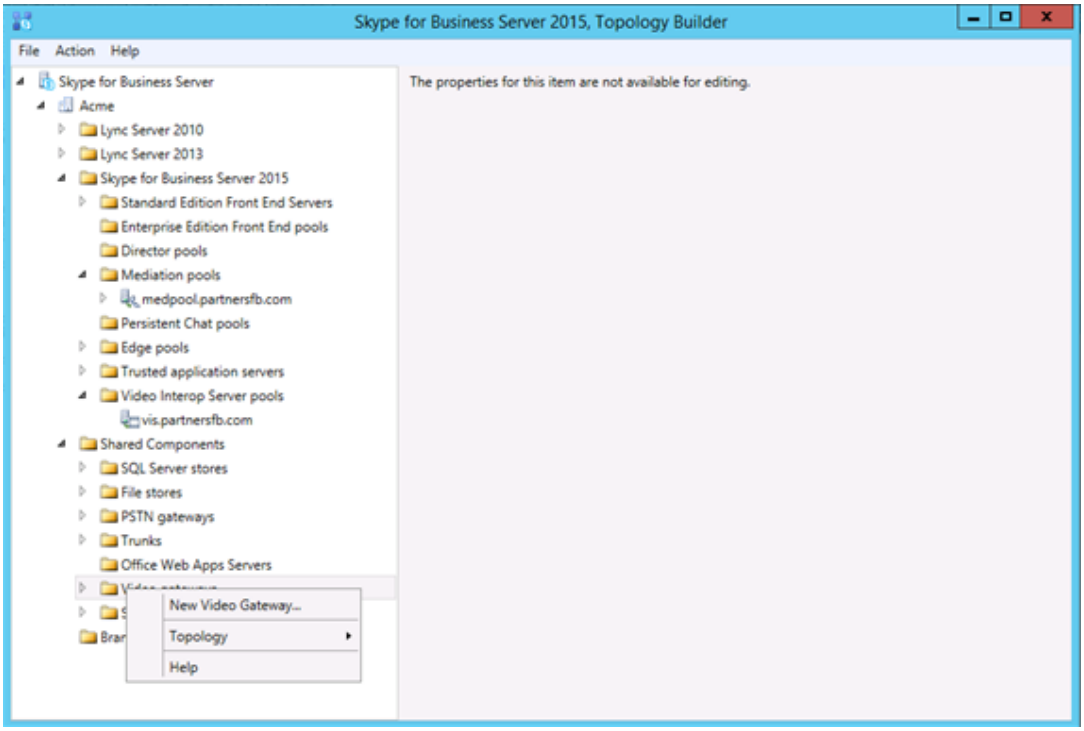
10. In the Edit Properties window, check the **Enable TCP port** checkbox and click **OK**.



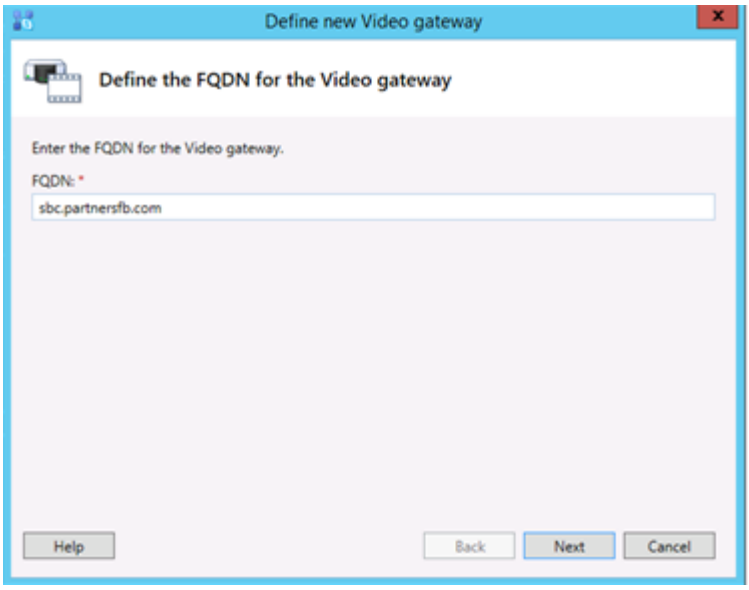
11. The VIS pool page will now show the TCP listening port as 6001.



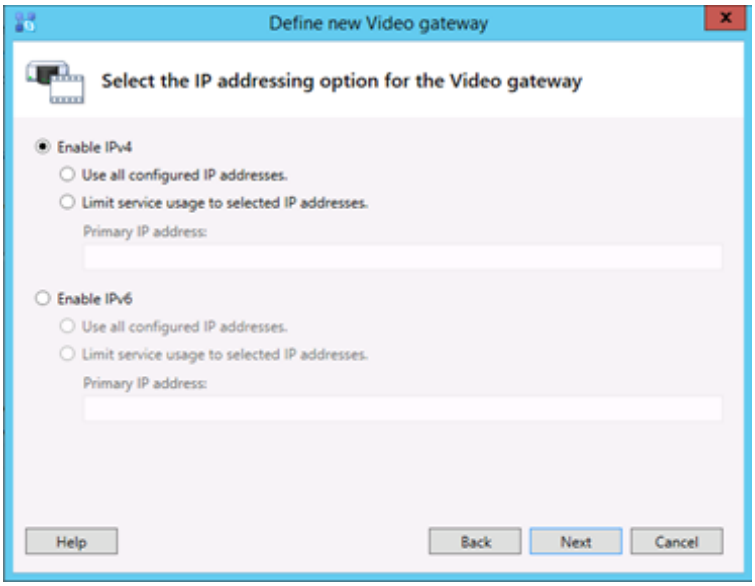
12. Expand the **Shared Components** section. Right-click on **Video Gateways** and select **New Video Gateway**.



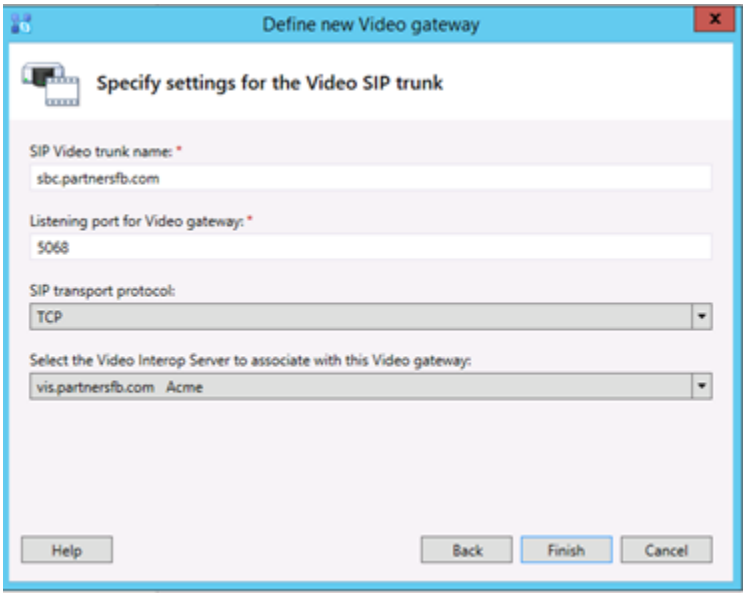
13. In the **Define new Video Gateway** window, enter the hostname of the SIP interface of the SBC in the **FQDN** text box and click **Next**.



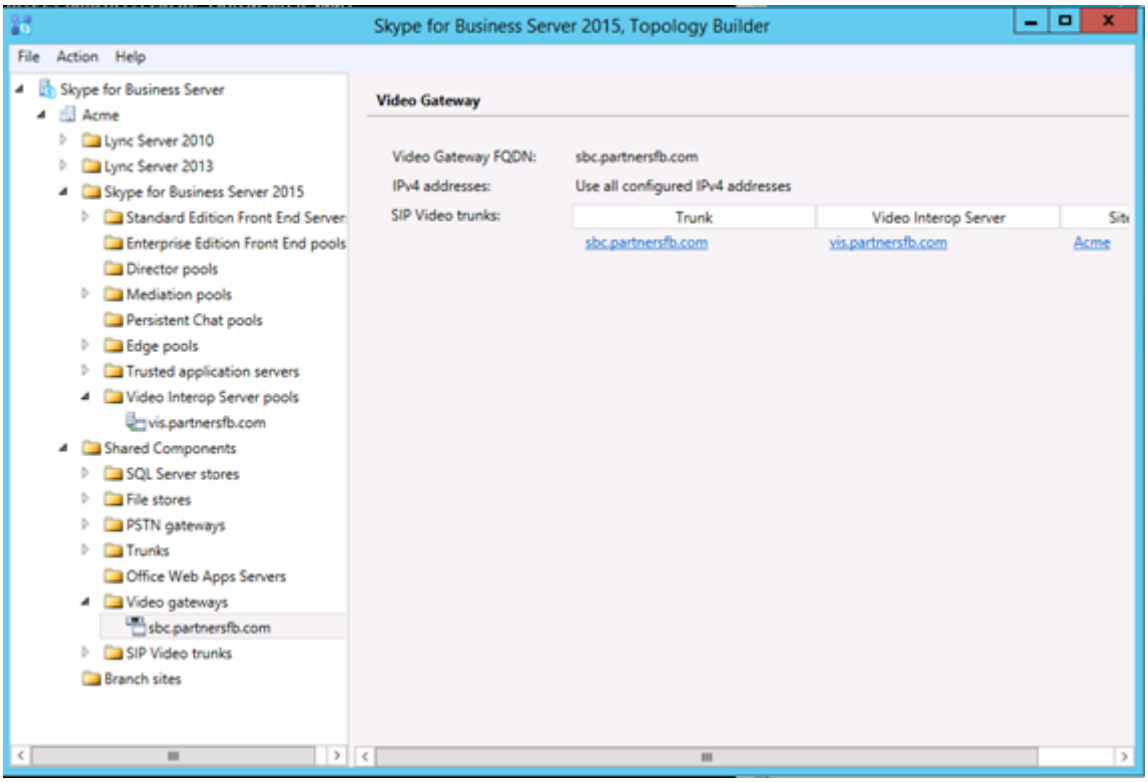
14. Select **Enable IPv4** in the **Select the IP addressing option** section and click **Next**.



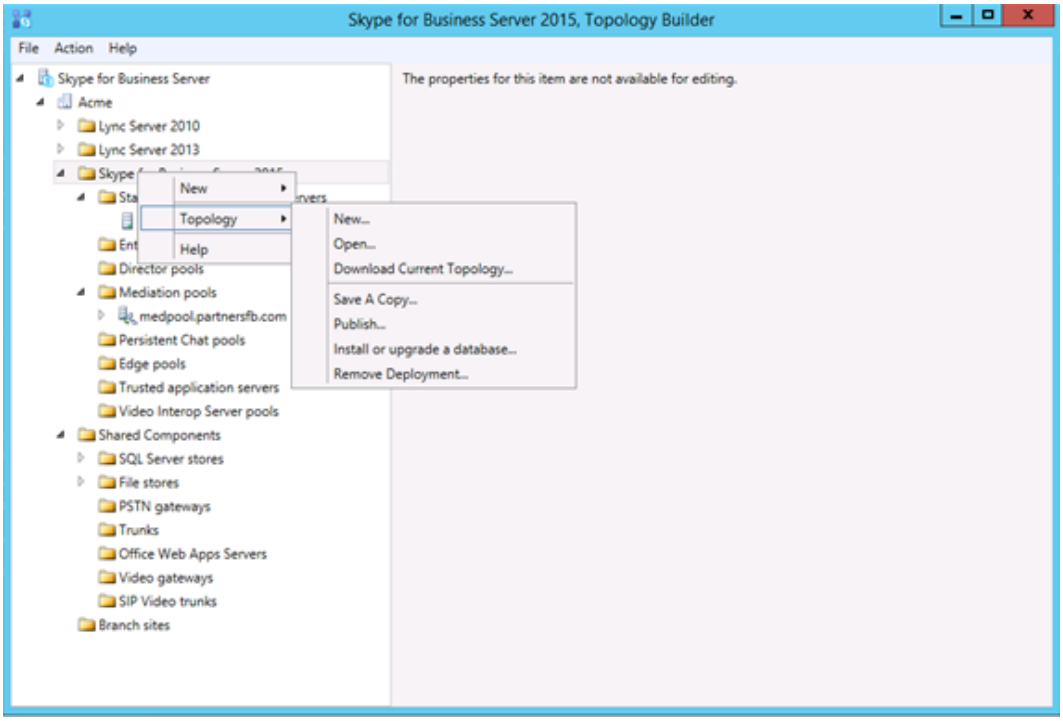
15. In the next section, enter the hostname of the SBC under **SIP Video Trunk name**. Configure the **Listening port for Video gateway** as 5068, TCP as the **SIP Transport Protocol,** select the VIS pool configured earlier under the **Select the Video Interop Server to associate with this Video gateway** drop-down menu and click **Finish**.



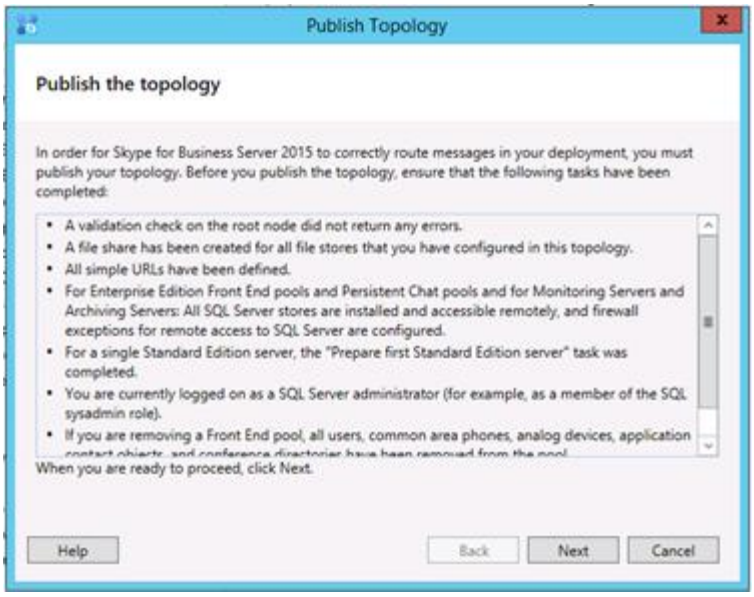
16. The video gateway for the Skype for Business server has been added. It will be listed under **Video gateways**. When you click on the video gateway, it will show the association of the video trunk with the video interop server.



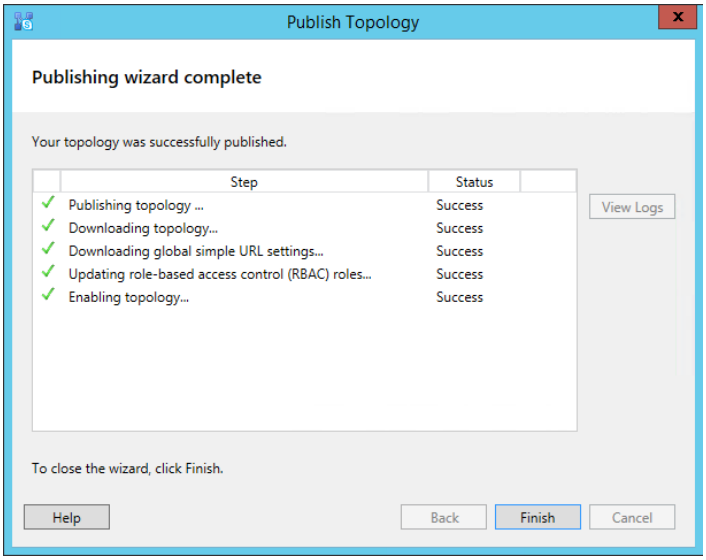
17. In the upper right hand corner of your screen under **Actions** select **Topology** then select **Publish**.



18. You will now see the **Publish Topology** window. Click on the **Next** button



19. When complete you should see a window from Topology Builder stating that your topology was successfully published. Click the **Finish** button.



Configuring video trunk settings on VIS

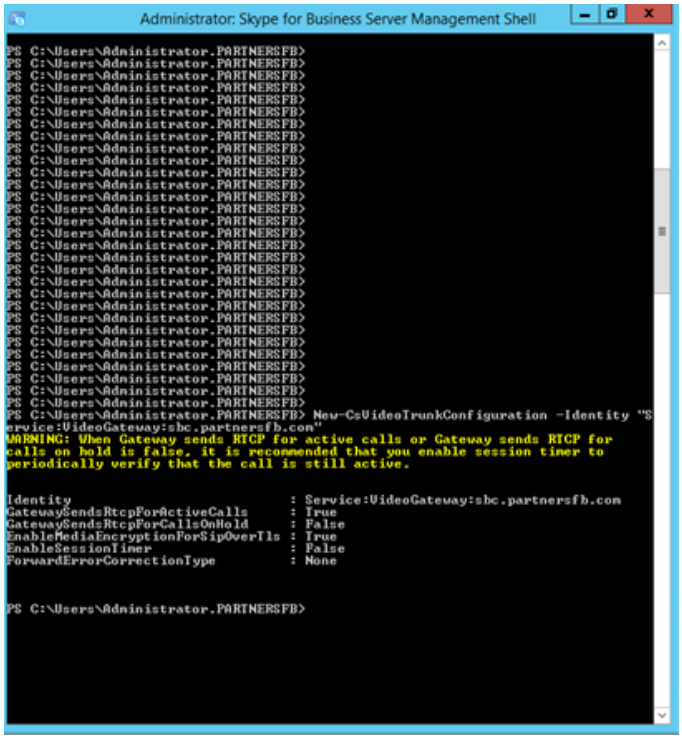
When the VIS is installed, a video trunk configuration with global scope is created. This global video trunk configuration is applied to all the video trunks that do not have a specific trunk configuration applied.

In this section, we will configure the video trunk configuration and the dial plan to be applied on the video trunk configured in the earlier step using powershell commands. If a specific dial plan is not assigned to the video trunk, the global dial plan is taken into consideration.

The following process details the steps to create the route:

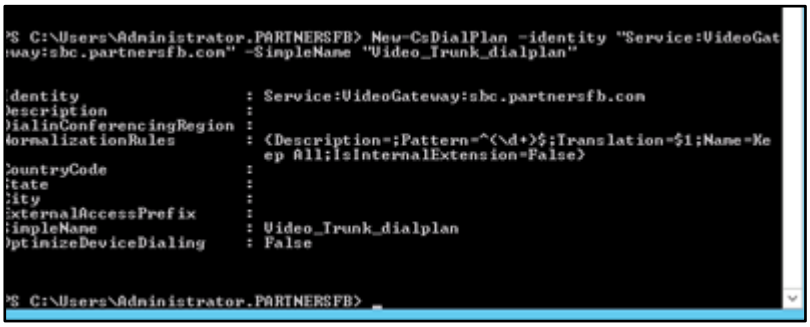
1. On the Video Interop Server, select **Skype for Business Management Shell** from the **Start** menu. Enter the following command to create a new video trunk configuration

```
New-CsVideoTrunkConfiguration -Identity "Service:VideoGateway:sbc.partnersfb.com"
```

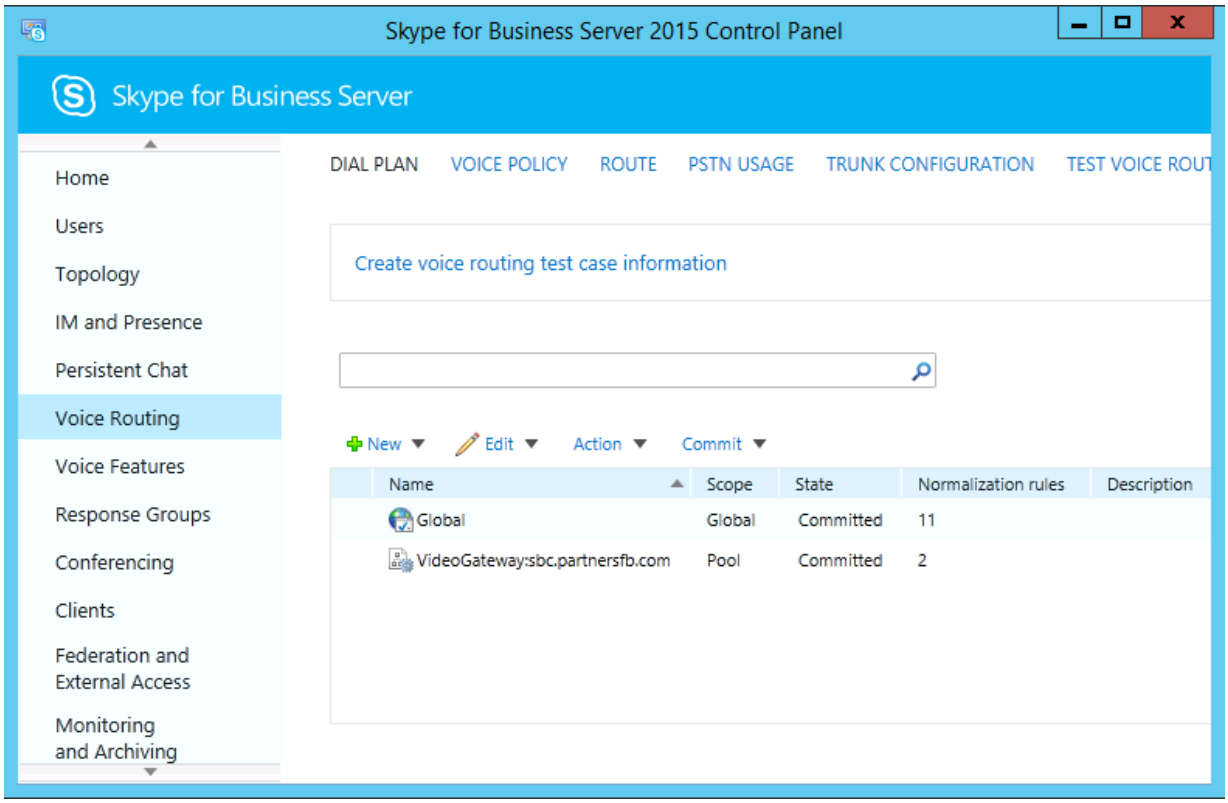


2. Next we create a dial plan to be used by the video trunk using the following command:

```
New-CsDialPlan -identity "Service:VideoGateway:sbc.partnersfb.com" -SimpleName
“Video_Trunk_dialplan”
```



3. This dial plan can now be found in the Voice Routing tab of the skype for Business control panel under the Dial Plan tab.



If any normalization rules need to be applied specifically to the video trunk, it can be configured under the dial plan created in the previous step.

Phase 2 – Configuring the Oracle Enterprise SBC

In this section we describe the steps for configuring an Oracle Enterprise SBC, formally known as an Acme Packet Net-Net Session Director ("SBC"), for use with Skype for Business Server in a SIP trunking scenario.

In Scope

The following guide configuring the Oracle SBC includes only the configuration necessary to make the peer to peer video calls from the Polycom endpoint to Skype for Business VIS.

Note that Oracle offers several models of SBC. This document covers the setup for the 3820 platform series running Net-Net OS ECZ7.3.0 or later. Please note that the same configuration has been used on a 4600 running the same software to make successful peer to peer video calls. If instructions are needed for other Oracle SBC models, please contact your Oracle representative.

Out of Scope

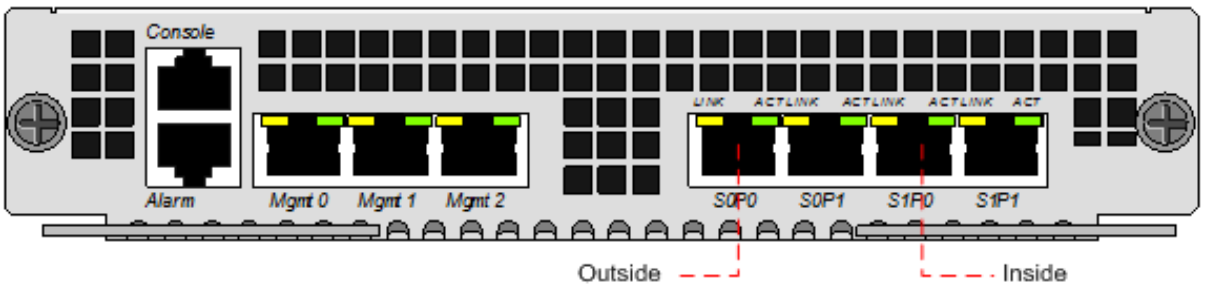
- Configuration of Network management including SNMP and RADIUS; and

What will you need

- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Oracle SBC
- IP address to be assigned to management interface (Wancom0) of the SBC - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support SBC configurations with management and media/service interfaces on the same subnet.
- IP address of Video Interop Server external facing NIC
- IP addresses to be used for the SBC internal and external facing ports (Service Interfaces)
- IP address of the next hop in the Polycom side (ip address of the Polycom endpoint)
- IP address of the enterprise DNS server

SBC- Getting Started

Once the Oracle SBC is racked and the power cable connected, you are ready to set up physical network connectivity. **Note: use the console port on the front of the SBC, not the one on the back.**



Plug the slot 0 port 0 (s0p0) interface into your outside (Polycom facing) network and the slot 0 port 1 (s1p0) interface into your inside (SFB server-facing) network. Once connected, you are ready to power on and perform the following steps.

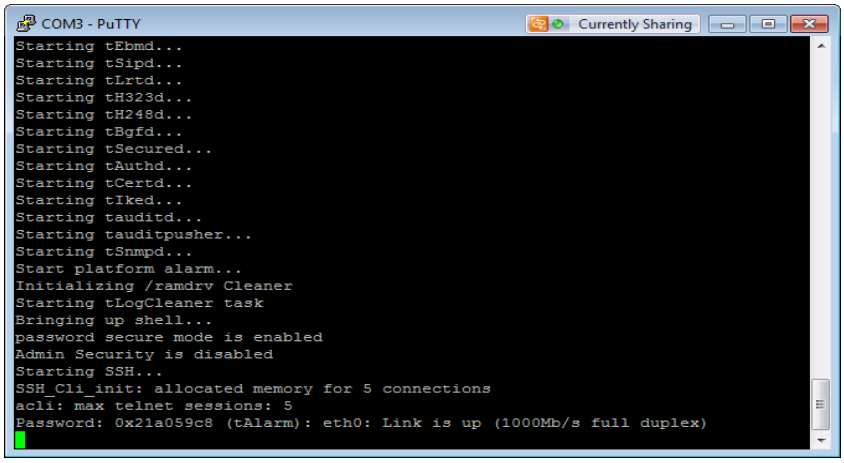
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as oraclesbc1 are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

Establish the serial connection and logging in the SBC

Confirm the SBC is powered off and connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as PuTTY. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Power on the SBC and confirm that you see the following output from the bootup sequence.



Enter the following commands to login to the SBC and move to the configuration mode. Note that the default SBC password is "**acme**" and the default super user password is "**packet**".

```
Password: acme
oraclesbc1> enable
Password: packet
oraclesbc1# configure terminal
oraclesbc1(configure)#
```

You are now in the global configuration mode.

Initial Configuration – Assigning the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the SBC by going to

oraclesbc1#configure terminal --- >bootparams

- Once you type "bootparam" you have to use "carriage return" key to navigate down
- A reboot is required if changes are made to the existing bootparams

```
ACMESYSTEM(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File             : /boot/nnECZ730m1p1.32.bz
IP Address            : 192.65.79.44
VLAN                  :
Netmask               : 255.255.255.224
Gateway               : 192.65.79.33
IPv6 Address          :
IPv6 Gateway          :
Host IP               : 0.0.0.0
FTP username          : vxftp
FTP password          : vxftp123
Flags                 :
Target Name           : ACMESYSTEM
Console Device        : COM1
Console Baudrate      : 115200
Other                 :

NOTE: These changed parameters will not go into effect until
reboot.
Also, be aware that some boot parameters may also be changed
through
PHY and Network Interface Configurations.
```

Additional Steps

There are other aspects to a Lync Server Enterprise Voice deployment such as

- Site, local, and global dial plans
- Voice Policies
- Assigning Voice Policies to users
- PSTN usage policies

Refer to MSDN technet for relevant information.

Configuring the SBC

The following section walks you through configuring the Oracle Enterprise SBC required for peer to peer video calling from the Polycom endpoint to Skype for Business (SFB) VIS.

It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

We have configured a sip-manipulation – NATting to implement topology hiding towards SFB VIS as it expects to see the SBC information in the SIP signaling.

SBC Configuration

The following section provides information on configuration required on the SBC to route video call to the Skype for Business environment.

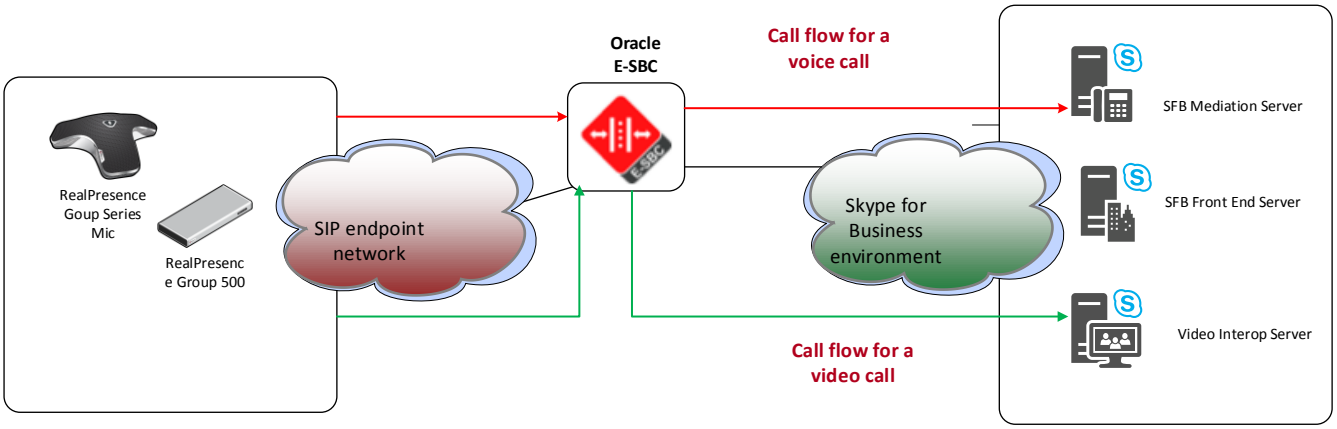
```
local-policy
        from-address                            *
        to-address                              *
        source-realm                            SFB
        policy-attribute
                next-hop                                192.168.5.126
                realm                                   towards-Polycom
                app-protocol                            SIP
local-policy
        from-address                            *
        to-address                              *
        source-realm                            towards-Polycom
        policy-attribute
                next-hop                                vis.partnersfb.com
                realm                                   SFB
                action                                  replace-uri
                app-protocol                            SIP
media-manager

network-interface
        name                                    s0p0
        ip-address                              192.168.5.125
        netmask                                 255.255.255.0
        gateway                                 192.168.5.1
        hip-ip-list                             192.168.5.125
        ftp-address                             192.168.5.125
        icmp-address                            192.168.5.125
        ssh-address                             192.168.5.125

network-interface
        name                                    s1p1
        hostname                                sbc.partnersfb.com
        ip-address                              192.168.4.121
        netmask                                 255.255.255.0
        gateway                                 192.168.4.1
        dns-ip-primary                          192.168.4.150
        dns-domain                              partnersfb.com
        hip-ip-list                             192.168.4.121
        ftp-address                             192.168.4.121
        icmp-address                            192.168.4.121

phy-interface
        name                                    s0p0
```

```
        operation-type                          Media

phy-interface
        name                                    s1p1
        operation-type                          Media
        port                                    1
        slot                                    1

realm-config
        identifier                              SFB
        network-interfaces                      s1p1:0
        mm-in-realm                             enabled

realm-config
        identifier                              towards-Polycom
        network-interfaces                      s0p0:0
        mm-in-realm                             enabled

session-agent
        hostname                                192.168.5.126
        ip-address                              192.168.5.126
        transport-method                        StaticTCP
        realm-id                                towards-Polycom

session-agent
        hostname                                192.168.5.127
        ip-address                              192.168.5.127
        transport-method                        StaticTCP
        realm-id                                towards-Polycom

session-agent
        hostname                                vis.partnersfb.com
        port                                    6001
        transport-method                        StaticTCP
        realm-id                                SFB
        ping-method                             OPTIONS
        ping-interval                           30

sip-config
        options                                 max-udp-length=0
        sip-message-len                         10000

sip-interface
        realm-id                                SFB
        sip-port
                address                                 192.168.4.121
                port                                    5068
                transport-protocol                      TCP
        out-manipulationid                      NATting

sip-interface
        realm-id                                towards-Polycom
        sip-port
                address                                 192.168.5.125
                transport-protocol                      TCP
        enforcement-profile                     noINFO
```

```
sip-manipulation
        name                                    NATting
        header-rule
                name                                    From
                header-name                             From
                action                                  manipulate
                element-rule
                        name                                    From_header
                        type                                    uri-host
                        action                                  replace
                        new-value                               $LOCAL_IP
        header-rule
                name                                    To
                header-name                             To
                action                                  manipulate
                msg-type                                request
                element-rule
                        name                                    To
                        type                                    uri-host
                        action                                  replace
                        new-value                               $REMOTE_IP

sip-monitoring
        match-any-filter                        enabled

steering-pool
        ip-address                              192.168.4.121
        start-port                              20000
        end-port                                40000
        realm-id                                SFB

steering-pool
        ip-address                              192.168.5.125
        start-port                              10000
        end-port                                40000
        realm-id                                towards-Polycom

system-config
        hostname                                Lync-video
        process-log-level                       NOTICE
        comm-monitor
                state                                   enabled
                monitor-collector
                        address                                 172.18.0.175
        default-gateway                         172.18.0.1

web-server-config
```

Call flow

The call flow of a video call with the interop server is different when compared to a normal voice call coming into a Skype for Business deployment. In a video call, the SIP messages are sent Video Interop Server and not the Mediation Servers.



The main function of the Video interop Server is to provide conversion between the different H.264 formats supported by Microsoft and third party providers like Polycom to allow for successful two way video calling between these systems.

When a call is placed from the Polycom endpoint, the SDP in the INVITE for video is as shown below

m=video 16764 RTP/AVP 116 109 110 111 96 34 31

b=TIAS:1024000

a=rtpmap:116 vnd.polycom.lpr/9000

a=fmtp:116 V=2;minPP=0;PP=150;RS=52;RP=10;PS=1400

a=rtpmap:109 H264/90000

a=fmtp:109 profile-level-id=42801f; max-mbps=216000; max-fs=3840; sar-supported=13; sar=13

a=rtpmap:110 H264/90000

a=fmtp:110 profile-level-id=42801f; packetization-mode=1; max-mbps=216000; max-fs=3840; sar-supported=13; sar=13

a=rtpmap:111 H264/90000

a=fmtp:111 profile-level-id=64001f; packetization-mode=1; max-mbps=216000; max-fs=3840; sar-supported=13; sar=13

a=rtpmap:96 H263-1998/90000

a=fmtp:96
CIF4=1;CIF=1;QCIF=1;SQCIF=1;CUSTOM=352,240,1;CUSTOM=704,480,1;CUSTOM=848,480,1;CUSTOM=640,368,1;CUSTOM=432,240,1

a=rtpmap:34 H263/90000

a=fmtp:34 CIF4=1;CIF=1;QCIF=1;SQCIF=1

a=rtpmap:31 H261/90000

a=fmtp:31 CIF=1;QCIF=1

a=sendrecv

a=rtcp-fb:* ccm tmmbr

a=rtcp-fb:* ccm fir

m=application 16768 RTP/AVP 100

a=rtpmap:100 H224/4800

a=sendrecv

m=application 16760 TCP/BFCP *

a=floorctrl:c-s

a=confid:1

a=userid:2

a=floorid:1 mstrm:3

a=setup:actpass

a=connection:new

The video SDP sent in the 200 OK from the VIS is as follows

m=video 10186 RTP/AVP 124

c=IN IP4 192.168.5.125

a=label:main-video

a=sendrecv

a=rtpmap:124 H264/90000

a=fmtp:124 profile-level-id=42C02A;packetization-mode=1;max-mbps=27600;max-fs=920;max-br=3333;max-fps=1500

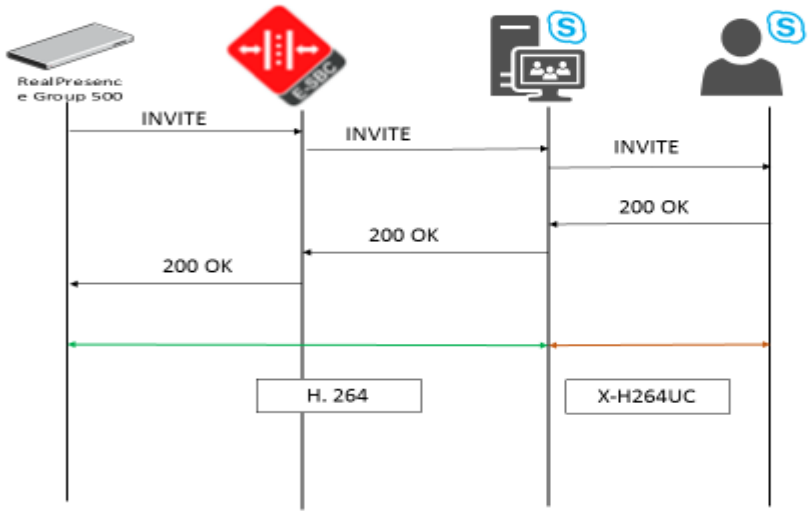
a=rtcp-rsize

a=rtcp-fb:* nack pli

m=application 0 RTP/AVP 100

m=application 0 TCP/BFCP *

The video packets sent from Polycom to SFB VIS are H.264 with a payload of 124 and VIS sends the H.264 with a payload of 110. It converts the H.264 received from Polycom to X-H264UC format as supported by Microsoft before passing the media to the SFB clients and vice versa (converts X-H264UC to H.264 as supported by Polycom)



Please note that as of now only inbound calls can be made into VIS using the video trunks and outbound calls are not supported.

As a part of this testing, successful video calls were made to VIS from Polycom Real Presence Group Series 500 and Counterpath Bria 4 soft client.

Troubleshooting Tools

If you find that you are not able to complete calls or have problems with the test cases, there are a few tools available for Windows Server, Lync Server, and the Oracle SBC like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting any issues you may encounter.

Since we are concerned with communication between the Lync Server mediation server and the SBC we will focus on the troubleshooting tools to use between those devices if calls are not working or tests are not passing.

Microsoft Network Monitor (NetMon)

NetMon is a network protocol analyzer which is freely downloadable from Microsoft. It can be found at www.microsoft.com/downloads. NetMon could be installed on the Lync Server mediation server, the Lync Server Standard Edition server, or Enterprise Edition front end server.

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org. Wireshark could be installed on the Lync Server mediation server, the Lync Server Standard Edition server, or MCS Enterprise Edition front end server.

Eventviewer

There are several locations in the event viewer where you can find valuable information to aid in troubleshooting issues with your deployment.

With the requirement that there is a completely functioning Lync Server with Enterprise Voice deployment in place, there are only a few areas in which one would use the Event Viewer for troubleshooting:

- The Enterprise Voice client;
- The Lync Server Front End server;
- A Lync Server Standard Edition Server; and
- A Lync Server Mediation Server.

On the Oracle SBC 3820 Series

The Oracle SBC provides a rich set of statistical counters available from the ACLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces.

Resetting the statistical counters, enabling logging and restarting the log files.

At the SBC Console:

```
oraclesbc1# reset sipd
oraclesbc1# notify sipd debug
oraclesbc1#
enabled SIP Debugging
oraclesbc1# notify all rotate-logs
```

Examining the log files

Note: You will FTP to the management interface of the SBC with the username user and user mode password (the default is "**acme**").

```
C:\Documents and Settings\user>ftp 192.168.5.24
Connected to 192.168.85.55.
220 oraclesbc1FTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
331 Password required for user.
```

```
Password: acme
230 User user logged in.
ftp> cd /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (204681
bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

You may now examine the log files with the text editor of your choice.

Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle Enterprise Session Border Controller, and provides traces in a common log format for local viewing or for exporting to your PC. Please check the “Monitor and Trace” section (page 145) of the Web GUI User Guide available at http://docs.oracle.com/cd/E56581_01/index.htm

Telnet

Since we are working within an architecture which uses bound TCP listening ports for functionality, the simplest form of troubleshooting can be seeing if the devices are listening on a particular port, as well as confirming that the there is nothing blocking them such as firewalls. Ensure that you have a TELNET client available on a workstation as well as on the Lync Server mediation server.

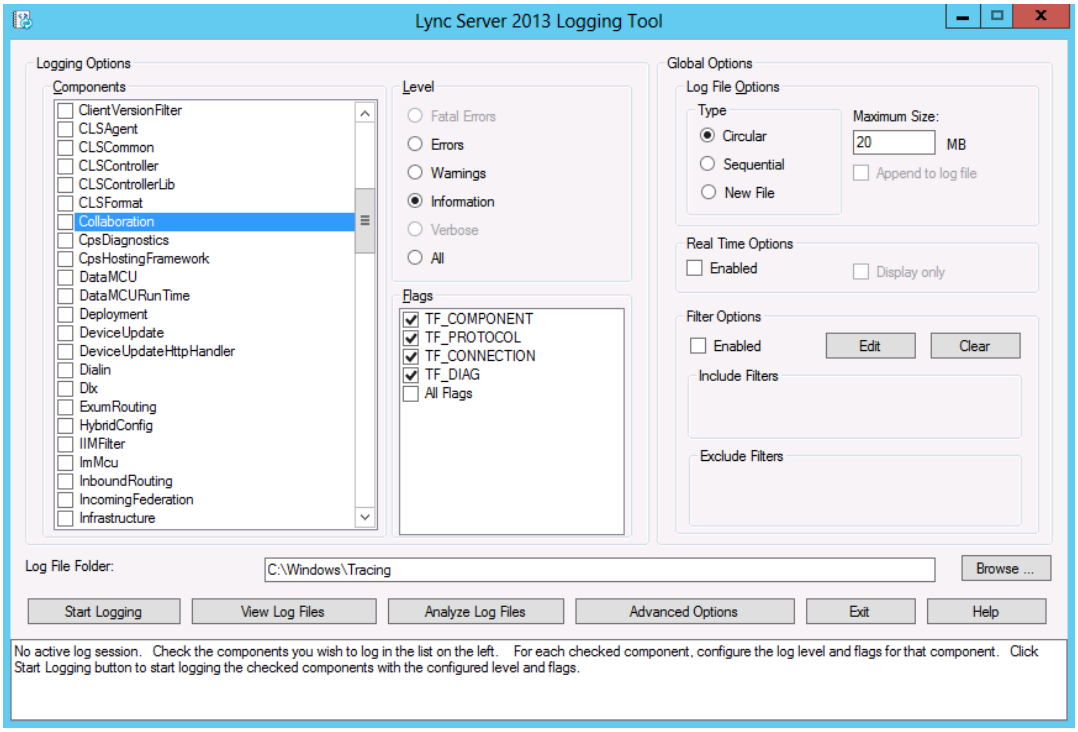
The Lync Server mediation server will listen on TCP port 5067 by default for SIP signaling. In our example we are listening on 5060 on the PSTN facing NIC. From the Standard Edition pool or Enterprise Edition pool the Mediation Server would be listening on port 5061. Tests may include:

- Client to pool server: **`telnet <servername> 5061`**
- Pool server to Mediation Server: **`telnet <servername> 5061`**

On the Lync Server

Lync Server Logging Tool

The Skype for Business Logging Tool provides internal traces and messaging between different Skype for Business elements like Front-end, Mediation server, Lync Clients, etc. File name is OCSReskit.msi. Once installed, it can be accessed from any one of the Lync Server servers by running Start/Microsoft Skype for Business/Lync Server Logging Tool.



Appendix A

Accessing the ACLI

Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH, this must be explicitly configured.

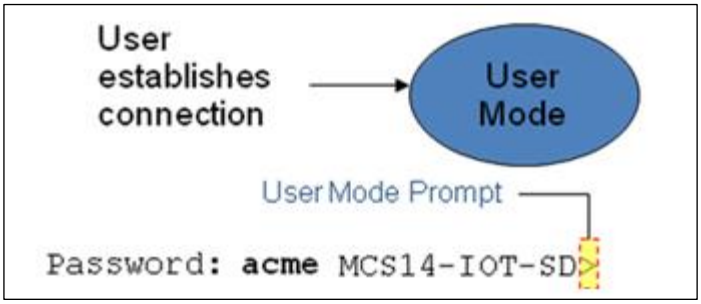
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

ACLI Basics

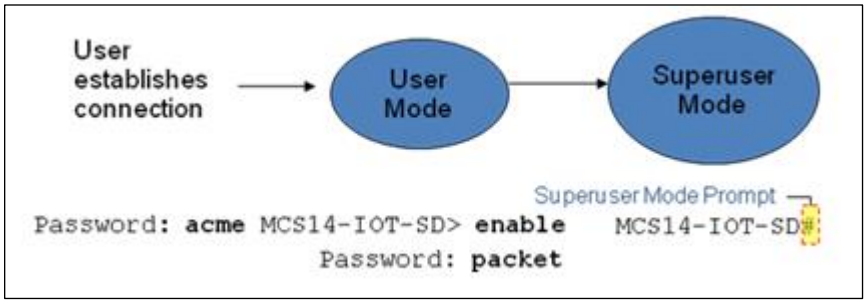
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the SBC, the prompt for the User mode password appears. The default password is acme.

User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.



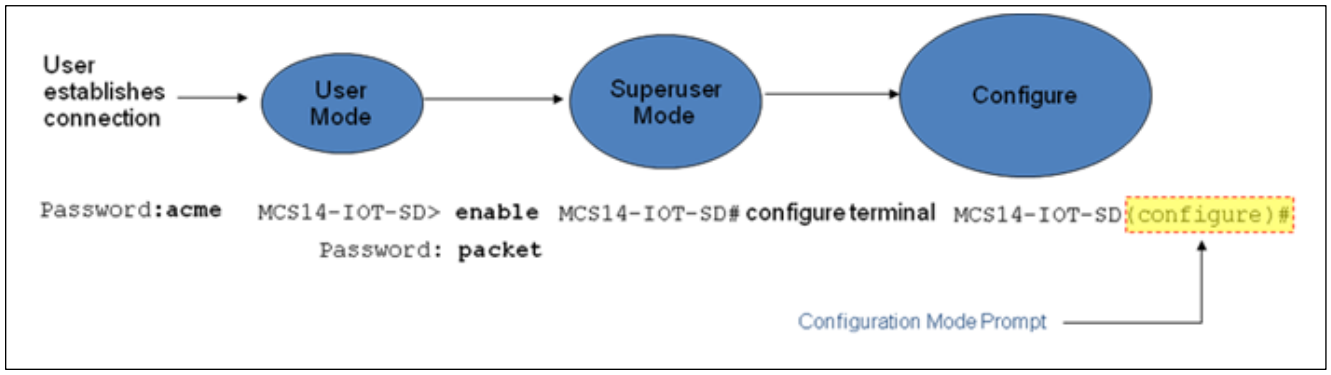
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

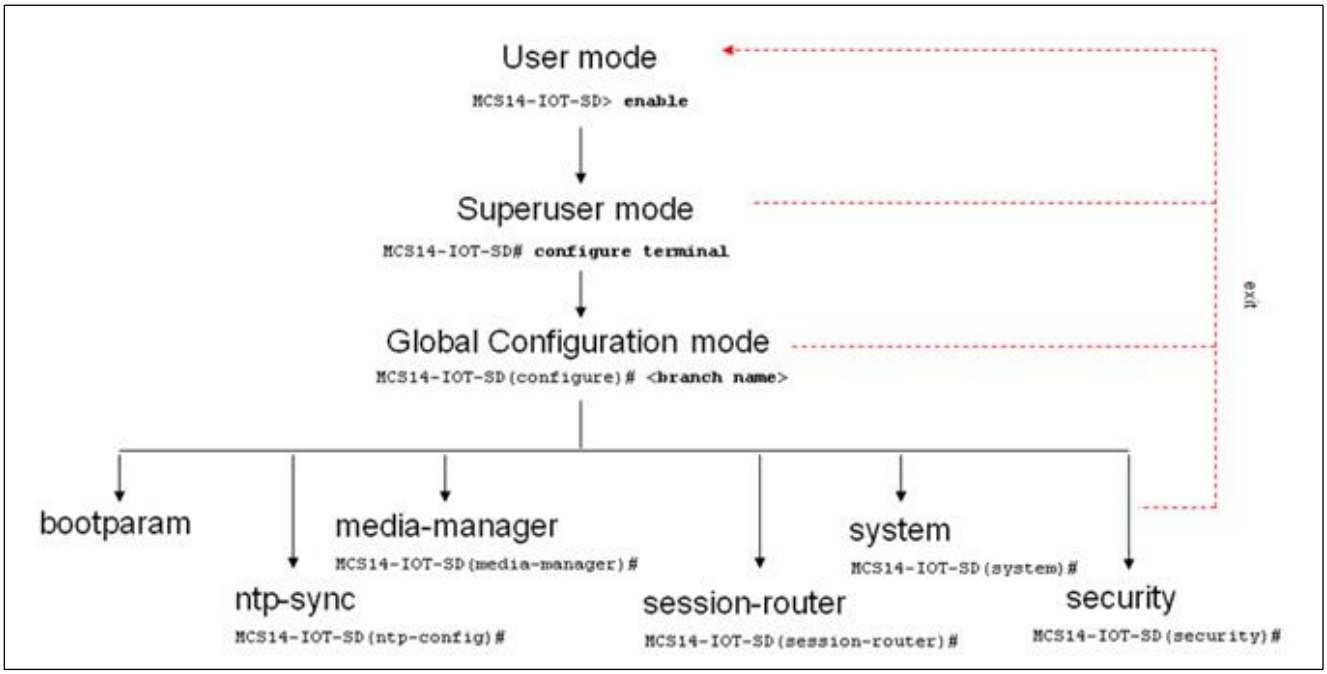
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **oraclesbc1(configure)#**. To return to the Superuser mode, issue the **`exit`** command.



In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.



The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to SBC boot parameters. Key boot parameters include:

- boot device – The global management port, usually eth0
- file name – The boot path and the image file.
- inet on ethernet – The IP address and subnet mask (in hex) of the management port of the SD.
- host inet –The IP address of external server where image file resides.
- user and ftp password – Used to boot from the external FTP server.
- gateway inet – The gateway IP address for reaching the external server, if the server is located in a different network.

```
'.' = clear field;  '-' = go to previous field;  q = quit
boot device             : eth0
processor number        : 0
host name               :
file name               : /tffs0/nnSCX620.gz
inet on ethernet (e)    : 10.0.3.11:ffff0000
inet on backplane (b)   :
host inet (h)           : 10.0.3.100
gateway inet (g)        : 10.0.0.1
user (u)                : anonymous
ftp password (pw) (blank = rsh)       : anonymous
flags (f)               : 0x8
target name (tn)        : MCS14-IOT-SD
startup script (s)      :
other (o)
```

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the SBC time and date.

The security branch provides access to security configuration.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, iwf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media-manager, and so forth.

You will use media-manager, session-router, and system branches for most of your working configuration.

Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element - for example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- SIP-ports - are children of the sip-interface element
- peers – are children of the redundancy element
- destinations – are children of the peer element

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the **show** command before issuing the **done** command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the **done** command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the **exit** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

1. Enter the element that you will edit at the correct level of the ACLI path.
2. Select the element that you will edit, and view it before editing it.
   The **select** command loads the element to the volatile memory for editing. The **show** command allows you to view the element to ensure that it is the right one that you want to edit.
3. Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.
4. It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the **show** command before issuing the **done** command.
5. On completion, you must issue the **done** command.
6. Issue the **exit** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

Deleting an Element

The **no** command deletes an element from the configuration in editing.

To delete a single-instance element,

1. Enter the **no** command from within the path for that specific element
2. Issue the **exit** command.

To delete a multiple-instance element,

1. Enter the **no** command from within the path for that particular element.
   The key field prompt, such as <name>:<sub-port-id>, appears.
2. Use the <Enter> key to display a list of the existing configured elements.

3. Enter the number corresponding to the element you wish to delete.
4. Issue the **`select`** command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the SBC: the edited configuration, the saved configuration, and the running configuration.

- The **edited configuration** – this is the version that you are making changes to. This version of the configuration is stored in the SBC's volatile memory and will be lost on a reboot.
  To view the editing configuration, issue the **`show configuration`** command.
- The **saved configuration –** on issuing the **`save-config`** command, the edited configuration is copied into the non-volatile memory on the SBC and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.
- The **running configuration** is the saved then activated configuration. On issuing the **`activate-config`** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect.
  To view the running configuration, issue command show **`running-config`**.

Saving the Configuration

The **`save-config`** command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the **`save-config`** command, the SBC displays a reminder on screen stating that you must use the **`activate-config`** command if you want the configurations to be updated.

```
oraclesbc1 # save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
oraclesbc1 #
```

Activating the Configuration

On issuing the **`activate-config`** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration.

Some configuration changes are service affecting when activated. For these configurations, the SBC warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
oraclesbc1# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc1#
```


Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services