Troubleshooting Guide for Cisco Webex Hybrid Call Service Connect

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Call Set-Up Issues
Mutual TLS Handshake Failures
Useful Mutual TLS Troubleshooting Tips
Issue 1. Expressway-E does not Trust Certificate Authority (CA) that signed Cisco Webex Certificate
Solution
Issue 2. Incorrect Name for TLS Subject Verify Name on Expressway-E Cisco Webex Hybrid DNS Zone
Solution
Issue 3. Expressway-E does Not Send Full Certificate Chain to Cisco Webex
Solution
Issue 4. Firewall Terminates Mutual TLS Handshake
Solution
Issue 5. Expressway-E is Signed by Public CA but Cisco Webex Control Hub has Alternate Certificates Loaded
Solution
Issue 6. Expressway is not Mapping Inbound Call to Cisco Webex Hybrid DNS Zone
Solution
Issue 7. Expressway-E uses Default Self-Signed Certificate
Solution
Inbound: Cisco Webex to On-Premises
Issue 1. Cisco Webex is unable to resolve the Expressway-E DNS SRV/hostname
Solution
Alternate Solution
Issue 2. Socket Failure: Port 5062 is Blocked Inbound to Expressway
Solution
Issue 3. Socket Failure: Expressway-E is not Listening on Port 5062
Solution
Issue 4. Expressway-E or C does not Support Preloaded SIP Route Headers
Solution
Issue 5. Cisco Webex app is receiving two call notifications (toasts)
Solution
Outbound: On-Premises to Cisco Webex
Issue 1. Expressway is unable to resolve the callservice.ciscoWebex.com address
Introduction

This document describes the Cisco Webex Hybrid Call Service Connect solution that allows your existing Cisco call control infrastructure to connect to the Cisco Collaboration Cloud so that they can work together.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of the Cisco Webex Offer
- Knowledge of the Expressway solution (B2B)
- Knowledge of Cisco Unified Communications Manager (Unified CM) and its integration with Expressway
- Unified CM 10.5(2) SU5 or later.
- Expressway (B2B) version X8.7.1 or later (X8.9.1 is recommended)
- Expressway (Connector Host) -- see Expressway Connector Host Support for Cisco Webex Hybrid Services for the currently supported versions

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Communications Manager
- Expressways
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

**Background Information**

The solution offers these capability:

- Use the Cisco Webex Teams app as a mobile soft client for audio and video calls
- Use the app to make and receive calls from anywhere, as if they were in the office
- Use Cisco Webex Teams, Cisco Jabber, or their desk phone to call, without the need to worry about which option they use
- Unlock call history in on-premise phones and integrate that history in Cisco Webex Teams

The scope of this guide is to cover issues that are unique to Hybrid Call Service Connect. Since Hybrid Call Service Connect runs over the same Expressway E & C pair as other solutions such as Mobile and Remote Access and Business to Business calling, issues with the other solutions can affect Hybrid Call Service Connect. For customers and partners who deploy an Expressway pair for use with Call Service Connect, the Cisco VCS Expressway and VCS Control Basic Configuration guide must be referenced before you attempt to deploy Hybrid Call Service Connect. This troubleshooting guide covers Firewall/NAT considerations along with Expressway design in both Appendix 3 & 4. Review this documentation thoroughly. Additionally, this document assumes that the Expressway connector host and Hybrid Call Service activation were completed.

**Call Set-Up Issues**

**Mutual TLS Handshake Failures**

Hybrid Call Service Connect uses mutual transport layer security (mutual TLS) for authentication between Cisco Webex and the Expressway-E. This means that both the Expressway-E and Cisco Webex check and inspect the certificate that each other present. Since mutual TLS issues are so prevalent during new deployments of the Expressway servers and the enablement of solutions such as Hybrid Call Service Connect, this section provides useful information and tips for troubleshooting certificate based issues between the Expressways and Cisco Webex.

What does the Expressway-E check?

- Was the Cisco Webex certificate signed by a Public CA that is listed in the Expressway-E Trusted CA list?
- Is callservice.ciscoWebex.com present in the Subject Alternate Name field of the Cisco Webex certificate?
What does Cisco Webex check?

- Has the Expressway-E certificate been signed by one of the Public CAs that Webex trusts. *(Cisco Webex Trusted CA List)*
- If the Expressway-E does not use a publicly signed certificate, was the Expressway certificate along with any root and intermediate certificates uploaded to the Cisco Webex Control Hub *(https://admin.ciscoWebex.com)*?

This is explained as shown in the image.

Useful Mutual TLS Troubleshooting Tips

1. Decode Mutual TLS Handshake

By default, Wireshark marks SIP TLS traffic as port 5061. What this means is that any time you want to analyze a (mutual) TLS handshake that occurs over port 5062, Wireshark won't know how to decode the traffic properly. Here is an example of the Mutual TLS handshake that's occurring over port 5062 as shown in the image.

As you can see, this is how the handshake looks with the default settings in Wireshark. Packet number 175 is the certificate the Expressway sends to Cisco Webex. However, you can't determine that without the traffic being decoded. There are two methods that you can use to decode this traffic so that you can more easily see the certificate information and any error messages that are present.

1a. Decod the Stream as SSL

a. When you analyze the Mutual TLS handshake, first filter the capture by `tcp.port==5062`. After
this, right-click the first packet in the stream and select **Decode As...** as shown in the image.

b. Once the **Decode As...** option is selected, you see a list where you can select how to Decode the stream you've selected. From the list, select **SSL**, click **Apply**, and close the window. At this point, the entire stream shows the certificate and error messages exchanged at the time of the handshake as shown in the image.

1b. Adjust SIP TLS Port

When you adjust the SIP TLS port to 5062 in the Wireshark preferences, you can then see all the details that surround the handshake, which includes the certificates. In order to make this change:

- Open Wireshark
- Navigate to **Edit > Preferences**
- Expand Protocols and select **SIP**
- Set the SIP TLS Port to 5062 and click **Apply**
Set the value back to 5061 when analysis is completed as shown in the image.

If you analyze the same capture now, you see packets 169 through 175 decoded. Packet 175 shows the Expressway-E certificate and if you drill down on the packet, you can see all the certificate details as shown in the image.

2. Wireshark Filtering

When you analyze packet captures, it's easy to get lost in the sheer amount of packets observed in a given capture. It's important to understand what type of traffic you're most interested in so that you can filter Wireshark to display just that. Here are some common Wireshark filters that can be used to get details about a mutual TLS handshake:

- tcp.port==5062
- ssl && tcp.port==5062
- ssl.handshake.certificate && tcp.port==5062

3. Extract Certificate from Pcap

From time to time, you may need to get a copy of a certificate (server, root, or intermediary). If you do not know where to find the certificate you're in search for, you can extract it directly from a packet capture. Here are the steps for how to pull the Cisco Webex certificate that is presented at a mutual TLS handshake.

1. Filter the packet capture with ssl.handshake.certificate && tcp.port==5062
2. Locate the packet that is sourced from the Webex server address and has Certificate printed in the Info section.
3. In the packet details expand Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificates Note: The bottom/last certificate in the chain is the root CA.
4. Right-click the certificate of interest and select Export Selected Packet Bytes... as shown in the image.
5. Save the file as a .cer.

6. Double-click the saved file to open the certificate as shown in the image.
4. Adjust Expressway Logging Levels

Two logging modules are available on the Expressway which can help you better understand what logic the Expressway performs when you analyze the certificates:

- developer.ssl
- developer.zone.zonemgr

By default, these logging modules are set to an INFO level. When set to a DEBUG level, you can begin to see the information about the certificate inspection that happens, along with what zone traffic gets mapped to. Both of these functions are relevant to Hybrid Call Service.

Example of the Expressway-E that conducts a SAN inspection of Cisco Webex's server certificate.

```
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.ssl" Level="DEBUG" CodeLocation="ppc mains/ssl/ttsl/ttsl_openssl.cpp(1960)" Method="::ttssl_cont inueHandshake" Thread="0x7f5f76cbee700":  Detail="Handshake succeeded"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.ssl" Level="DEBUG" CodeLocation="ppc mains/ssl/ttsl/ttsl_openssl.cpp(1629)" Method="::TTSSL_retrieveCommonName" Thread="0x7f5f76cbee700": Detail="Found common name in peer certificate" CommonName="l2sip-cfa-01.ciscoWebex.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.ssl" Level="DEBUG" CodeLocation="ppc mains/ssl/ttsl/ttsl_openssl.cpp(1654)" Method="::TTSSL_retrieveAltNames" Thread="0x7f5f76cbee700": Detail="Found DNS alt-name in peer certificate" AltName="l2sip-cfa-01.ciscoWebex.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.ssl" Level="DEBUG" CodeLocation="ppc mains/ssl/ttsl/ttsl_openssl.cpp(1654)" Method="::TTSSL_retrieveAltNames" Thread="0x7f5f76cbee700": Detail="Found DNS alt-name in peer certificate" AltName="l2sip-cfa-01.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.ssl" Level="DEBUG" CodeLocation="ppc mains/ssl/ttsl/ttsl_openssl.cpp(1654)" Method="::TTSSL_retrieveAltNames" Thread="0x7f5f76cbee700": Detail="Found DNS alt-name in peer certificate" AltName="callservice.ciscoWebex.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.ssl" Level="DEBUG" CodeLocation="ppc mains/ssl/ttsl/ttsl_openssl.cpp(1654)" Method="::TTSSL_retrieveAltNames" Thread="0x7f5f76cbee700": Detail="Found DNS alt-name in peer certificate" AltName="callservice.call.ciscoWebex.com"
```

Example of the Expressway-E mapping the MTLS connection to the Cisco Webex Hybrid DNS Zone

```
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.zone.zonemgr" Level="DEBUG" CodeLocation="ppc mains/oak/ zones/ZoneManager.cpp(1226)" Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" getDNSZoneByTLSVerifySubjectName classified subject name callservice.ciscoWebex.com into DNS zone Hybrid Call Services DNS
```
Here is a list of the most common issues that are related to mutual TLS failures between the Expressway-E and Cisco Webex.

**Issue 1. Expressway-E does not Trust Certificate Authority (CA) that signed Cisco Webex Certificate**

The Cisco Webex server that is in direct communication with the Expressway-E is called an L2SIP server. This L2SIP server is to be signed by an intermediary server with a common name of **Hydrant SSL ICA G2**. The intermediary is signed by a root certificate authority that has a common name of **QuoVadis Root CA 2** as shown in the image.

**Note:** This could be subject to change.
The first step to analyze this traffic from the Expressway diagnostic perspective is to search for **TCP Connecting**. After you search **TCP Connecting**, you'll look for the **Dst-port=5062** value.

Once you identify the area in the logs where this connection was attempted and established, you can then look for the TLS Handshake which is generally denoted by the log entries that indicates Handshake in progress.

```
Reason="want read/write"
```

If the Expressway-E does not trust the Cisco Webex signed certificates, you can expect that the Expressway-E can reject the certificate immediately after the handshake completes. This can be spotted in the Expressway-E logging by these log entries:

```
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2" Dst-port="5062" Detail="self signed certificate in certificate chain" Protocol="TLS" Level="1" UTCTime="2017-09-20 14:49:18,724"
```

The Expressway error message can slightly mislead because it refers to a self signed certificate in
the certificate chain. Wireshark allow you to take a closer look at the exchange. From a wireshark packet capture analysis perspective, you can clearly see that when the Webex environment presents its certificate then Expressway turns around and rejects with certificate with a Unknown CA error as shown in the image.

Solution

In order to resolve this situation, you must ensure that the Expressway-E trusts the Cisco Webex certificate authorities. While you could simply extract these certificates from a wireshark trace and upload them to the Trusted CA certificate store on the Expressway, the Expressway offers a simpler method:

- Log into the Expressway-E
- Navigate to Applications > Cloud Certificate management
- Select Get Certificates option as shown in the image.

At this point, the Cisco Webex certificate authorities are uploaded to the Expressway-E Trusted CA store (Maintenance > Security > Trusted CA certificate).

Issue 2. Incorrect Name for TLS Subject Verify Name on Expressway-E Cisco Webex Hybrid DNS Zone

As part of the mutual TLS handshake, Hybrid Call Service Connect uses TLS Verification. This means that in addition to trusting the Cisco Webex CA certificates, the Expressway verifies the certificate by checking the Subject Alternate Name (SAN) field of the certificate that is presented to ensure it has a value such as callservice.ciscoWebex.com present. If this value is not present, the inbound call fails.

In this particular scenario, the Cisco Webex server present its certificate to the Expressway-E. The certificate actually has 25 different SANs. Consider the case where the Expressway-E checks the certificate for the callservice.ciscoWebex.com SAN but doesn't find that. When this condition is met, you can see an error similar to this within the diagnostic logging:
2017-09-20T11:42.701-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2" Dst-port="5062" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1" UTCTime="2017-09-20 15:17:42,700"

2017-09-20T11:42.701-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 15:17:42,700" Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2" Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was unacceptable"

If you use wireshark to analyze this certificate handshake, you can find that after Cisco Webex presents its certificate, the Expressway RSTs the connection shortly after as shown in the image.

In order to confirm the configuration of this value, you can go to the Webex Hybrid DNS Zone that was configured for the solution. If you have the Expressway-E xConfiguration, you can look for the Zone configuration section to determine how the TLS verify subject name was configured. For xConfiguration, note that the zones are ordered with Zone 1 being the first. Here is an xConfiguration from the problematic environment analyzed above.

```
xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "calllservice.Webex.com"
```

As you can see in the example above the TLS Verify Subject Name is set to calllservice.Webex.com instead of calllservice.ciscoWebex.com.

**Solution**

In order to resolve this issue, the TLS Verify Subject Name must be modified:

- Log into the Expressway-E
- Navigate to Configuration > Zones > Zones
- Select Webex Hybrid Services DNS Zone
- Set the TLS verify subject name to calllservice.ciscoWebex.com
- Select Save

Note: See thefor baseline logging behavior. This section shows the Expressway performing certificate verification and the mapping to the Webex Hybrid DNS Zone.

### Issue 3. Expressway-E does Not Send Full Certificate Chain to Cisco Webex

As part of the mutual TLS handshake, Cisco Webex must trust the Expressway-E certificate. Cisco Webex has a full list of public CAs that it trusts. Typically, a TLS handshake is successful when your Expressway-E certificate is signed by a public CA that Cisco Webex supports. By design, the
Expressway-E only sends its certificate during a TLS handshake despite being signed by a public CA. In order to send the full chain of certificates (root and intermediate), those certificates must be added to the Trusted CA certificate store on the Expressway-E itself.

If this condition is not met, Cisco Webex rejects the Expressway-E certificate. When you troubleshoot a condition that matches this problem, you can use the diagnostic logs and tcpdump from the Expressway-E. When you analyze the Expressway-E diagnostic logs, you'll see an error similar to that here:

```
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1"
```

If you analyze this from a Wireshark perspective, you see that the Expressway-E presents its certificate. If you expand the packet, you can see that only the server certificate is sent. Cisco Webex then rejects this TLS handshake with an Unknown CA error message as shown in the image.

**Solution**

In order to address the issue in this scenario, you must upload the intermediate and root CAs that are involved in the signing of the Expressway-E certificate to the Trusted CA certificate store:

1. **Step 1.** Log into the Expressway-E.
2. **Step 2.** Navigate to **Maintenance > Security > Trusted CA certificate**.
3. **Step 3.** Select **Choose File** under the Upload menu near the bottom of the UI.
4. **Step 4.** Choose the CA certificate that was involved in the signing of the Expressway-E.
5. **Step 5.** Select **Append CA Certificate**.
6. **Step 6.** Repeat steps for all CA certificates involved in the signing of the Expressway-E certificate (Intermediate, Root).
7. **Step 7.** Select **Append CA Certificate**.
Once this process is completed, you see that the full chain of certificates involved in signing the Expressway-E server certificate included in the key exchange. Here is a sample of what you would see if you analyzing a packet capture with Wireshark.

**Issue 4. Firewall Terminates Mutual TLS Handshake**

The Expressway solution typically interfaces with a firewall. Many times, the inline firewall for the solution is runs some type of application layer inspection. Often with the Expressway solution, when the firewall runs application layer inspection, administrators see an undesirable results. This particular issue helps you identify when a firewall's application layer inspection abruptly tore down the connection.

With the use of the diagnostic logs from the Expressway, you can look for the attempted Mutual TLS handshake. This handshake, as mentioned earlier, should come shortly after the TCP Connection is established over port 5062. In this scenario, when the firewall tears down the connection, you see these errors within the diagnostic logging.

Thread="0x7f6496669700": TTSSL_continueHandshake: Failed to establish SSL connection iResult="-1" error="5" bServer="false" localAddress="[IPv4]'TCP'172.17.31.10:28351'"

From a packet capture perspective, you'll see that the Expressway-E presents its certificate to Cisco Webex. You see a TCP RST come in from the direction of Cisco Webex as shown in the image.
At first glance, you may think something is wrong with the Expressway-E certificate. In order to troubleshoot this issue, you first have to determine answers to these questions:

- Is the Expressway-E signed by a Public CA that Cisco Webex trusts?
- Is the Expressway-E certificate and any certificates involved in the signing of the Expressway-E certificate manually uploaded to the Cisco Webex Control Hub (https://admin.ciscoWebex.com)?

In this particular condition, the solution was not to use the Cisco Webex Control Hub to manage the Expressway-E certificates. This mean the Expressway-E certificate must be signed by a public CA that Cisco Webex trusts. By selecting on the Certificate packet in the Wireshark capture (as illustrated above), you can see that the certificate was signed by a Public CA and that the full chain was sent to Cisco Webex. Therefore, the issue should not be related to the Expressway-E certificate.

At this point, if further isolation is required, you could take a packet capture off the outside interface of the firewall. However, the lack of SSL error in the diagnostic log is an important data point. If you recall above (Issue 3.), if Cisco Webex doesn’t trust the Expressway-E certificate, you must see some type of SSL disconnect reason. In this condition, there was no SSL error available.

**Note:** If you were to get a packet capture off the firewall outside interface you would not see a TCP RST coming in from the Cisco Webex environment.

**Solution**

For this particular solution, you as a partner or customer must rely on your security team. The team must investigate if they use any sort of application layer inspection for the Expressway solution and if they are, this should be disabled. Appendix 4 of the VCS Control and Expressway Deployment Guide explains why it is recommended customers turn off this functionality.

**Issue 5. Expressway-E is Signed by Public CA but Cisco Webex Control Hub has Alternate Certificates Loaded**

This particular condition can often occur when you deployed the Expressway solution from scratch and you do not have the Expressway-E certificate signed by a public CA initially. What happens in this scenario is that you upload the Expressway-E server certificate (which has been signed internally) to the Cisco Webex Control Hub so that you can complete the mutual TLS negotiation successfully. Afterwards, you end up getting the Expressway-E certificate signed by a Public CA,
however you forget to remove the server certificate from the Cisco Webex Control Hub. It's important to know that when a certificate is uploaded to the Cisco Webex Control Hub, that certificate takes priority over what certificate and chain the Expressway presents during the TLS handshake.

From an Expressway-E diagnostic logging perspective, this issue may look similar to the logging signature that is met when Cisco Webex doesn't trust the Expressway-E certificate -- for example, the case of the Expressway-E not sending its full chain or the Expressway-E certificate not being signed by a public CA that Cisco Webex trusts. Below is a sample of what you can expect in the Expressway-E logging during the TLS handshake:

```

2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13.668" Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)" Method="::TTSSLErrorOutput" Thread="0x7f4a2c16f700" TTSSL_continueHandshake: Failed to establish SSL connection iResult="0" error="1" bServer="true" localAddress="[IPv4]'TCP'"172.16.2.2:5062]'" remoteAddress="[IPv4]'TCP'"146.20.193.45:48520]'" ssl_error_reason="error:14094416:SSL routines:sslv3_read_bytes:sslv3 alert certificate unknown"

```

Take a look at this from the Wireshark perspective you can see here that the Expressway-E presents its certificate in line item 175. A few line items later, the Cisco Webex environment rejects the certificate with a Certificate Unknown error as shown in the image.

If you select the Certificate packet that the Expressway-E sends, you can expand the certificate information to determine if the Expressway-E certificate:

1. is signed by a Public CA that Cisco Webex trusts, and
2. is including its full chain involved in the signing.

In this situation, both of these conditions are met. This suggests there is nothing wrong with the Expressway-E certificate.

**Solution**
Step 1. Log into the Cisco Webex Control Hub.
Step 2. Select Services from the left pane.

Step 3. Choose Settings under the Hybrid Call card.

Step 4. Scroll to the Call Service Connect section and look under the Certificates for Encrypted SIP Calls to see if undesired certificates are listed. If so, click the trash can icon next to the certificate.

step 5. Select Remove.

Note: It is important that the analysis is conducted and it is determined that the customer is not using the certificates uploaded to the Webex Control Hub prior to removing them.

For more information about uploading your Expressway-E certificate in the Cisco Webex Control Hub, check this section of the Hybrid Call Deployment Guide.

Issue 6. Expressway is not Mapping Inbound Call to Cisco Webex Hybrid DNS Zone

The Inbound TLS mapping feature works in conjunction with the TLS Verify Subject Name, both of which are configured on the Hybrid Call DNS Zone. The feature breaks down into a three step process:

1. Expressway-E accepts the Cisco Webex certificate.
2. Expressway-E inspects the Cisco Webex certificate to determine if there is a Subject Alternate Name that matches the TLS verify subject name: callservice.ciscoWebex.com.
3. Expressway-E maps the inbound connection through the Cisco Webex Hybrid DNS Zone.

If authentication is not successful, this means that the certificate validation failed. The call enters into the Default Zone and is routed according to the search rules provided for business-to-business scenarios, if business-to-business is configured on Expressway-E.

Like the other scenarios, you must use both the diagnostic logging and packet captures to determine what this failure looks like, then use the packet capture to see which side is sending the RST. Here is a sample of the TCP Connection being attempted, then establishing.

```
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471" Module="network.tcp" Level="DEBUG":  Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2" Dst-port="5062" Detail="TCP Connecting"
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471" Module="network.tcp" Level="DEBUG":  Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2" Dst-port="5062" Detail="TCP Connection Established"
```

Now that the TCP connection has established, the TLS Handshake can ensue. You can see shortly after the handshake starts, it quickly errors out.

```
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2" Dst-port="5062" Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
```
Look at this situation from a pcap perspective, you can get a better sense of

- who is sending the RST, and
- what certificates are being passed to determine if they are correct.

When you analyze this particular capture, you can see that the Expressway-E sends the RST. When you look at the Cisco Webex certificate that is passed, you can see that it sends the full chain. Additionally, you can conclude that based on the error message in the diagnostic log, you can rule out the scenario where the Expressway-E doesn’t trust the Cisco Webex Public CAs. Otherwise, you would see an error like "self signed certificate in certificate chain". You can dig into the packet details as shown in the image.

By click the Webex server certificate and expanding it to see the Subject Alternate Names (dnsName) you can verify to ensure it has callservice.ciscoWebex.com listed.

Navigate to Wireshark: Certificate > Extension > General Names > GeneralName > dnsName: callservice.ciscoWebex.com

This fully confirms that the Webex certificate looks just fine.

You can now confirm that the TLS Verify Subject Name is correct. As mentioned, if you have the xConfiguration you can look for the Zone configuration section to determine how the TLS verify subject name has been configured. One thing to note about the xConfiguration is that the zones are ordered with Zone 1 is the first created. Here is an xConfiguration from the problematic environment analyzed above. It’s clear that nothing is wrong with the TLS Verify Subject Name.

* c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
* c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscoWebex.com"

The next thing that must be investigated is the TLS verify inbound mapping. This confirms if you are correctly mapping the TLS connection to the Webex Hybrid DNS Zone. The xConfiguration can be leveraged to analyze this as well. In the xConfiguration the TLS verify inbound mapping is called DNS ZIP TLS Verify InboundClassification. As you can see in this example the value is set to Off.
Given that this value is set to Off, what this means is that the VCS is prevented from attempting to map inbound TLS connections to this zone. The call thus enters into the Default Zone and is checked and routed according to the search rules provided for business-to-business scenarios, if business-to-business is configured on Expressway-E.

Solution

In order to address this you need to set the TLS verify inbound mapping on the Hybrid Call DNS Zone to On. Here are the steps to complete that.

1. Log into the Expressway-E
2. Navigate to Configuration > Zones > Zones
3. Select Hybrid Call DNS Zone
4. For the TLS verify inbound mapping, choose On
5. Select Save

Note: See the for baseline logging behavior. This section shows the Expressway performing certificate verification and the mapping to the Webex Hybrid DNS Zone.

Issue 7. Expressway-E uses Default Self-Signed Certificate

In some new deployments of Hybrid Call Service Connect, the signing of the Expressway-E certificate is overlooked or it's believed that the default server certificate can be used. Some people think that this is possible because the Cisco Webex Control Hub lets you load a custom certificate into the portal. (Services > Settings (Under Hybrid Call card) > Upload (Under Certificates for Encrypted Calls))

If you pay close attention to the wording about the Certificates for Encrypted SIP Calls, you see this: 'Use certificates provided from the Cisco Collaboration default trust list or upload your own. If you use your own, ensure the hostnames are on a verified domain.' The key piece to that statement is "make sure hostnames are on a verified domain."

When you troubleshoot an issue that matches this condition, keep in mind that the symptom is going to be dependent on the direction of the call. If the call originated by an on-premises phone, you can expect that the Cisco Webex app would not ring. Also, if you tried to trace the call from the Expressways Search History, you'd find that the call would make it to the Expressway-E and stop there. If the call originated from a Cisco Webex app and was destined for the premises, the on-premises phone does not ring. In that instance, the Expressway-E and Expressway-C Seach History would not show anything.

In this particular scenario, the call originated from an on-premises phone. Using the Expressway-E Search History, you can determine that the call made it to the server. At this point, you can dive into the diagnostic logging to determine what happened. To start this analysis, first look to see if a TCP Connection was attempted and established over port 5062. By searching the Expressway-E diagnostic logs for "TCP Connecting" and searching the line item with the tag "Dst-port=5062", you can determine if the connection establishes.
Now that you confirmed the TCP Connection established, you can analyze the mutual TLS handshake that happens immediately after. As you can see in the snippet here, the handshake fails and the certificate is unknown (Detail="sslv3 alert certificate unknown")

Take a closer look at the packet capture provided with the Expressway-E diagnostic logging, you can see that the Certificate Unknown error is getting sourced from the direction of Cisco Webex as shown in the image.

If you inspect the Default Server certificate from the Expressway-E, you can see that the ‘Common Name’ and ‘Subject Alternate Names’ do not contain the ‘Verified Domain’ (rtp.ciscotac.net). You then have evidence about what causes this issue as shown in the image.
At this point, you determined that the Expressway-E server certificate needs to be signed by either a Public CA or an Internal CA.

Solution

In order to resolve this issue, you have two options:

1. Have the Expressway-E certificate be signed by a Public CA that Cisco Webex trusts.
   - Log into the Expressway. Navigate to Maintenance > Security > Server certificate. Select Generate CSR. Enter the required certificate information and ensure that the Additional alternative names field contains the Verified Domain listed in the Webex Control Hub. Click Generate CSR. Provide the CSR to a 3rd party Public CA for signing. Upon return of the certificate, Navigate to Maintenance > Security > Server certificates. In the Upload New Certificate section next to Select the server certificate file, select Choose File and select the signed certificate. Select Upload server certificate data. Navigate to Maintenance > Security > Trusted CA certificate. In the Upload section next to Select the file containing trusted CA certificates select Choose File. Select any root and intermediate CA certificates provided by the Public CA. Select Append CA certificate. Restart the Expressway-E.

2. Have the Expressway-E certificate be signed by an Internal CA and then upload the Internal CA and Expressway-E to the Cisco Webex Control Hub.
2a. Upload the Internal CA and Expressway-E certificate to the Cisco Webex Control Hub
   1. Log into the [Cisco Webex Control Hub](#) as an Administrator.
   2. Select **Services**.
   3. Select **Settings** under the Hybrid Call Service card.
   4. In the **Certificates for Encrypted SIP Calls section** select **Upload**.
   5. Choose the Internal CA and Expressway-E certificates.

**Inbound: Cisco Webex to On-Premises**

Almost every inbound Cisco Webex to on-premises failure results in the same reported symptom: "When I call from my Cisco Webex app to another colleague's app, the colleague's app rings but the on-premises phone does not." In order to troubleshoot this scenario, you'll find it helpful to understand both the call flow and logic that occur when this type of call is being placed.

**High Level Logic Flow**

1. Cisco Webex app calling party initiates the call
2. Called party's app rings
3. The call is forked to the Cisco Webex environment
4. The Cisco Webex environment must perform a DNS Lookup based on the customer's configured SIP Destination in the Cisco Webex Control Hub
5. The Cisco Webex environment attempts to connect to the Expressway over port 5062
6. The Cisco Webex environment attempts to perform a mutual TLS handshake
7. The Cisco Webex environment sends a SIP INVITE to the Expressway which is passed down to the on-premises collaboration endpoint/IP phone
8. Cisco Webex and the enterprise complete the SIP negotiation
9. Cisco Webex and the enterprise begin sending and receiving media.

**Call Flow**

Navigate to [Cisco Webex app](#) > [Cisco Webex environment](#) > [Expressway-E](#) > [Expressway-C](#) > [On-Premises Collaboration Endpoint/IP Phone](#) as shown in the image.
Here are some of the common issues observed with Inbound calls from Webex to the on-premises infrastructure.

**Issue 1. Cisco Webex is unable to resolve the Expressway-E DNS SRV/hostname**

When thinking about the Cisco Webex to on-premises call flow, Cisco Webex’s first logical step is how to contact the on-premises Expressway. As noted above, Cisco Webex will attempt to connect to the on-premises Expressway by performing an SRV lookup based on the configured SIP Destination that is listed in the Hybrid Call Service Settings page in the Cisco Webex Control Hub.

If you attempt to troubleshoot this situation from an Expressway-E diagnostic log perspective, you do not see any traffic from Cisco Webex. If you try to search for TCP Connecting, you would not see the Dst-port=5062, nor would you see any subsequent MTLS handshake or SIP Invite from Cisco Webex.

If this is the situation, you must check how the SIP Destination was configured in the Cisco Webex Control Hub. You can also use the Hybrid Connectivity Test Tool to aid in troubleshooting. The Hybrid Connectivity Test Tool checks if there is a valid DNS address, if Cisco Webex can connect to the port returned in the SRV lookup, and if the on-premises Expressway has a valid certificate that Cisco Webex trusts.

1. Log into the Cisco Webex Control Hub
2. Select Services
3. Select the Settings link in the Hybrid Call card.
4. In the Call Service Connect section verify the domain used for the public SIP SRV address in the **SIP Destination** field.
5. If the record has been entered correct, click **Test** to see if the record is valid.
6. As pictured below, you can clearly see that the public domain does not have a corresponding SIP SRV record associated to it as shown in the image.

```
SIP Destination

mtls.rtp.ciscotac.net

⚠️ Your SIP Destination is not configured correctly. View test results
```

select **View test results** and you can see more detail about what failed as shown in the image.

As another approach, you can also look up the SRV record by using nslookup. Here are the commands you can run to verify if the SIP Destination exists.

```
C:\Users\pstojano>nslookup
  > server 8.8.8.8
  Default Server: google-public-dns-a.google.com
  Address: 8.8.8.8
  > set type=SRV
  > _sips._tcp.mtls.rtp.ciscotac.net
  Server: google-public-dns-a.google.com
  Address: 8.8.8.8
  DNS request timed out.
timeout was 2 seconds.
  DNS request timed out.
timeout was 2 seconds.
  *** Request to google-public-dns-a.google.com timed-out
```

As you can see in the code block above, the nslookup command was initiated then the server is set to 8.8.8.8 which is a public Google DNS server. Lastly, you are setting the record types to lookup to SRV records. At that point, you can then issue the full SRV record you want to look up. The net result is that the requests ultimately times out.

**Solution**

1. Configure a public SIP SRV address for the Expressway-E on the site they use to host public domain names.
2. Configure a hostname that will resolve to the public IP address of the Expressway-E
3. Configure the SIP Destination to list the domain used for the SIP SRV address created in Step 1. Log into the [Cisco Webex Control Hub](https://control.webex.com)Select **Services**Select the **Settings** link in the **Hybrid Call card**In the Call Service Connect section enter the domain used for the public SIP SRV address in the **SIP Destination** field. Select **Save**
Note: If the SIP SRV record you would like to use is already being leveraged for business-to-business communications, we recommend specifying a subdomain of the corporate domain as the SIP discovery address in Cisco Webex Control Hub, and consequently a public DNS SRV record, as follows:

Service and protocol: _sips._tcp.mtls.example.com
Priority: 1
Weight: 10
Port number: 5062
Target: us-expe1.example.com

The above recommendation was pulled directly from the Cisco Webex Hybrid Design Guide.

Alternate Solution

If the customer does not have a SIP SRV record present (and does not plan to create one), they can alternatively list the Expressway Public IP address suffixed by ":5062". By doing this, the Webex environment will not attempt an SRV lookup but rather connect directly to the %Expressway_Pub_IP%:5062. (Example: 64.102.241.236:5062)

1. Configure the SIP Destination to be formatted as %Expressway_Pub_IP%:5062. (Example: 64.102.241.236:5062) Log into the Cisco Webex Control Hub Select Services Select the Settings link in the Hybrid Call card In the Call Service Connect section enter the %Expressway_Pub_IP%:5062 in the SIP Destination field. Select Save

For more information about the SIP Destination address and/or SRV record that must be setup. Refer the Enable Hybrid Call Service Connect for Your Organization section of the Cisco Webex Hybrid Call Service Deployment Guide or the Cisco Webex Hybrid Design Guide.

Issue 2. Socket Failure: Port 5062 is Blocked Inbound to Expressway

After the DNS resolution completes, the Cisco Webex environment to attempt to establish a TCP connection over port 5062 to the IP address that was returned during the DNS lookup. This IP address is going to be the public IP address of the on-premises Expressway-E. If the Cisco Webex environment is unable to establish this TCP connection, the call inbound to the premises is subsequently fail. The symptom for this particular condition is the same as almost every other Cisco Webex inbound call failure: the on-premises phone does not ring.

If you're troubleshooting this issue using the Expressway diagnostic logs, you will not see any traffic from Cisco Webex. If you try to search for TCP Connecting, you would not see any connection attempts for the Dst-port=5062, nor would you see any subsequent MTLS handshake or SIP Invite from Cisco Webex. Since the Expressway-E diagnostic logging is of no use in this situation, you have a few possible methods for verification:

1. Get a packet capture off the outside interface of the firewall
2. Leverage a port checking utility
3. Use the Hybrid Connectivity Test tool

Since the Hybrid Connectivity Test tool is built right into the Cisco Webex Control Hub and simulates the Cisco Webex environment trying to connect to the on-premises Expressway, it is the most ideal verification method available. To test the TCP Connectivity into the organization:
1. Log into the Cisco Webex Control Hub
2. Select Services
3. Select the Settings link in the Hybrid Call card
4. In the Call Service Connect section ensure the value entered in the SIP Destination is correct
5. Click Test as shown in the image.

![SIP Destination Test](image1)

6. Since the test has failed you can click the View test results link to check the details as shown in the image.

![Verify SIP Destination](image2)

As observed in the image above, you can see that the Socket test has failed when trying to connect to 64.102.241.236:5062. Having this data in addition to the Expressway diagnostic logs/pcaps not show any connection attempts, you now have enough evidence to investigate the firewall ACL/NAT/Routing configuration.

**Solution**

Since this particular issue isn’t caused by the Cisco Webex environment or the on-premises collaboration equipment, you need to focus on the firewall configuration. Since you cannot necessarily predict the type of firewall you will be interfacing with, you need to rely on someone with familiarity with the device. It’s possible that the issue could be related to a firewall ACL, NAT, or routing misconfiguration.

**Issue 3. Socket Failure: Expressway-E is not Listening on Port 5062**

This particular condition is often diagnosed incorrectly. Many times, it is assumed that the firewall is the cause for why the traffic over port 5062 is getting blocked. To troubleshoot this particular condition, you can use the techniques in the "Port 5062 is blocked inbound to the Expressway"
scenario above. You will find that the Hybrid Connectivity Test tool and any other tool used to check port connectivity will fail. The first assumption is that the firewall is blocking the traffic. Most people will then double check the diagnostic logging from the Expressway-E to determine if they can see the TCP connection trying to establish. They will generally look for a log line item such as this as shown in the image.

```
2017-09-19T14:01:46.462-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:46,461" Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="40342" Dst-ip="172.16.2.2" Dst-port="5062" Detail="TCP Connecting"
```

In this condition, the particular log entry above will not exist. Therefore, many people will misdiagnose the condition and assume it is the firewall.

If a packet capture is included with the diagnostic logging, you can verify that the firewall is not the cause. Below is a packet capture sample from the scenario where the Expressway-E was not listening over port 5062. This capture filtered by using `tcp.port==5062` as the applied filter as shown in the image.

As you can see in the packet capture that was obtained from the Expressway-E, the traffic over tcp port 5062 is not being blocked by the firewall but is in fact arriving. In packet number 56, you can see that the Expressway-E is sending the RST immediately after the initial TCP SYN packet arrived. With this information, you can conclude that the issue is isolated to the Expressway-E receiving the packet; you must troubleshoot the issue from the Expressway-E perspective. Given the evidence, consider possible reasons for why the Expressway-E would RST the packet. Two possibilities that could attribute to this behavior are:

1. The Expressway-E has some type of firewall rules set up that could be blocking the traffic
2. The Expressway-E is not listening for Mutual TLS traffic and/or not listening for traffic over port 5062.

The Expressway-E's firewall functionality exists under `System > Protection > Firewall rules > Configuration`. When this was checked in this environment, there was no firewall configuration present.

There are several ways to verify if the Expressway-E is listening for Mutual TLS traffic over port 5062. You can do this either through the Web Interface or the CLI as a root user.

From the root of the Expressway, if you issue `netstat -an | grep ':5062'`, you should get some output similar to what you see below.

```
~ # netstat -an | grep ':5062'
tcp 0 0 172.16.2.2:5062 0.0.0.0:* LISTEN <-- Outside Interface
```
This information can also be captured through the web interface of the Expressway-E. See the steps below to gather this information:

1. Log into the Expressway-E

2. Navigate to **Maintenance Tools > Port usage > Local inbound ports**

3. Search for Type SIP and IP port 5062. (highlighted in red as shown in the image)

Now that you know what you should see, you can compare that to the current environment. From the CLI perspective, when you run `netstat -an | grep ':5062'`, the output looks like this:

```
~ # netstat -an | grep ':5062'
tcp  0  0 172.16.2.2:5062  0.0.0.0:* LISTEN  <-- Outside Interface
tcp  0  0 192.168.1.6:5062  0.0.0.0:* LISTEN  <-- Inside Interface
tcp  0  0 ::1:5062  :::* LISTEN
```

Additionally, the web UI does not show the Mutual TLS port listed under Local inbound ports

With this data, you can conclude that the Expressway-E is not listening for Mutual TLS traffic.

**Solution**

In order to solve this problem, you must ensure that the Mutual TLS mode is enabled and that the Mutual TLS port is set to 5062 on the Expressway-E:

1. Log into the Expressway-E
2. Navigate to **Configuration > Protocols > SIP**
3. Ensure the Mutual TLS mode is set to **On**
4. Ensure the Mutual TLS port is set to **5062**
5. Click **Save** as shown in the image.
Issue 4. Expressway-E or C does not Support Preloaded SIP Route Headers

With Hybrid Call Service Connect, the call routing is done based on route header. The route header is populated based on the information that the Call Service Aware (Expressway Connector) portion of the solution delivers to Cisco Webex. The Expressway connector host queries the Unified CM for users who are enabled for the Call Service and pull both their Directory URI and the Cluster FQDN of their Unified CM home cluster. See these example, using Alice and Bob:

<table>
<thead>
<tr>
<th>Directory URI</th>
<th>Destination Route Header</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:bob@example.com">bob@example.com</a></td>
<td>emea-cucm.example.com</td>
</tr>
<tr>
<td><a href="mailto:alice@example.com">alice@example.com</a></td>
<td>us-cucm.example.com</td>
</tr>
</tbody>
</table>

If Alice or Bob make a call, the call is routed to their on-premises Unified CM so that it can be anchored to their Cisco WebexRD before routing out to the called user.

If Alice were to call Bob, the call would route to Alice's Unified CM Home Cluster FQDN (us-cucm.example.com). If you analyze the SIP INVITE that Cisco Webex sends inbound to the Expressway-E, you'd find the following information within the SIP header:

Request URI: sip: bob@example.com
Route Header: sip:us-cucm.example.com;lr

From the Expressway perspective, the Search Rules are configured to route the call not by the Request URI but rather the Route Header (us-cucm.example.com) -- in this case, Alice's Unified CM home cluster.

With this foundation set, you can understand troubleshoot situations where the Expressways are misconfigured, which causes the above logic not to work. As nearly every other inbound Hybrid Call Service Connect call setup failure, the symptom is that the on-premises phone does not ring.

Before you analyze the diagnostic logs on the Expressway, consider how to identify this call:

1. The SIP Request URI will be the Directory URI of the Called Party.
2. The SIP FROM field will be formatted with the Calling Party listed as "First Name Last Name" <sip:WebexDisplayName@subdomain.call.ciscoWebex.com>
With this information, you can search the diagnostic logs by Directory URI of Called Party, First and Last Name of Calling Party, or Cisco Webex SIP Address of the Calling Party. If you don't have any of this information, you can search on "INVITE SIP:" which locates all SIP calls running over the Expressway. Once you have identified the SIP INVITE for the Inbound call, you can then locate and copy the SIP Call ID. After you have this value, you can simply search the diagnostic logs based on the Call-ID to see all messages that correlate to this call leg.

Another thing to help isolate the routing problem is to determine how far the call goes into the enterprise. You can try to search for the information noted above on the Expressway-C to see if the call was routed that far. If so, you will likely want to start your investigation there.

In this scenario, you can see that the Expressway-C has received the INVITE from the Expressway-E.

```
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15.830" Module="network.sip" Level="DEBUG": Action="Received" Local-port="26847" Local-ip="192.168.1.5" Src-ip="192.168.1.6" Src-port="7003" Msg-Hash="11449260850208794722"
SIPMSG: [INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0 Via:SIP/2.0/TLS 192.168.1.6:7003;transport=tls;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-id=a82052ef-6fd7-4506-8173-e73a6655b5d;rport Via:SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8a97ff3c204124;x-cisco-local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone Via:SIP/2.0/TLS 64.102.241.236:5061;branch=z9hG4bK6fe399bae58f8b0d70c9d69b8e37e13e5912.424893487bffe4af6f649b586c7696bb.proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016 Via:SIP/2.0/TLS 192.168.5.5:66:5062;branch=z9hG4bfK6fe399bae58f8b0d70c9d69b8e37e13e5912.424893487bffe4af6f649b586c7696bb.proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=146.20.193.45;rport=35464;ingress-zone=HybridCallServicesDNS Via:SIP/2.0/TLS 127.0.0.1:5061;branch=10.10.10.1:35464;ingress-zone=DefaultZone Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1 CSeq: 1 INVITE Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared From: <sip:pstojano-test@dmzlab.call.ciscoWebex.com>;tag=872524918 To: <sip:jorobb@rtp.ciscotac.net Max-Forwards: 15 Route: <sip:cucm.rtp.ciscotac.net;lr> Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-e73a6655b5d@192.168.1.6:7003;transport=tls;lr> Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-e73a6655b5d@192.168.1.6:5073;transport=tls;lr>
The important thing is that the route header (Cluster FQDN) is still intact. However, there's no search logic being performed based on the route header (Cluster FQDN) cucm.rtp.ciscotac.net. Rather, you see the message getting rejected immediately with a 404 Not Found.
```
Compared to a working scenario, you would see that in the working scenario the search logic is being performed based on the Router Header (Cluster FQDN).
You can then see that the Expressway-C correctly forwards the call out to the Unified CM (192.168.1.21).
Having analyzed the diagnostic logging which isolated the problem to the Expressway-C and a specific error (404 Not Found), you can focus on what would cause this type of behavior. Some things to consider are the following:

1. Calls are moved in and out of Zones on the Expressway by way of Search Rules.
2. The Expressways use logic called Preloaded SIP routes support which processes SIP INVITE requests that contain Router header. This value can be turned On or Off in the Zones (Traversal server, Traversal client, Neighbor) on both the Expressway-C and Expressway-E. You can now use the xConfiguration to view the configuration on both the Expressway-E Traversal server and Expressway-C client zones, specifically those that are set up for Hybrid Call Service Connect. In addition to the Zone configuration, you can analyze the Search Rules that are configured to pass this call through from one Zone to another. You also know that the Expressway-E did pass the call to the Expressway-C so the Traversal server zone configuration there is most likely set up correctly.

To break this down, the xConfig below tells us that the name of this zone is called Hybrid Call Service Traversal. It's of the TraversalServer zone type. It communicates to the Expressway-C over SIP TCP port 7003.

The key piece for Hybrid Call Service is that it must have Preloaded SIP routes support On. The Expressway Web interface calls this value Preloaded SIP routes support whereas the xConfiguration will display it as SIP PreloadedSipRoutes Accept

Expressway-E
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
You can also determine that this Zone has Search Rule 3 (Webex Hybrid) tied to it. Essentially the Search Rule is sending an "Any" alias that comes in through the Hybrid Call Services' DNS zone and passing it to the zone above, Hybrid Call Service Traversal. As expected, both the Search Rule and Traversal Server zone on the Expressway-E are configured correctly.

If you focus on the xConfiguration of the Expressway-C, you can start by looking for the Traversal Client zone for Webex Hybrid. One easy way to find it is to search on the port number you learned from the Expressway-E xConfiguration (SIP Port: "7003"). This helps you quickly identify the correct Zone in the xConfiguration.

As before, you can learn the Zone Name (Hybrid Call Service Traversal), the Type (Traversal Client), and what has been configured for the SIP PreloadedSipRoutes Accept (Preloaded SIP routes support). As you can see from this xConfiguration, this value is set to Off. Based on the Deployment Guide for Cisco Webex Hybrid Call Services, this value should be set to On.

Additionally, if we check the definition of the Preloaded SIP routes support we can see clearly that the Expressway-C should REJECT a message if this value is set to Off AND the INVITe contains a route header: "Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header."
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 6 TraversalClient Accept Delegated Credential Checks: "Off"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Password: "[cipher]qeh8eq+fuVY1GHGgRLder/1lYDd760/6KrHGA7g8bJs="
*c xConfiguration Zones Zone 6 TraversalClient Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 6 TraversalClient Collaboration Edge: "Off"
*c xConfiguration Zones Zone 6 TraversalClient H323 Port: "1719"
*c xConfiguration Zones Zone 6 TraversalClient H323 Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient Peer 1 Address: "amer-expressway01.ciscotac.net"
*c xConfiguration Zones Zone 6 TraversalClient Peer 2 Address: 
*c xConfiguration Zones Zone 6 TraversalClient Peer 3 Address: 
*c xConfiguration Zones Zone 6 TraversalClient Peer 4 Address: 
*c xConfiguration Zones Zone 6 TraversalClient Peer 5 Address: 
*c xConfiguration Zones Zone 6 TraversalClient Peer 6 Address: 
*c xConfiguration Zones Zone 6 TraversalClient Registrations: "Allow"
*c xConfiguration Zones Zone 6 TraversalClient RetryInterval: "120"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Port: "7003"
*c xConfiguration Zones Zone 6 TraversalClient SIP PreloadedSipRoutes Accept: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Address: 
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Port: 
*c xConfiguration Zones Zone 6 TraversalClient SIP Transport: "TLS"
*c xConfiguration Zones Zone 6 Type: "TraversalClient"

At this point, you've isolated the problem to a misconfiguration of the Expressway-C Traversal client zone configuration. You must switch the Preloaded SIP routes support to On.

Solution

To properly set the Preloaded SIP routes support:

1. Log into the Expressway-C
2. Navigate to Configuration > Zones > Zones
3. Select the Hybrid Call Service Traversal client zone (naming will vary customer to customer)
4. Set the Preloaded SIP routes support to On
5. Select Save

Note: While this scenario demonstrated the failure on the Expressway-C, the same diagnostic logging errors could be observed on the Expressway-E if the Preloaded SIP routes support was Off on the Webex Hybrid Call Traversal Server zone. In that event you would have never seen the call reach the Expressway-C and the Expressway-E would have been responsible for Rejecting the call and sending the 404 Not Found.

Issue 5. Cisco Webex app is receiving two call notifications (toasts)

This particular issue happens to be the only inbound calling scenario that doesn't result in the call dropping. For this issue, the person receiving the call (called party) is receiving two notifications (toasts) in the Cisco Webex app from the person who had placed the call (calling party). The first
notification is generated from Cisco Webex and the second notification comes from the on-premises infrastructure. Below are samples of the two notifications that are received as shown in the image.

The first notification (toast) is from the person who is initiating the call (calling party) from the Cisco Webex side. The calling ID in this instance is the Display Name of the user initiating that call. The second notification (toast) is coming from the on premises CTI or Cisco Webex RD that is assigned to the user who is making the call. At first, this behavior seems peculiar. However, if you review the inbound calling diagram (from the Cisco Webex Hybrid Call Design Guide), the behavior makes more sense as shown in the image.
From the illustration, you can see the Alice is calling Bob from her Cisco Webex app and that the call is being forked down to the premises. This call should match the Directory URI that is assigned to Bob’s phone. The problem is that with this design, the Directory URI is also assigned to his CTI-RD or Cisco Webex RD. Therefore, when the call is offered to the CTI-RD or Cisco Webex RD, the call is sent back out to Cisco Webex because the device has a Remote Destination configured for bob@example.call.ciscoWebex.com. The way Cisco Webex handles this situation is that it cancels the particular call leg.

For Cisco Webex to properly cancel the call leg, Cisco Webex initially needed to put a parameter in the SIP header which it would look for to cancel that given leg. The parameter Cisco Webex inserts into the SIP INVITE is called "call-type=squared" and this value is entered into the Contact header. If this value is stripped from the message, Cisco Webex does not understand how to cancel the call.

With this information, you can revisit the scenario presented earlier where the user’s Cisco Webex app was receiving two notifications (toasts) when Cisco Webex user Jonathan Robb was making a call. To troubleshoot this type of problem, you’re always going to need to collect diagnostic logging off the Expressway-C and Expressway-E. As a starting point, you can review the Expressway-E logs to determine that the SIP INVITE does in fact have the call-type=squared value present in the Contact header of the initial Cisco Webex INVITE sent inbound. This will ensure that the firewall is not manipulating the message in any way. Below is a sample snippet of the INVITE coming inbound to the Expressway-E from this scenario.
The Contact header has the `call-type=squared` value present. At this point, the call must route through the Expressway and be sent out of the Webex Hybrid Traversal Server zone. We can search the Expressway-E logs to determine how the call was sent out of the Expressway-E. This will give us an idea if the Expressway-E is manipulating the INVITE in any way.

When reviewing this SIP INVITE that is being sent from the Expressway-E to the Expressway-C, note that the Contact header is missing the `call-type=squared`. One other thing to point out is that in line item 4, you can see that the egress-zone is equal to `HybridCallServiceTraversal`. You can now conclude that the reason the Cisco Webex app is getting a second notification (toast) when dialed is because of the Expressway-E stripping the `call-type=squared` tag from the SIP INVITE Contact header. The question to answer is what could be causing this stripped header.

The call must route through the Hybrid Call Service Traversal you set up on the Expressway, so that is a good place to start the investigation. If you have the xConfiguration, you can see how this zone has been configured. To identify the Zone in the xConfiguration, you can simply use the name recorded in the Via line that gets printed in the logs. You can see above it was called `egress-zone=HybridCallServiceTraversal`. When this name is printed into the Via line of the SIP Header, the spaces are removed. The real zone name from the xConfiguration perspective would have spaces and is formatted at Hybrid Call Service Traversal.

```
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
```
With the settings identified for the Hybrid Call Service Traversal, you can look for potential settings that stand out, such as:

- **SIP PreloadedSIPRoutes Accept**: On
- **SIP ParameterPreservation Mode**: Off

Using the web interface of any Expressway, you can see what the definition of these values are and what they do.

**Preloaded SIP Routes support**

Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header.

Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.

**SIP parameter preservation**

Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone.

**On** preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA.

**Off** allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.

Based off these definitions, the xConfiguration, and that the *call-type=squared* value is placed in the "Contact" header of the SIP INVITE, you can conclude that having the SIP parameter preservation value Off on the Hybrid Call Service Traversal zone is the reason that tag is getting stripped and the Cisco Webex app is getting double ring notifications.
Solution

To preserve the call-type=squared value in the Contact header of the SIP INVITE, you must ensure that the Expressways support SIP parameter preservation for all Zones involved in handling the call:

1. Log into the Expressway-E
2. Navigate to Configuration > Zones > Zones
3. Select the Zone that's being used for the Hybrid Traversal Server
4. Set the SIP parameter preservation value to On
5. Save the settings.

Note: In this example scenario it was the Webex Hybrid Traversal Server zone on the Expressway-E that was misconfigured. Keep in mind that it is entirely possible for the SIP parameter preservation value to be set to Off on the Webex Hybrid Traversal client or CUCM neighbor zones. Both of these configurations would be done on the Expressway-C. If that were the case you could expect that the Expressway-E would have sent the call-type=squared value to the Expressway-C and it would have been the Expressway-C stripping it off.

Outbound: On-Premises to Cisco Webex

Almost every call failure involving outbound on-premises to Cisco Webex results in the same reported symptom: "When I call from my Unified CM-registered phone to another user who is enabled for Call Service Connect, their on-premises phone rings but their Cisco Webex app does not." To troubleshoot this scenario, it's important to understand both the call flow and logic that are occurring when this type of call is being placed.

High Level Logic Flow

1. User A makes a call from their on-premises phone to the Directory URI of User B
2. User B’s on-premises phone and CTI-RD/Webex-RD accept the call
3. User B’s on-premises phone begins to rings
4. User B’s CTI-RD/Webex-RD forks this call out to the destination of UserB@example.call.ciscoWebex.com
5. Unified CM passes this call to the Expressway-C
6. Expressway-C sends the call to the Expressway-E
7. Expressway-E performs a DNS lookup on the callservice.ciscoWebex.com domain
8. Expressway-E attempts to connect to the Cisco Webex environment over port 5062.
9. Expressway-E and the Cisco Webex environment begin a Mutual handshake
10. The Cisco Webex environment passes the call onto User B’s available Cisco Webex app
11. User B’s available Cisco Webex app begins to ring.

Call Flow

Navigate to User B on-prem phone > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco Webex environment > Cisco Webex app as shown in the image.
Log Analysis Tips

If you were troubleshooting a situation where the outbound forked calls to Cisco Webex were failing, you’d want to collect the Unified CM, Expressway-C, and Expressway-E logs. By having these sets of logs, you can see how the call is passing through the environment. Another quick way to understand how far the call is getting within your on-premises environment is to use the Expressway “Search History”. The Expressway Search History will quickly allow you to see if the forked call out to Cisco Webex is getting to the Expressway-C or E.

To use the Search History you can perform these:

1. Log into the Expressway-E
   Place a test call
   Navigate to **Status > Search History**
   Verify if you see a call that has a destination address of the Webex SIP URI that should be called (user@example.call.ciscoWebex.com)
   If the Search History does not show the call hitting the Expressway-E Search History repeat this process on the Expressway-C

Before you analyze the diagnostic logs on the Expressway, consider how to identify this call:

1. The SIP Request URI will be the Cisco Webex User’s SIP Address
2. The SIP FROM field will be formatted to have the Calling Party listed as "First Name Last Name" <sip:Alias@Domain>

With this information you can search the diagnostic logs by Directory URI of Calling Party, First and Last Name of Calling Party, or Cisco Webex SIP Address of the Called Party. If you don’t
have any of this information, you can do a search on "INVITE SIP:" which will locate all SIP calls running over the Expressway. Once you have identified the SIP INVITE for the Outbound call, you can then locate and copy the SIP Call-ID. After you have this you can simply search the diagnostic logs based on the Call-ID to see all messages that correlate to this call leg.

Here are some of the most common issues observed with outbound calls from the Unified CM-registered phone to the Cisco Webex environment when the call is made to a user who is enabled for Call Service Connect.

**Issue 1. Expressway is unable to resolve the callservice.ciscoWebex.com address**

The standard operating procedure for an Expressway DNS zone is to perform a DNS lookups based on the domain that shows up on the righthand side of a Request URI. To explain this, consider an example. If the DNS Zone were to receive a call that had a Request URI of pstojano-test@dmzlab.call.ciscoWebex.com, a typical Expressway DNS Zone would perform the DNS SRV Lookup logic on dmzlab.call.ciscoWebex.com which is the right hand side of the Request URI. If the Expressway were to do this you could expect that the following lookup and response would occur.

```text
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "Off" <-- Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On" <-- Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

If you look closely, you see that the SRV record response is providing a server address and port 5061, not 5062.

This means that the Mutual TLS handshake that occurs over port 5062 will not happen and a separate port is used for signaling between the Expressway and Cisco Webex. The challenge with this is that the *Deployment Guide for Cisco Webex Hybrid Call Services* doesn't explicitly call out the use of port 5061 because some environments do not allow business to business calling.
The way to work past this standard DNS Zone SRV lookup logic on the Expressway is to configure the Expressway so that it does explicit searches based on a value that you provide.

Now when analyzing this particular call, you can focus on the Expressway-E because you determined (using Search History) that the call has made it this far. Start with the first SIP INVITE that comes into the Expressway-E to see what zone it came in over, which Search Rules are being used, which Zone the call goes out, and if sent correctly to the DNS zone, what DNS lookup logic occurs.

In this SIP INVITE, you can gather up the Request URI (pstojano-test@dmzlab.call.ciscoWebex.com), the Call-ID (991f7e80-9c11517a-130ac-1501a8c0@192.168.1.21), From ("Jonathan Robb" <sip:5010@rtp.ciscotac.net>), To (sip:pstojano-test@dmzlab.call.ciscoWebex.com), and User-Agent (Cisco-CUCM11.5). After this INVITE is received, the Expressway must now make logic decisions to determine if it can route the call to another Zone. The Expressway will do this based on Search Rules.
Based on the log snippet above, you can see that the Expressway-E parsed through four Search Rules, however only one (Webex Hybrid - to Webex Cloud) was considered. The Search Rule had a priority of 90 and was targeted to go to the Hybrid Call Services DNS Zone. Now that the call is being sent to a DNS Zone, you can review the DNS SRV Lookups that are occurring on the Expressway-E.

In the snippet above, you can see that the Expressway-E performed the SRV lookup based on the right hand side on the Request URI (_sips._tcp.dmzlab.call.ciscoWebex.com) and it has resolved to a hostname of l2sip-cfa-01.wbx2.com and port 5061. The hostname l2sip-cfa-01.wbx2.com resolves to 146.20.193.64. With this information, the next logical step the Expressway will take is to send a TCP SYN packet to 146.20.193.64 so it can try to setup the call. From the Expressway-E logging, you can review to see if this is happening.

In the above Expressway-E diagnostic logging snippet, you can see that the Expressway-E is trying to connect to the IP 146.20.193.64 which was previously resolved over TCP port 5061 however this connection is outright failing. The same can be seen from the packet capture that was collected.
Based on these results, it's clear that traffic over port 5061 is not succeeding. However, Hybrid Call Service Connect intended to use TCP port 5062, not 5061. Therefore, you need to think about why isn't the Expressway-E resolving an SRV record that would return port 5062. To attempt to answer that question, you can look for possible configuration issues on the Expressway-E Webex Hybrid DNS Zone.

*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Zone 6 DNS SIP Authentication Trust Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Default Transport: "TLS"
*c xConfiguration Zones Zone 6 DNS SIP DnsOverride Name: "ciscoWebex.com"
*c xConfiguration Zones Zone 6 DNS SIP DnsOverride Override: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Media Encryption Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 6 DNS SIP ParameterPreservation Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP PreloadedSipRoutes Accept: "On"
*c xConfiguration Zones Zone 6 DNS SIP Record Route Address Type: "IP"
*c xConfiguration Zones Zone 6 DNS SIP SearchAutoResponse: "Off"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscoWebex.com"
*c xConfiguration Zones Zone 6 DNS SIP UDP BFCP Filter Mode: "Off"
*c xConfiguration Zones Zone 6 DNS SIP UDP IX Filter Mode: "Off"

In the xConfiguration of the Expressway-E, you can see there are two particular values of interest that relate to DNS lookups: DnsOverride Name and DnsOverride Override. Based off this xConfiguration the DnsOverride Override is set to Off, therefore the DnsOverride Name would not take effect. To better understand what these values do, you can use the Expressway Web UI to look up the definition of the values.

Modify DNS request (Translates to DnsOverride Override in xConfig)

Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. This option is primarily intended for use with Cisco Webex Call Service. See www.cisco.com/go/hybrid-services.

Domain to search for (Translates to DnsOverride Name in xConfig)

Enter a FQDN to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected.

Now that you have these definitions, it's clear that these values if set correctly would be entirely relevant for our DNS lookup logic. If you couple this with the statements from the Deployment Guide for Cisco Webex Hybrid Call Services, you would find that the Modify DNS Request must be set to On and the Domain to search for should be set to callservice.ciscoWebex.com. If you were to change these values to specify the correct information, the DNS SRV lookup logic would be entirely different. Below is a snippet of what you could expect from the Expressway-E
diagnostic logging perspective

2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscoWebex.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4''TCP''146.20.193.70:5062'] (A/AAAA) ['IPv4''TCP''146.20.193.64:5062'] (A/AAAA)"
Hostname:'l2sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)
Hostname:'l2sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of
relevant records retrieved: 4"

Solution

1. Log into the Expressway-E
2. Navigate to Configuration Zones > Zones
3. Select the Webex Hybrid DNS Zone that has been configured
4. Set the Modify DNS request to On
5. Set the Domain to search for value to callservice.ciscoWebex.com
6. Save the changes

Note: If there is only one DNS Zone being used on the Expressway, a separate DNS Zone
should be configured to be used with Hybrid Call Service that can take advantage of these
values.

Issue 2. Port 5062 is blocked outbound to Cisco Webex

One thing that is unique about the forked outbound call failures to Cisco Webex is that the called
party's Cisco Webex app will present a Join button on their app although the client never rings.
Like the scenario above, for this issue you will again need to use the same tools and logging to
best understand where the failure exists. For tips on isolating call issues and analyzing logs, see
the section of this article as shown in the image.

Illustration of the Join button being presented

Like Outbound call Issue #1, you can start analysis at the Expressway-E diagnostic logging,
because you've used the Search History on the Expressway to determine that the call is getting
that far. As before, start out with the initial INVITE that comes into the Expressway-E from the Expressway-C. Remember the things you want to look for are:

1. Whether the Expressway-E receives the INVITE
2. Whether Search Rule logic passes the call to the Hybrid DNS Zone
3. Whether the DNS Zone performs the DNS Lookup and on the correct domain
4. Whether the system attempted and correctly established a TCP Handshake for Port 5062
5. Whether the Mutual TLS Handshake succeeded

As you can see in the INVITE above, the INVITE is received as normal. This is a "received" action and it is coming from the Expressway-C IP address. You can now move on to the Search Rule Logic.
Based on the log snippet above, you can see that the Expressway-E parsed through four Search Rules however only one (Webex Hybrid - to Webex Cloud) was considered. The Search Rule had a priority of 90 and was targeted to go to the Hybrid Call Services DNS Zone. Now that the call is being sent to a DNS Zone, you can review the DNS SRV Lookups that are occurring on the Expressway-E. All of this is entirely normal. Now you can focus on the DNS Lookup logic.

You can clearly see that in this instance, the callservice.ciscoWebex.com SRV record is resolved. The response is four different valid records all of which use port 5062. This is normal behavior. At this point, you can now analyze the TCP handshake that should come next. As mentioned earlier in the document, you can search the diagnostic logs for "TCP Connecting" and look for the line item that lists the Dst-port="5062". Below is a sample of what you'll see in this scenario:

At this point, you can conclude that the Expressway-E is routing the call correctly. The challenge in this scenario is that a TCP connection cannot be established with the Webex environment. This could be happening because the Webex environment is not responding to the TCP SYN packet however that would be unlikely considering the server handling the connection is shared between many customers. The more likely cause in this scenario is some type of intermediary device (firewall, IPS, etc) is not allowing the traffic out.
Solution

Because the issue was isolated, this data should be provided to the customer's network administrator. Additionally, if they need more information, you can take a capture off the outside interface of the edge device and/or firewall for further proof. From the Expressway perspective, there is no further action to perform since the issue doesn't reside on that device.

Issue 3. Expressway Search rule misconfiguration

Search rule misconfiguration is one of the largest configuration related issues on the Expressways. Search rule configuration issues can be bi-directional, because you need Search rules for inbound calls and you need Search rules for outbound calls. As you walk through this issue, you'll discover that while regex issues are quite common on the Expressway, they are not always the cause of a search rule issue. In this particular segment, you will walk through an outbound call that is failing. Like all of our other outbound forked call scenarios, the symptoms remain the same:

- The Called user’s Cisco Webex app presented Join button
- The Calling phone was playing a ring back
- The Called user’s on-premises phone was ringing
- The Called user's Cisco Webex app never rang

Like all of the other scenarios, you will also want to leverage CUCM SDL traces along with Expressway-C and E diagnostic logs. As before, you should reference the for leveraging Search History and tips for identifying a call in the diagnostic logs. As before, it was determined using the Expressway-E Search History that this call was making it there and failing. Below is the beginning of the analysis for which we take a look at the initial SIP INVITE coming into the Expressway-E from the Expressway-C.

```
2017-09-25T11:26:02.959-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,959"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="25675" Msg-Hash="1536984498381728689"
SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscoWebex.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<xip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=505817-c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972
To: <sip:pstojano-test@dmzlab.call.ciscoWebex.com>
Max-Forwards: 15
Record-Route: <sip:proxy-call-id-f79b8631-947b-46d4-a888-911bf0150bfe@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id-f79b8631-947b-46d4-a888-911bf0150bfe@192.168.1.21:5065;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
```
Using the Call-ID (d58f2680-9c91200a-1c7ba-1501a8c0) from the SIP header, you can quickly search down all messages associated to this dialogue. When looking at the third hit in the logs for the Call-ID, you can see that the Expressway-E immediately sends a 404 Not Found to the Expressway-C.

This data tells you two things:

1. The Expressway-E never attempted to send the INVITE to Cisco Webex
2. The Expressway-E was the responsible party for making the logic decision to reject the call with a 404 Not Found error.

A 404 Not Found error generally means the Expressway is not able to find the destination address. Since the Expressways use Search Rules to route calls between themselves and to different environments, start by focusing on the xConfiguration of the Expressway-E. Within this xConfiguration, you can look for the Search Rule that should pass the call out to the Webex Hybrid DNS Zone. To find the search rules configured on the Expressway from the xConfiguration perspective, you can search for "xConfiguration Zones Policy SearchRules Rule" By doing this, you'll see a list of Service Rule configuration for each Search Rule created on the Expressway. The number that comes after the "Rule" will increase based on the search rule that was created first being marked 1. If you're having trouble finding the search rule, you can use commonly used naming values such as "Webex" to better locate the Search Rule. Another way to identify the rule is finding the Pattern String value that is set to ".*@.*\.ciscoWebex\.com". That is the Pattern String that is supposed to be configured. (Assuming the Pattern String is configured correctly)

After reviewing the xConfiguration from this scenario, you can see that Search Rule 6 is the correct rule to pass the call out to Cisco Webex.
To test this pattern, we can use the Check pattern function described in the. The important call out here is that we will want the following values configured:

Maintenance > Tools > Check pattern

- Alias: %Request URI in the initial INVITE% (Ex: pstojano-test@dmzlab.call.ciscoWebex.com)
- Pattern type: Regex
- Pattern String: \.*@\.*\ciscoWebex\com
- Pattern behavior: Leave

If the Regex for the rule is set up correct, you should see the result of this Check pattern Succeed. Below is an illustration demonstrating this as shown in the image:

Now that you can confirm the Search rule is present and configured correctly, you can look closer at the Search logic that the Expressway is performing to determine if it is affecting the Expressway-E that is sending the 404 Not Found. Below is a sample of the search rule logic that the Expressway was performing.
In this sample, you can see the Expressway processed four search rules. The first 3 were not considered because of various reasons, however the 4th was considered. The interesting piece of data is that immediately after consideration the Expressway jumps straight to DNS lookup logic. If you recall what we had seen in the xConfiguration the Search rule configured for Webex Hybrid was named Webex Hybrid - to Webex Cloud and it wasn't even considered in this Search rule logic above. At this point, it is worth looking into how the considered search rule (to DNS) was implemented so that you can better understand if it is impacting the use of the Webex Hybrid Search rule. To do that, you can revisit the xConfig this time looking for the Search Rule named "to DNS"

After review of this Search rule, you can conclude the following:

- The pattern string would match the Cisco Webex Request URI
- The Priority is set to 100
- The Progress (Pattern behavior) is set to Stop.

What this information tells us is that the Cisco Webex Request URI being called would match this rule and if the rule was matched the Expressway would stop searching (Considering) other Search rules. With this understanding, the Rule Priority becomes a key factor. The way the Expressway Search rule priority works is the lowest priority rule is attempted first. Below is an example.
**Search Rule: Local**

Pattern behavior: Continue

Priority 1

**Search Rule: Neighbor**

Pattern behavior: Continue

Priority 10

**Search Rule: DNS**

Pattern behavior: Stop

Priority 50

In this example, the Search rule named Local (1) would be attempted first and if a match was found it would move to Search rule Neighbor (10) because of the Pattern behavior being set to Continue. If search rule Neighbor wasn't matched, it will still continue to Search Rule DNS (50) and consider that last. If Search Rule DNS was matched, the search would stop regardless of whether there was another Search Rule with a priority higher than 50, because the Pattern behavior was set to Stop.

With this understanding, you can take a look at the Search Rule priorities between the "to DNS" and "Webex Hybrid - to Webex Cloud" rules.

* c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
* c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
* c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"

* c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
* c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
* c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"

Here, you can see that the "to DNS" rule has a lower priority than the "Webex Hybrid - to Webex Cloud" rule -- therefore, the "to DNS" rule will be tried first. Given that the Pattern behavior (Progress) is set to Stop, the Expressway-E never considers the Webex Hybrid - to Webex Cloud rule and the call ultimately fails.

**Solution**

This type of problem is increasingly common with Hybrid Call Service Connect. Many times when the solution is deployed, people create a high priority rule to use for the Cisco Webex searches. Many times this rule that is created isn't getting invoked because of existing lower priority rules are being matched and it results in a failure. This issue happens on both inbound and outbound calls to Cisco Webex. To resolve this, you'll need to follow these steps:

1. Log into the Expressway-E
2. Navigate to Configuration > Dial Plan > Search rules
3. Find the Webex Hybrid Search rule and click it (Ex: Name: Webex Hybrid - to Webex Cloud)
4. Set the Priority value to something lower than other Search rules, yet high enough so that it
won't impact others. *(Ex: Priority: 99)*

The general rule of thumb with Search rules is the more specific the Pattern string, the lower it can
be placed in the Search rule priority list. Generally a DNS Zone is configured with a Pattern string
that is going to catch anything that is not a local domain and send it to the Internet. Due to this, we
recommend that you set that type of Search rule to a high priority so it's invoked last.

**Issue 4. Expressway CPL misconfiguration**

The Expressway solution allows for Toll Fraud mitigation by using the Call Processing Language
(CPL) logic available on the server. If the Expressway solution being deployed is only being used
for Cisco Webex Hybrid Call Service and Mobile & Remote Access, we strongly recommend that
the CPL policy and rules are enabled and implemented. While the CPL configuration on the
Expressway for Cisco Webex Hybrid is fairly straightforward, if misconfigured it can easily block
call attempts from happening. The scenarios below show you how to use the diagnostic logging to
identify a CPL misconfiguration.

Like all of the other scenarios, you can use the CUCM SDL traces along with Expressway-C and E
diagnostic logs. As before, you should reference the for using Search History and tips for
identifying a call in the diagnostic logs. As before, it was determined using the Expressway-E
Search History that this call was arriving there and failing. Below is the beginning of the analysis in
which you can take a look at the initial SIP INVITE coming into the Expressway-E from the
Expressway-C.

```plaintext
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26404" Msg-Hash="17204952472509519266"

SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscoWebex.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aace86834368739430283256.34216c32a0d336e16590b1ae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8ac;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: c030f100-9c916d13-1cddcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
Contact: <sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=512579~9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000
To: <sip:pstojano-test@dmzlab.call.ciscoWebex.com>
Max-Forwards: 15
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8ac@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8ac@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
```
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 20:54:43 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAA Tag: 4fffed-0512-4067-ac8c-35828f0a1150
Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
Content-Type: application/sdp
Content-Length: 714

Using the Call-ID (c030f100-9c916d13-1cdcb-1501a8c0) from the SIP header, you quickly search down all messages associated to this dialog. When looking at the third hit in the logs for the Call-ID, you can see that the Expressway-E immediately sends a **403 Forbidden** to the Expressway-C.

```
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="26404" Msg-Hash="9195436101110134622"
SIPMSG:
|SIP/2.0 403 Forbidden
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aacc86834368739430283256.34216c32a0de3e16590bae36df3期待b94a-082e-4088-8f5a-5ea7e82f8aacc;received=192.168.1.5;rport=26404;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=512579-c9cc7dcd-9592-49e8-a13c-79e26f48eebc-30107000
To: <sip:joestano-test@dmzlab.call.ciscoWebex.com>;tag=64fe7f9eab37029d
Server: TANDBERG/4135 (X.8.10.2)
Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa512577
Content-Length: 0
```

To understand why the Expressway-E denied this call and sent a 403 Forbidden error to the Expressway-C, you want to analyze the log entries between the 403 Forbidden and the original SIP INVITE that entered into the Expressway. By analyzing these log entries, you can typically see all the logic decisions that are being made. Note that you do not see any Search rules being invoked but do see Call Process Language (CPL) logic being invoked. Below is a snippet of that.

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
<routed>"
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
<rule-switch>"
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
<rule unauthenticated-origin=".*" destination=".*@dmzlab.call.ciscoWebex.com." message-regex=""> matched"
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
<reject/>"
```
Based on the log analysis above, you can make the determination that the CPL is rejecting the call.

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed" Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscoWebex.com" Call-serial-number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4ffeved-0512-4067-ac8c-35828f0a1150" Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-25 20:54:43,726"

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Call Rejected" Service="SIP" Src-ip="192.168.1.5" Src-port="26404" Src-alias-type="SIP"

Note: In this situation you will not see Search rules being invoked because CPLs, FindMe, and Transforms are all processed before a Search rule

In most circumstances, you can leverage the xConfig of the Expressway to better understand the circumstances. However, for CPLs, you cannot see the Rules that are defined, only if the policy is enabled. Below is the portion of the xConfig that shows us this Expressway-E is using the Local CPL logic.

```
c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"
```

To better understand the rule configuration, you need to log in to the Expressway-E and navigate to **Configuration > Call Policy > Rules** as shown in the image.

When reviewing this configuration, you can see the following is configured

Source: .* Destination: .*@dmzlab\call\ciscoWebex\..*

Action: Reject

Compared to what's been documented in the *Cisco Webex Hybrid Call Service Deployment Guide*, you can see that the Source and Destination were configured backwards.

<table>
<thead>
<tr>
<th>Field</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Type</td>
<td>From address</td>
</tr>
<tr>
<td>Rule applies to</td>
<td>Unauthenticated callers</td>
</tr>
<tr>
<td>Source pattern</td>
<td>.<em>@example\call\ciscospark..</em>, where example is your company's subdomain.</td>
</tr>
<tr>
<td>Destination pattern</td>
<td>.*</td>
</tr>
<tr>
<td>Action</td>
<td>Reject</td>
</tr>
</tbody>
</table>

**Solution**

To resolve this issue, you need to readjust the CPL rule configuration so that the Source is set to
1. Log into the Expressway-E
2. Navigate to Configuration > Call Policy > Rules
3. Select the rule that was setup for the Cisco Webex Hybrid Call service
4. Enter the Source Pattern as
   .*@%Webex_subdomain%.call\ciscoWebex\com.* (Ex: .*@dmzlab\call\ciscoWebex\com.*)
5. Enter the Destination Pattern as .*
6. Select Save

For more information on the CPL implementation for Webex Hybrid refer to the Cisco Webex Hybrid Design Guide.

Bidirectional: Cisco Webex to On-Premises or On-Premises to Cisco Webex

Issue 1. IP Phone/Collaboration Endpoint is offering an audio codec other than G.711, G.722, or AAC-LD.

Hybrid Call Service Connect supports three different audio codecs: G.711, G.722, and AAC-LD. To successfully establish a call with the Cisco Webex environment, one of these audio codecs must be used. The on-premises environment can be setup to use many types of audio codecs but at the same time it can be setup to restrict them. This can happen intentionally or unintentionally by the use of custom and/or default region settings on the Unified CM. For this particular behavior, the logging patterns can differ based on the direction of the call and if the Unified CM was configured to use Early or Delayed Offer. Below are examples of a few different situations where this behavior could present itself:

1. Cisco Webex sends an inbound INVITE w/ SDP that offers G.711, G.722, or AAC-LD. The Expressway-C sends this message to Unified CM but Unified CM is configured to only allow G.729 for this call. So, Unified CM will reject the call due to no available codec.
2. Unified CM attempts the outbound call as Early Offer to Cisco Webex which means the initial INVITE sent to the Expressway-C will contain SDP ONLY supporting G.729 audio. Cisco Webex then sends a 200 OK w/ SDP that zeros out the audio (m=audio 0 RTP/SAVP) because it doesn't support G.729. Once the Expressway-C passes this INVITE to the Unified CM, the Unified CM terminates the call because there isn't an available codec.
3. Unified CM attempts the outbound call as Delayed Offer to Cisco Webex which means the initial INVITE sent to the Expressway-C will not contain SDP. Cisco Webex then sends a 200 OK w/ SDP containing all the supported audio codecs Cisco Webex supports. The Expressway-C sends this 200 OK to Unified CM but Unified CM is only configured to only allow G.729 for this call. So, Unified CM will reject the call due to no available codec.

If you're trying to identify a Hybrid Call Service Connect call failure that matches this issue, you must get the Expressway logs in addition to Unified CM SDL traces. The example log snippets below match situation #2 where Unified CM is attempting the outbound call as Early Offer. Because we know that the call is getting out to Cisco Webex, the log analysis starts on the Expressway-E.

Below is a snippet of the initial INVITE out to Cisco Webex. You can see that the preferred audio codec is set to G.729 (Payload 18). The 101 is for DTMF and for this particular scenario isn't relevant.
SIP/2.0 200 OK
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKfcf4cfd09d2f2331cef0bc8b540559.494a140082bd66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-c60a8b17a8b4d;received=192.168.1.5;port=26513;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
Content-Type: application/sdp
Content-Length: 1407
v=0
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
c=IN IP4 64.102.241.236
b=AS:384
m=audio 52668 RTP/SAVP 18 101 CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=rtmap:101 telephone-event/8000
a=rtmap:101 annexb=no
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:
  a=rtpmap:12 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:
  a=rtpmap:101 telephone-event/8000
  a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:5 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:5 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:6 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:6 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:7 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:7 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:8 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:8 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:9 AES_CM_128_HMAC_SHA1_32 inline:
  a=rtpmap:18 G729/8000
  a=rtmap:101 telephone-event/8000
  a=crypto:9 AES_CM_128_HMAC_SHA1_32 inline:
In response to this initial INVITE, Cisco Webex responds with a 200 OK message. If you take a closer look at this message, you can see that the audio codec was zeroed out. This is problematic because without an audio port assigned, the call will not be able to negotiate that stream.

v=0
o=linus 0 1 IN IP4 146.20.193.109
s=-
c=IN IP4 146.20.193.109
You can now use TranslatorX to review the remainder of the dialog. You can see that the dialog itself completes with an ACK. The problem is immediately after the dialogue completes there is a BYE that comes from the direction of the Expressway-C as shown in the image.

Below is a detailed sample of the BYE message. You can clearly see that the User-Agent is Cisco-CUCM11.5 which means that the message was generated by the Unified CM. Another thing to point out is that the Reason code is set to cause=47. The common translation for this is No resource available.

2017-09-19T10:46:27.175-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,175" Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003" Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="237943800593485079" SIPMSG:
BYE sip:192.168.1.6:5071;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
Because the Cisco Webex component zeroed out the audio codec for this call sample, the focus must be on

a) the initial INVITE that was sent to Cisco Webex and

b) what was the logic Cisco Webex used to zero out that port.

Now looking at what is unique about the initial INVITE what can be noticed is it only contains G.729. Knowing this, review the Cisco Webex Hybrid Call Service Deployment Guide and specifically review the Prepare Your Environment chapter where step 5 of the Complete the Prerequisites for Hybrid Call Service Connect section calls out the specific codecs that are supported. There we would see this:

Cisco Webex supports the following codecs:

- Audio—G.711, G.722, AAC-LD
- Video—H.264

Note: Opus is not used on the on premise leg of the call for Cisco Webex Hybrid Call.

With this information at hand, you can conclude that Unified CM is sending an unsupported audio codec which is the reason the Cisco Webex is zeroing out the port.

Solution

To address this particular situation, you may need to review the region configuration between the Cisco Webex RD that is anchoring the call on-premises and the SIP Trunk for the Expressway-C. To do so, determine which Device Pool those two elements are in. The Device Pool contains the mappings to the Regions.

To determine the Device Pool of the Expressway-C SIP Trunk:

1. Log into the Unified CM
2. Navigate to Device > Trunk
3. Search for the Trunk name or click Find
4. Select the Expressway-C trunk
5. Record the name of the Device Pool
To determine the Device Pool of the CTI-RD or Cisco Webex-RD that anchored the call

1. Navigate to Device > Phone
2. When searching you can select Device Type contains Webex or CTI Remote Device (depending on what the customer is using.
3. Record the name of the Device Pool

Determine the Region attached to each Device Pool

1. Navigate to System > Device Pool
2. Search for the Device Pool used for the Expressway-C SIP Trunk
3. Click on the Device Pool
4. Record the Region name
5. Search for the Device Pool used for the Webex-RD or CTI-RD
6. Click on the Device Pool
7. Record the Region name

Determine the Region relationship

1. Navigate to System > Region information > Region
2. Search on one of the Regions identified above
3. Determine if there is a Region relation between both regions that is using G.729

At this point, if you identify the relationship that is using G.729, you'll need to adjust the relationship to support of the supported audio codecs that Cisco Webex uses or use a different Device Pool that has a Region that supports this. In the scenario documented above, the following was determined:

Expressway-C Trunk Region: ReservingBandwidth

Webex-RD Region: RTP-Devices

Below is a graphical illustration of the relationship between the RTP-Devices and ReservingBandwidth regions as shown in the image.

By changing the Device Pool the Expressway-C trunk was in, you change the Region relationship. The new Device Pool had a Region set to RTP-Infrastructure, therefore the new region relationship between the Cisco Webex-RD and Expressway-C trunk was RTP-Devices and RTP-Infrastructure. As pictured above, you can see this relationship supports AAC-LD which is one of the supported audio codecs for Cisco Webex and so the call will set up correctly.

Issue 2. Unified CM Max Incoming Message Size exceeded

Because video has become more prevalent within the enterprise, the size of SIP messages that contain SDP has grown substantially. The servers that process these messages must be
configured in such as way that they can accept a large packet. On many call control servers, the default values are fine. With the Cisco Unified Communications Manager (Unified CM), the default values to handle a large SIP message containing SDP in past releases were not. In later releases of Unified CM the value size allowed for a SIP message have been increased however this value is only set on new installs not upgrades. With this all said, customers who are upgrading their older releases of Unified CM to support Hybrid Call Service Connect might be affected by the Max Incoming Message Size on Unified CM being too low.

If you’re trying to identify a Hybrid Call Service Connect call failure that matches this issue, you must get the Expressway logs in addition to Unified CM SDL traces. To identify the failure, first understand what happens and then the types of scenarios in which the failure can occur.

To answer question of what happens, you must know that once the Unified CM receives a SIP message that is too large, it simply closes the TCP socket and does not respond to the Expressway-C.

With this said, there are many situations and ways this could occur:

1. Cisco Webex sends an inbound INVITE w/ SDP that is too large. The Expressway-C passes this onto the Unified CM and Unified CM closes the TCP socket then the SIP dialog will time out.

2. Unified CM attempts the outbound call as Early Offer to Webex which means the initial INVITE sent to the Expressway-C will contain SDP. Cisco Webex then sends a 200 OK w/ SDP in response and the 200 OK response when passed from the Expressway-C to the Unified CM is too large. Unified CM closes the TCP socket then the SIP dialog will time out.

3. Unified CM attempts the outbound call as Delayed Offer to Webex which means the initial INVITE sent to the Expressway-C will not contain SDP. Cisco Webex then sends a 200 OK w/ SDP and the 200 OK offer when passed from the Expressway-C to the Unified CM is too large. Unified CM closes the TCP socket then the SIP dialog will time out.

Looking through the Expressway-C logs for this particular condition helps you understand the message flow. If you were to use a program like TranslatorX, you could see that the Expressway-C is passing the Cisco Webex 200 OK w/ SDP to Unified CM. The challenge is that the Unified CM never responds back with a SIP ACK as shown in the image.
Since the Unified CM is the responsible party for not responding, it is worth reviewing the SDL traces to see how the Unified CM is handling this condition. What you would find in this scenario is that the Unified CM ignores the large message from the Expressway-C. A log line item such as the one below would be printed.

**CUCM Traces**

```
53138762.000 | 09:05:19.762 | AppInfo | SIPSocketProtocol(5,100,14,707326)::handleReadComplete
53138763.000 | 09:05:19.762 | SdlSig  | SdlReadRsp
53138763.001 | 09:05:19.762 | AppInfo | SIPTcp - SdlRead bufferLen=5000
53138763.002 | 09:05:19.762 | AppInfo | //SIP/Stack/Error/0x0/httpish_cache_header_val: DROPPING
unregistered header Locus: c904ecb1-d286-11e6-bfdf-b60ed914549d
53138763.003 | 09:05:19.762 | AppInfo | //SIP/Stack/Info/0x0/httpish_msg_process_network_msg:
Content Length 4068, Bytes Remaining 3804
53138763.004 | 09:05:19.762 | AppInfo | //SIP/Stack/Info/0x0/ccsip_process_network_message:
process_network_msg: not complete
53138763.005 | 09:05:19.762 | AppInfo | SIPTcp - Ignoring large message from %Expressway-C_IP%:[5060]. Only allow up to 5000 bytes. Resetting connection.
```

After the SIP dialogue times out, Cisco Webex will send an Inbound SIP 603 Decline message to the Expressway-E as noted in the log sample below.

**Expressway-E Traces**

```
2017-01-04T09:05:40.645-05:00 vcs-expressway tvcs: UTCTime="2017-01-04 14:05:40.645"
Module="network.sip" Level="DEBUG" Action="Received" Local-ip="%Exp-E%" Local-port="25150" Src-ip="%Webex_IP%" Src-port="5062" Msg-Hash="248307375671246315" SIPMSG: SIP/2.0 603 Decline
```

As mentioned, there are three different scenarios in which you could see this behavior. For clarity,
the log samples provided in this illustration matched situation 3 where the call was sent outbound to Cisco Webex as Delayed offer.

Solution

1. Log into the Unified CM
2. Navigate to **System > Service Parameters**
3. Select the Server that is running the Call Manager service
4. Choose the **Cisco Call Manager service** when prompted for a Service selection
5. Select the **Advanced** Option
6. Under the Clusterwide Parameters (Device - SIP) settings change the **SIP Max Incoming Message Size** to **18000**.
7. Select **Save**
8. Repeat this process for every Unified CM node that is running the Cisco Call Manager service.

**Note:** In order for an IP Phone, Collaboration endpoint, and/or SIP Trunk to leverage this setting it must be restarted. These devices can be restarted individually to minimize impact to the environment. **DO NOT reset every device on the CUCM unless you know it is absolutely acceptable to do so.**

Appendix 1: Expressway Troubleshooting Tools

**Check Pattern utility**

The Expressway has a pattern checking utility that is useful when you want to test whether a pattern matches a particular alias and is transformed in the expected way. The utility can be found on the Expressway under the **Maintenance > Tools > Check pattern** menu option. Most commonly, this is used if you want test whether your Search Rule regex is going to properly match an alias to a pattern string and then optionally perform successful manipulation of the string. For Hybrid Call Service Connect, you can also test that the Unified CM Cluster FQDN is going to match the Pattern string that you set up for the Unified CM cluster FQDN. When using this utility, remember that the call will route based on the Unified CM Cluster FQDN parameter listed in the Route Header, not the Destination URI. For example if, the following invite came into the Expressway, test the Check pattern functionality against **cucm.rtp.ciscotac.net**, not jorobb@rtp.ciscotac.net.

```
SIPMSG: |INVITE sip:JOROBB@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-id=abcba873-eaae-4d64-a83b4-c4541d4e620c;Rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4f5e58eddb51bf12;x-cisco-local-service=nettle;received=192.168.1.6;rport=41913;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;branch=z9hG4bK524f89592d00f0f4d57b530002711676c370.88b5177ac4d7cfa12eb8f8be78d055;proxy-call-id=2db939b2+a49b-4307-8d96-23716a2c90b;received=172.16.2.2;rport=25010;ingress-zone=DefaultZone;branch=z9hG4bK524f89592d00f0f4d57b530002711676c370.88b5177ac4d7cfa12eb8f8be78d055
Via: SIP/2.0/TLS 192.168.4.150:5062;branch=z9hG4bK92f9ef952712e6610c3e6b72770c1230;received=148.62.40.63;rport=39986;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-313634-
```
To use Check pattern to test the Hybrid Call Service Connect Route header search rule routing, follow these steps:

1. Navigate to **Maintenance > Tools > Check pattern**
2. For the Alias, enter the **Unified CM Cluster FQDN**
3. Set the Pattern Type to **Prefix**
4. Set the Pattern String to **Unified CM Cluster FQDN**
5. Set the Pattern behavior to **Leave**
6. Select **Check pattern**

If the search rules on the Expressway are configured correctly, you can expect to see the Results return a Succeeded message.

Below is an example of a successful Check pattern test as shown in the image.

The reason this is successful is because this Alias (cucm.rtp.ciscotac.net) matches the Prefix pattern string of (cucm.rtp.ciscotac.net). To understand how a call is routed based off these results, you can use the Expressway **Locate Utility** described below.

**Locate Utility**

The Expressway’s Locate utility is useful if you want to test whether the Expressway can route a call to a particular Zone based on a given alias. All this can be completed without having to place a real call. The Locate utility can be found on the Expressway under the **Maintenance > Tools > Locate** menu. Below provides some instruction on how you could use the Locate functionality on the Expressway-C to determine if the server could route a call based on the Unified CM Cluster FQDN found in the SIP Route header.

1. Navigate to **Maintenance > Tools > Locate**
2. Enter the **Unified CM Cluster FQDN** in the Alias field
3. Select **SIP** as the Protocol
4. Select your **Cisco Webex Hybrid Traversal client Zone** for the Source
5. Select **Locate**

At the bottom of the interface, you will now see the search results. Below is an example of the sample test that was run with the matching results as shown in the image.

Below are the results of the Locate (above). Bolded are the values of interest These results show the following:

- The fact that the Alias could be routed (True)
- Source information (Zone name/type)
- Destination information (alias being routed)
- Search Rule being matched (Hybrid Call Service Inbound Routing)
- Zone that the call would be sent to (CUCM11)

Search (1)
- **State:** Completed
- **Found:** True
- **Type:** SIP (OPTIONS)
- **SIPVariant:** Standards-based
- **CallRouted:** True
  - **CallSerial Number:** ae73fb64-c305-457a-b7b3-59ea9688c630
  - **Tag:** 473a5b19-9a37-40bf-bbee-6f7bc94e7c77

**Source (1)**
- **Authenticated:** True
- **Aliases (1)**
  - **Alias (1)**
    - **Type:** Url
    - **Origin:** Unknown
    - **Value:** xcom-locate

**Zone (1)**
- **Name:** Hybrid Call Service Traversal
- **Type:** TraversalClient
  - **Path (1)**
  - **Hop (1)**
    - **Address:** 127.0.0.1
  - **Destination (1)**
    - **Alias (1)**
      - **Type:** Url
      - **Origin:** Unknown
      - **Value:** sip:cucm.rtp.ciscotac.net
    
- **StartTime:** 2017-09-24 09:51:18
- **Duration:** 0.01
SubSearch (1)
Type: Transforms
Action: Not Transformed
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Admin Policy
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: FindMe
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Search Rules
SearchRule (1)
Name: as is local
Zone (1)
Name: LocalZone
Type: Local
Protocol: SIP
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
Zone (2)
Name: LocalZone
Type: Local
Protocol: H323
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SearchRule (2)
Name: Hybrid Call Service Inbound Routing
Zone (1)
Name: CUCM11
Type: Neighbor
Protocol: SIP
Found: True
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.21:5065
Diagnostic Logging

Any time you're troubleshooting a calling or media issue for a call that traverses the Expressway solution, you must use the diagnostic logging. This Expressway capability gives an engineer a great detail of information for all the logic decisions the Expressway is going through as the call passes. You can see the full body SIP messages, how the Expressway passes that call through, and how the Expressway sets up the media channels. The diagnostic logging has a number of different modules that feed into it. The logging levels can be adjusted to show FATAL, ERROR, WARN, INFO, DEBUG, TRACE. By default everything is set to INFO which captures almost everything you need to diagnose a problem. From time to time, you may need to adjust a logging level of a particular module from INFO to DEBUG to get a better understanding of what is happening. The steps below illustrate how you can adjust the logging levels of the developer.ssl module which is responsible for providing information for (mutual) TLS handshakes.

1. Log into the Expressway server *(Must be done on both the Expressway-E and C)*
2. Navigate to Maintenance > Diagnostics > Advanced > Support Log configuration
3. Scroll to the module you would like to adjust, in this instance developer.ssl and click it.
4. Next to the Level parameter, choose DEBUG from the menu
5. Click Save

At this point, you're prepared to capture the diagnostic logging:

1. Log into the Expressway server *(Must be done on both the Expressway-E and C)*
2. Navigate to Maintenance > Diagnostics > Diagnostic logging
3. Click Start New Log *(Note: Ensure you check the tcpdump option)*
4. Reproduce the issue
5. Click Stop Logging
6. Click Download Log

For the Expressway diagnostic logging, keep in mind that you would start the logging from both the Expressway-C and Expressway-E in parallel: first start the logging on the Expressway-E, then go to the Expressway-C and start it. At that point, you can then reproduce the problem.

**Note:** Currently the Expressway/VCS diagnostic log bundle does not contain information about the Expressway Server certificate or Trusted CA list. If you have a case where having this functionality would be beneficial, please attach your case to this defect.

References

- Deployment Guide for Cisco Webex Hybrid Call Services
- Cisco Webex Hybrid Design Guide
- Cisco Expressway Administrator Guide
- Technical Support & Documentation - Cisco Systems