Cisco Webex 混合呼叫服务连接故障排除指南

目录

简介

本文档介绍可让您现有思科呼叫控制基础设施连接到思科协作云以便让它们能够正常工作的 Cisco Webex 混合呼叫服务连接解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Webex 产品知识
- Expressway 解决方案知识 (B2B)
- 思科统一通信管理器 (Unified CM) 以及其与 Expressway 集成的知识
- Unified CM 10.5(2) SU5 或更高版本。
- Expressway (B2B) 版本 X8.7.1 或更高版本（建议 X8.9.1）
- Expressway（连接器主机）— 有关当前受支持的版本，请参阅Expressway连接器主机支持Cisco Webex混合服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Unified Communications Manager
- Expressways
- Windows版Webex
- Webexfor Mac
- iOS的Webex
- Android版Webex
- 思科协作终端
- 协作服务台终端
- IP 电话
- 软件客户端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

该解决方案提供以下功能：

- 将Webex应用用作音频和视频呼叫的移动软客户端
- 使用此应用程序可在任何地方拨打和接听呼叫，如同在办公室中一样
- 使用Webex、Cisco Jabber或其台式电话进行呼叫，无需担心使用哪个选项
- 在内部电话中解锁呼叫历史记录并将该历史记录集成到Webex

本指南涵盖混合呼叫服务连接特有的问题。由于混合呼叫服务连接与其他解决方案（如移动和远程访问以及企业到企业呼叫）在同一Expressway E & C对上运行，因此其他解决方案的问题可能会影响混合呼叫服务连接。如果客户和合作伙伴需要部署 Expressway 对用于呼叫服务连接，则在部署混合呼叫服务连接之前，必须参考思科 VCS Expressway 与 VCS 控制基本配置指南。本故障排除指南在附录 3 和 4 中均介绍了防火墙/NAT 注意事项以及 Expressway 设计。 请仔细查看本文档。此外，本文档假设已完成 Expressway 连接器主机和混合呼叫服务激活。

呼叫设置问题

双向 TLS 握手失败

在 Cisco Webex 和 Expressway E 之间进行身份验证时，混合呼叫服务连接使用双向传输层安全（双向 TLS）。这表示 Expressway E 和 Cisco Webex 会检查相互展示的证书。由于双向TLS问题在Expressway服务器的新部署以及混合呼叫服务连接等解决方案的启用期间非常普遍，本部分提供了有用的信息和提示，用于对Expressway和Cisco Webex之间基于证书的问题进行故障排除。

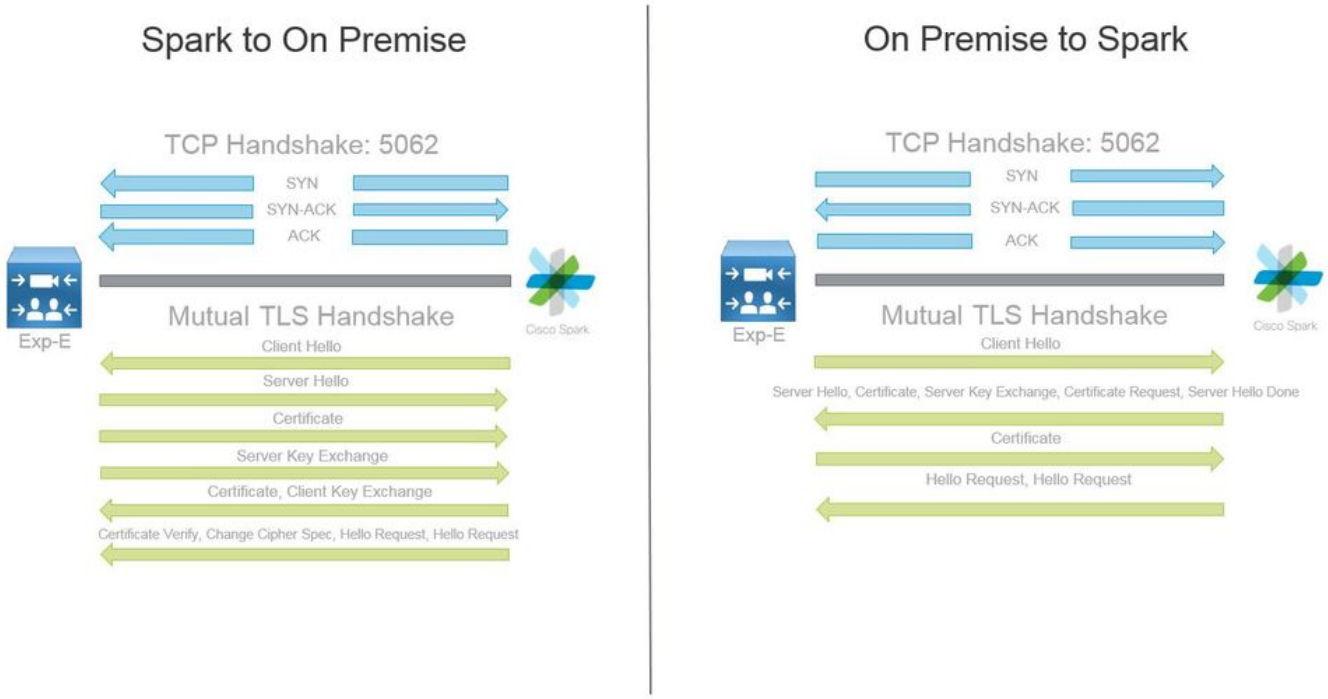
Expressway E 检查什么？

- Cisco Webex 证书是否由 Expressway E 受信任 CA 列表中列出的公共 CA 签署？
- Cisco Webex证书的Subject Alternate Name字段中是否存在callservice.ciscospark.com?

Cisco Webex 检查什么？

- Expressway E证书是否已由Webex信任的一个公共CA签名？（Cisco Webex 受信任 CA 列表）
- Expressway E 不使用公开签署的证书，Expressway 证书是否随同任何根证书和中间证书一起上传到 Cisco Webex Control Hub (https://admin.ciscospark.com)？

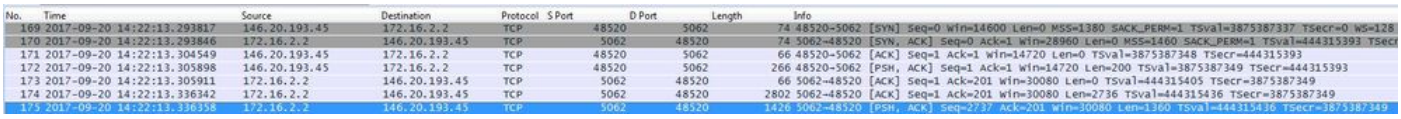
下图对此进行了说明。



双向 TLS 故障排除实用技巧

1.解码相互TLS握手

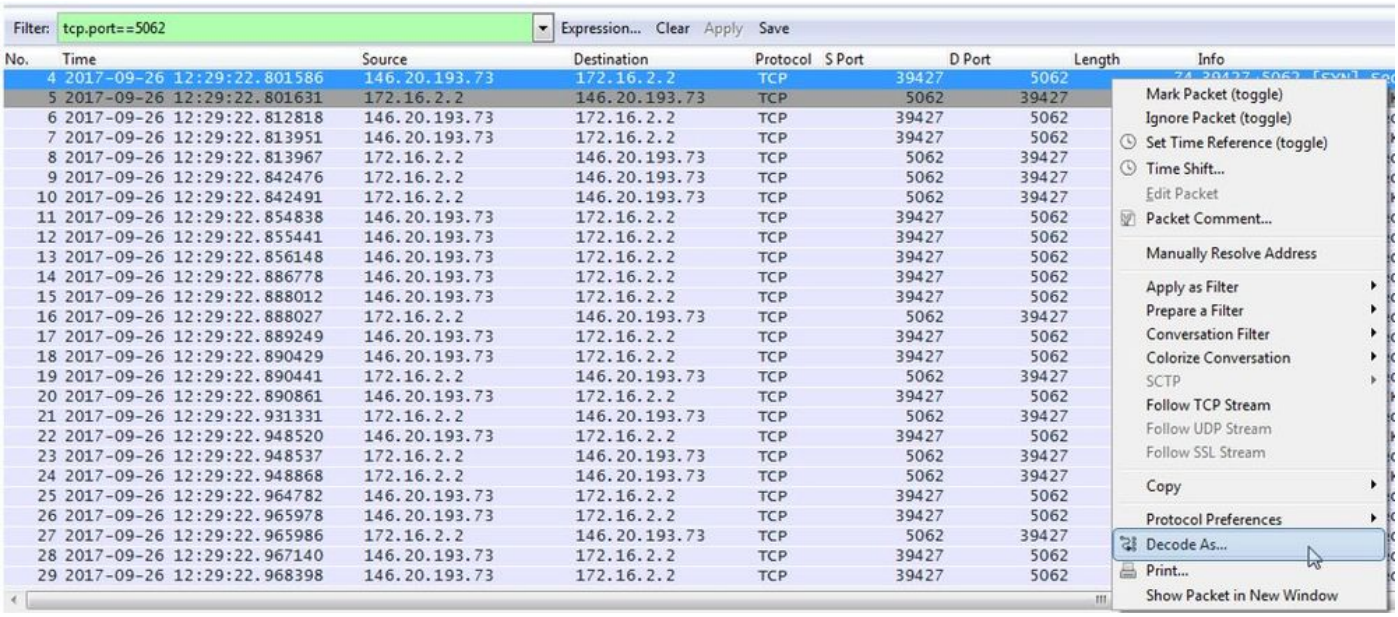
默认情况下，Wireshark 会将 SIP TLS 流量标记为端口 5061。这意味着，每当您想分析端口5062上发生的（相互）TLS握手时，Wireshark都不知道如何正确解码流量。以下为端口 5062 上发生的双向 TLS 握手的示例（如图所示）。



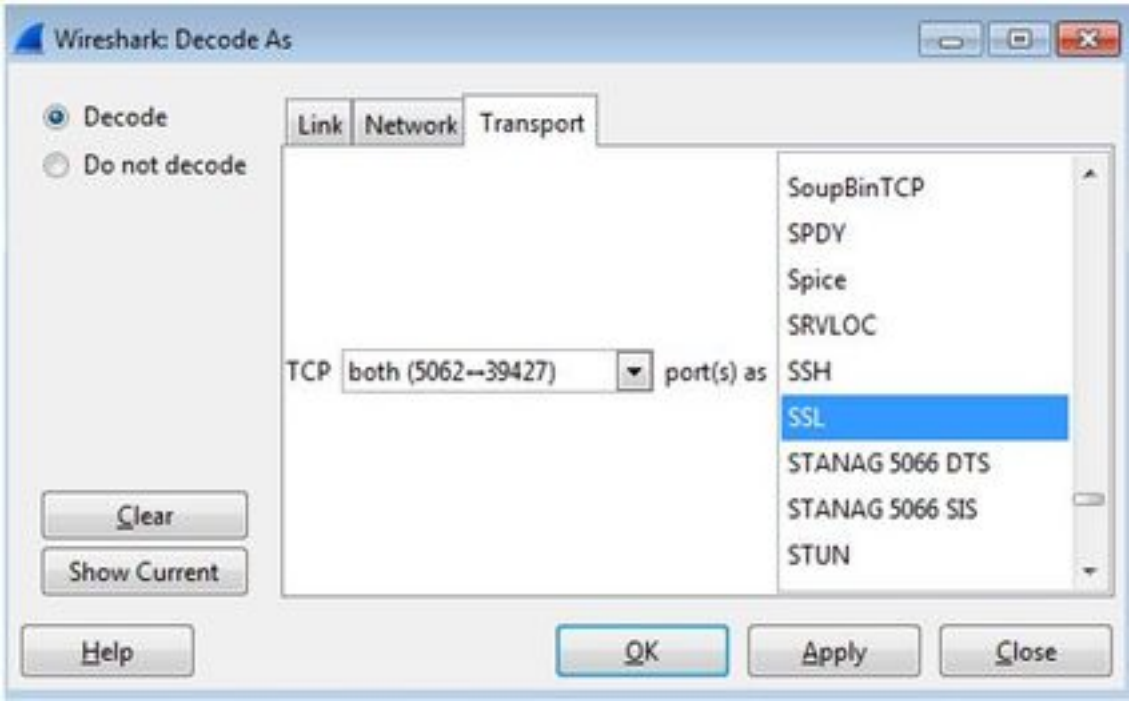
这便是 Wireshark 采用默认设置时的握手情形 。175 号数据包是 Expressway 发送到 Cisco Webex 的证书。但是，如果不解码流量，您无法确定这一点。您可以使用两种方法来解码此流量，以便您可以更轻松地查看证书信息以及存在的任何错误消息。

1a。将流解码为 SSL

a.分析相互TLS握手时，首先按**tcp.port==5062**过滤捕获。然后，右键单击流中的第一个数据包，然后选择**Decode As...** 如图所示.



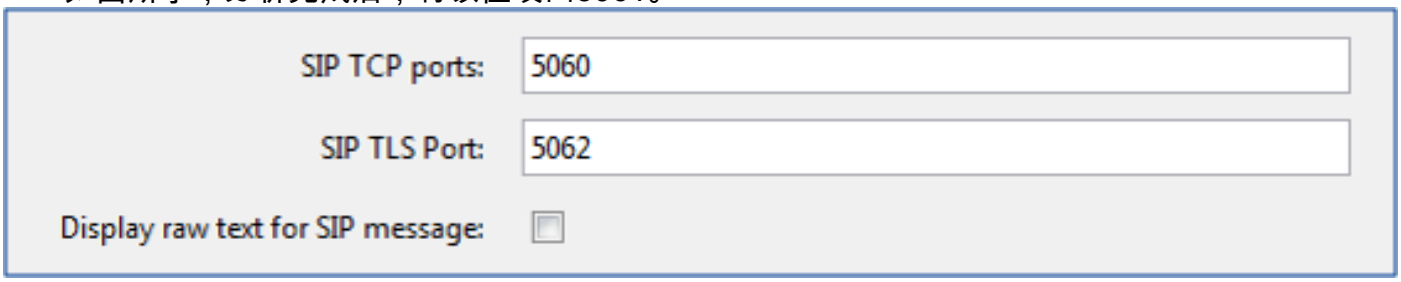
b.选中**解码为...选项后，您将看到一个列表，您可以在其中选择如何解码您选择的流。**从列表中选择SSL，**单**击**Apply**并关闭窗口。此时，整个流会显示在握手时交换的证书和错误消息（如图所示）。



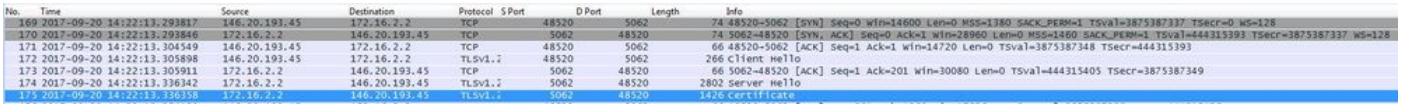
1b调整 SIP TLS 端口

在 Wireshark 首选项中将 SIP TLS 端口调整为 5062 后，您可以看到有关握手的所有详细信息，包括证书信息。请执行以下操作进行此更改：

- 打开 Wireshark
- 导航到**编辑 > 首选项**
- 展开“协议”，并选择 **SIP**
- 将 SIP TLS 端口设置为 5062，然后点击**应用**
- 如图所示，分析完成后，将该值设回5061。



如果您现在对相同的捕获进行分析，您会看到数据包 169-175 已解码。数据包 175 显示 Expressway E 证书，并且如果深入查看数据包，您可以看到证书的全部详细信息（如图所示）。



2. Wireshark过滤

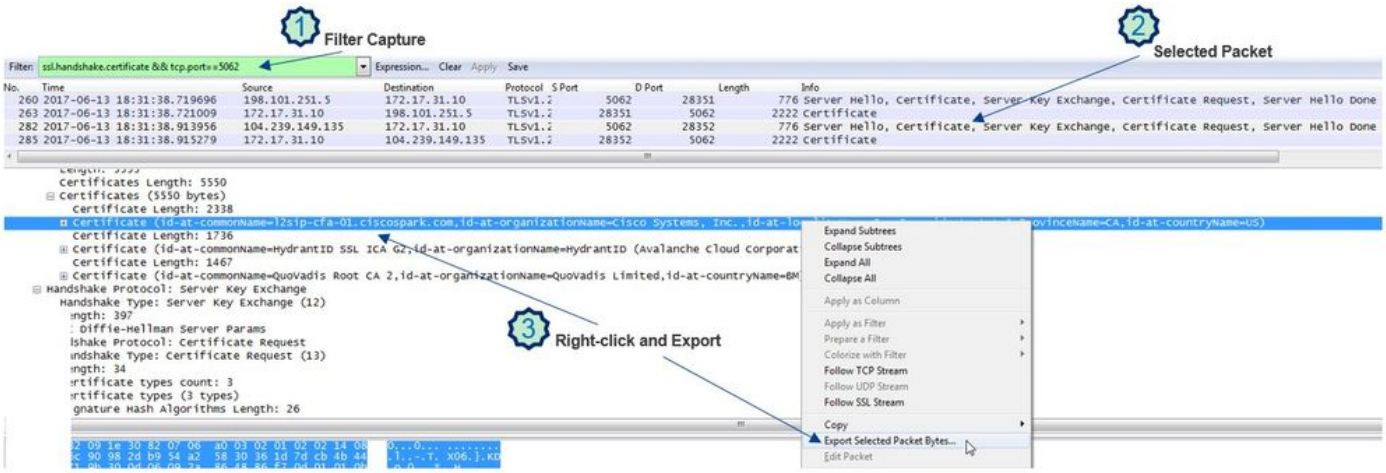
在分析数据包捕获时，您很容易迷失在给定捕获中观察到的大量数据包中。您需要了解您最感兴趣的流量类型，以便您能够对 Wireshark 进行过滤，仅显示这些流量类型。以下是一些常见的 Wireshark 过滤器，可以用来获取有关双向 TLS 握手的详细信息：

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

3.从Pcap提取证书

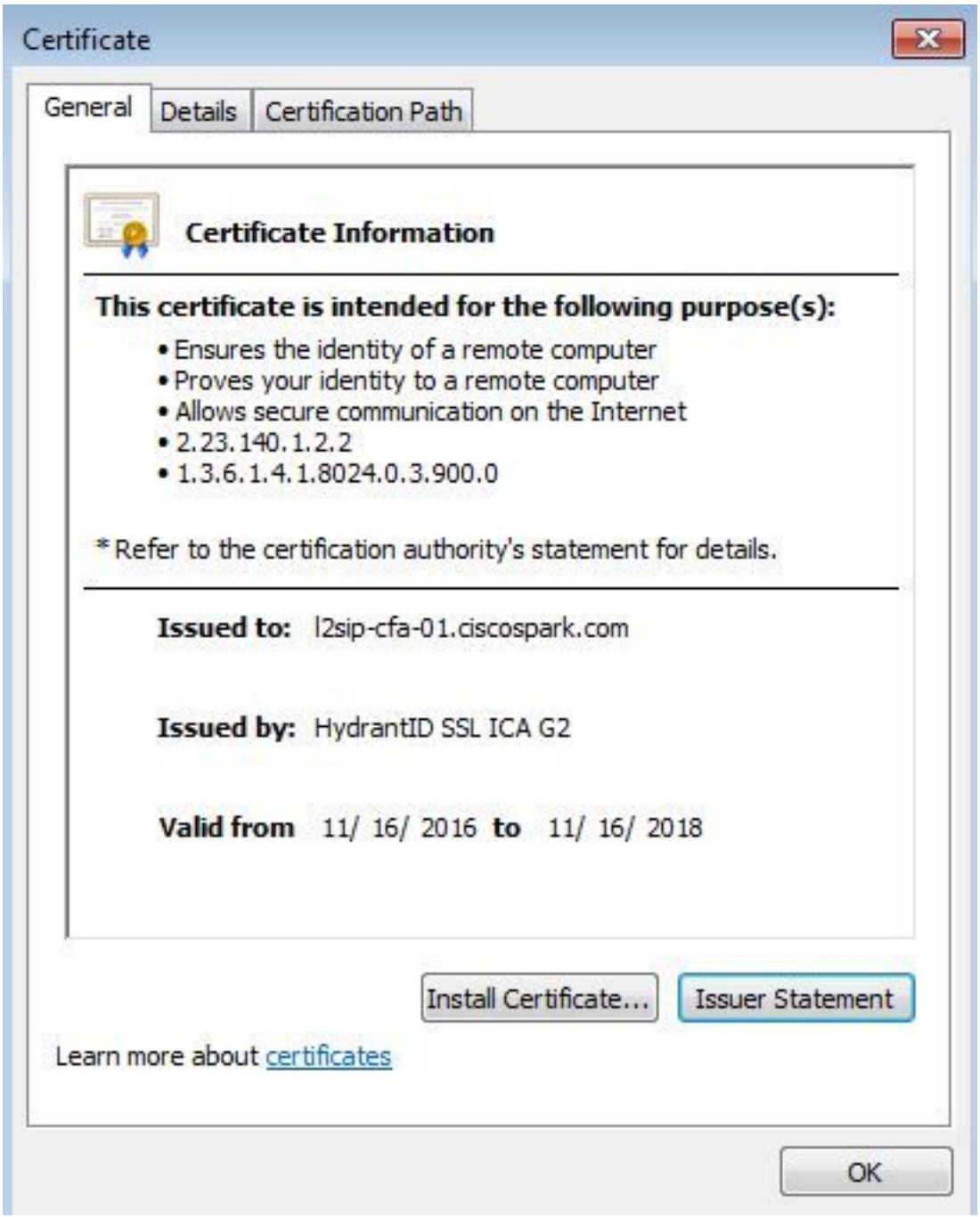
有时，您可能需要获取证书（服务器、根或中间）的副本。 如果不知道在哪里可以找到要搜索的证书，您可以直接从数据包捕获中提取证书。以下是有关如何提取双向 TLS 握手中提供的 Cisco Webex 证书的步骤。

1. 使用 **ssl.handshake.certificate && tcp.port==5062 过滤数据包捕获**
2. 找到来自 Webex 服务器地址且包含“信息”部分介绍的证书的数据包。
3. 在数据包详细信息中，展**开安全套接字层> TLS证书>握手协议>证书。 注意**：证书链中的底层/最后一个证书是根 CA。
4. 右键单击感兴趣的证书，然后选择**导出所选数据包字节...（如图所示）。**



5.将文件另存为**.cer**。

6.双击保存的文件以打开证书，如图所示。



4.调整Expressway日志记录级别

Expressway 上有两个可用的日志记录模块，这可以帮助您更好地了解，在分析证书时 Expressway 所执行的逻辑：

- developer.ssl
- developer.zone.zonemg

默认情况下，这些日志模块设置为 INFO 级别。当日志模块设置为 DEBUG 级别时，您将可看到证书检测的相关信息，以及流量被映射到哪个区域。这些功能都与混合呼叫服务有关。

Expressway E 对 Cisco Webex 服务器证书执行 SAN 检测的示例。

```
2017-09-22T11:11:19.485-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,485"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700":  Detail="Handshake in progress"
Reason="want read/write"
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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1960)"
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700":  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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1629)"
Method="::TTSSL_retrieveCommonName" Thread="0x7f576cbee700":  Detail="Found common name in peer
certificate" CommonName="l2sip-cfa-01.ciscospark.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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700":  Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.ciscospark.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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700":  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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700":  Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01-web.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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700":  Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-web.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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700":  Detail="Found DNS alt-name in peer
certificate" AltName="callservice.ciscospark.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="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654)"
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700":  Detail="Found DNS alt-name in peer
certificate" AltName="callservice.call.ciscospark.com"
```

Expressway E 将 MTL 连接映射到 Cisco Webex 混合 DNS 区域的示例:

```
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="ppcmains/oak/zones/ZoneManager.cpp(1226)"
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" getDNSZoneByTLSVerifySubjectName classified subject name
callservice.ciscospark.com into DNS zone Hybrid Call Services DNS
```

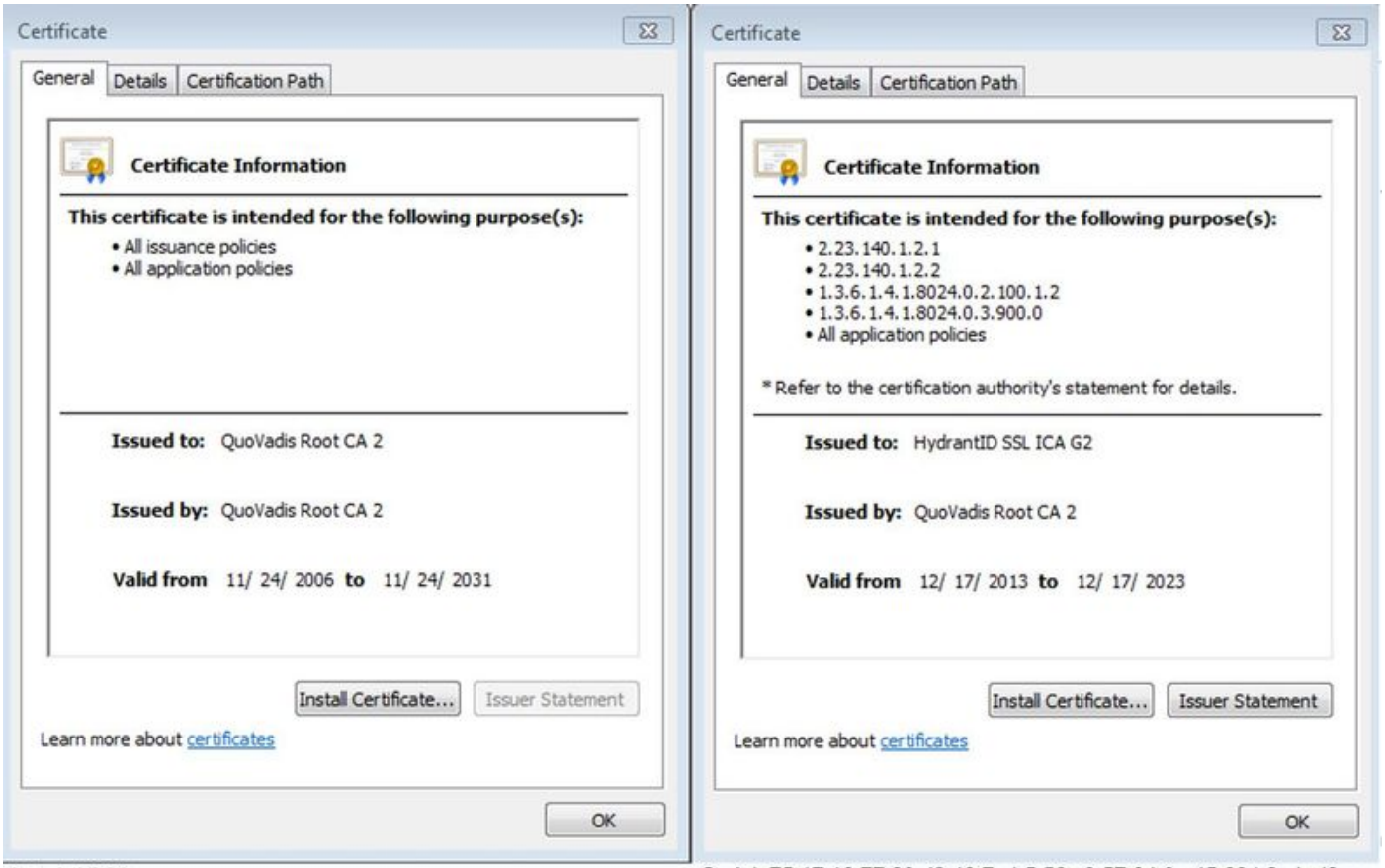
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564" Module="developer.zone.zonemgr" Level="DEBUG" CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1183)" Method="ZoneManager::getDNSZoneByTLSVerifySubjectNameList" Thread="0x7f577f0a0700": this="0x56408ff81220" Detail="**Searched for DNS Zones by Subject Name**" Found="True" Candidates="l2sip-cfa-01.ciscospark.coml2sip-cfa-01.ciscospark.coml2sip-cfa-01.wbx2.coml2sip-cfa-01-web.wbx2.coml2sip-cfa-web.wbx2.comcallservice.ciscospark.com" **MatchedZone="Hybrid Call Services DNS" MatchedIdentity="callservice.ciscospark.com"**
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="ppcmains/oak/zones/ZoneManager.cpp(1054)" Method="ZoneManager::getZoneByIdentities" Thread="0x7f577f0a0700": this="0x56408ff81220" Detail="getZoneByIdentities, **match complete**" Identitites="{CN: l2sip-cfa-01.ciscospark.com, Alt-DNS: l2sip-cfa-01.ciscospark.com, Alt-DNS: l2sip-cfa-01.wbx2.com, Alt-DNS: l2sip-cfa-01-web.wbx2.com, Alt-DNS: l2sip-cfa-web.wbx2.com, Alt-DNS: callservice.ciscospark.com, **Alt-DNS: callservice.call.ciscospark.com**, Alt-DNS: l2sip-a-Webexcall.ciscospark.com, Alt-DNS: l2sip-prod-11-dfw-public.wbx2.com, Alt-DNS: l2sip-prod-12-dfw-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-294-riad-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-817-riad-public.wbx2.com, Alt-DNS: l2sip-l2sip-prod-wpsjc-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpsjc-web.wbx2.com, Alt-DNS: l2sip-l2sip-prod-wpdfw-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpdfw-web.wbx2.com, Alt-DNS: l2sip-cfa-02.wbx2.com, Alt-DNS: Webexcmr-wpa.ciscospark.com, Alt-DNS: Webexcmr-wpb.ciscospark.com, Alt-DNS: Webexcmr-wpc.ciscospark.com, Alt-DNS: l2sip-wpa-01.wbx2.com, Alt-DNS: l2sip-wpa-02.wbx2.com, Alt-DNS: l2sip-wpb-01.wbx2.com, Alt-DNS: l2sip-wpb-02.wbx2.com, Alt-DNS: l2sip-wpc-01.wbx2.com, Alt-DNS: l2sip-wpc-02.wbx2.com}" **MatchMechanism="DNSZoneMatch" MatchedZone="Hybrid Call Services DNS"**

下文列出了与 Expressway E 和 Cisco Webex 双向 TLS 故障相关的最常见问题。

问题1. Expressway-E不信任签署Cisco Webex证书的证书颁发机构(CA)

直接与 Expressway E 通信的 Cisco Webex 服务器称为 L2SIP 服务器。此L2SIP服务器将由中间服务器签名，该中间服务器的公用名称为Hydrant SSL ICA G2。中间服务器由根证书颁发机构签名，根证书颁发机构的公用名称为QuoVadis Root CA 2，如图所示。

注意：这可能会有变动。



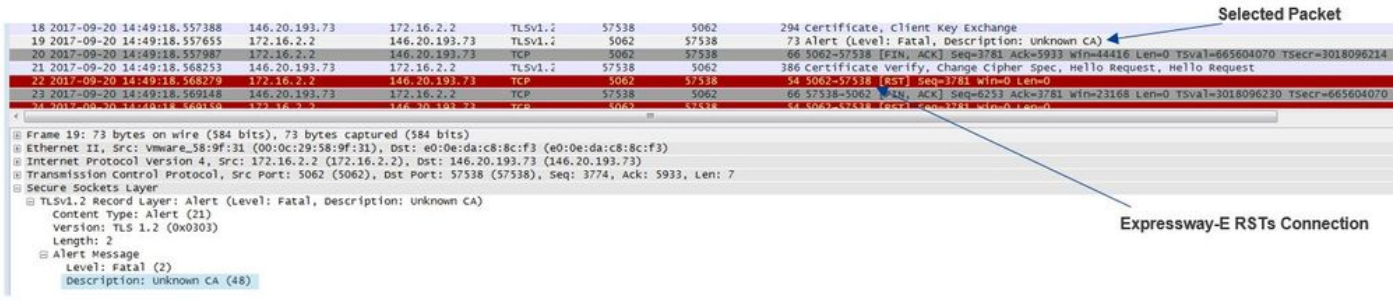
从 Expressway 诊断角度分析流量时，第一步是要搜索 **TCP 连接**。搜索 **TCP 连接**后，您需要寻找 **Dst-port=5062 的值**。您在日志中确定尝试并建立此连接的区域后，可寻找 TLS 握手（通常由指示正在进行握手的日志条目表示）。

```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700":  Detail="Handshake in progress"
Reason="want read/write"
```

如果 Expressway-E 不信任 Cisco Webex 签名证书，则在握手完成后，Expressway E 会立即拒绝此证书。您可以通过这些日志条目在 Expressway E 日志记录中看到这些：

```
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"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSLErrorOutput" Thread="0x7f29ddefa700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="-1" error="1" bServer="true"
localAddress="['IPv4''TCP''172.16.2.2:5062']" remoteAddress="['IPv4''TCP''146.20.193.73:58531']"
ssl_error_reason="error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify
failed"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="self signed certificate in certificate
chain"
```

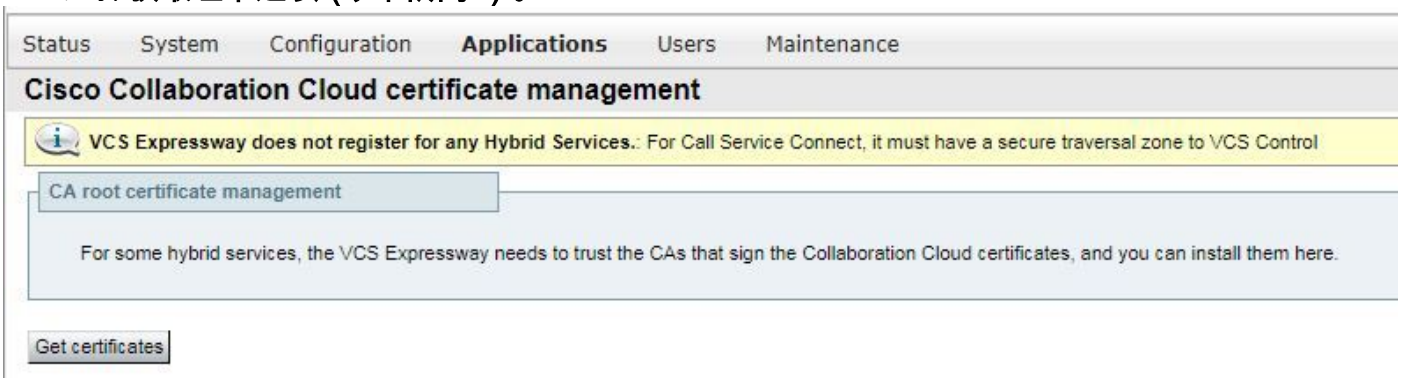
Expressway错误消息可能会稍有误导，因为它是指证书链中的自签名证书。Wireshark允许您更仔细地查看交换。从Wireshark数据包捕获分析的角度来看，您可以清楚地看到，当Webex环境提供其证书时，Expressway会转过身来拒绝带有未知CA错误的证书，如图所示。



解决方案：

为了解决这个问题，您必须确保 Expressway E 信任 Cisco Webex 证书颁发机构。尽管常用的方法已经很简单（您只需从 Wireshark 跟踪提取这些证书并将其上传到 Expressway 上受信任 CA 证书库），但 Expressway 提供方法更加简单：

- 登录到 Expressway E
- 导航至“应**用”>“云证书管理”**
- 选择**获取证书选项（如图所示）。**



此时，Cisco Webex 证书颁发机构已上传到 Expressway E 受信任 CA 库（**维护 > 安全 > 受信任 CA 证书**）。

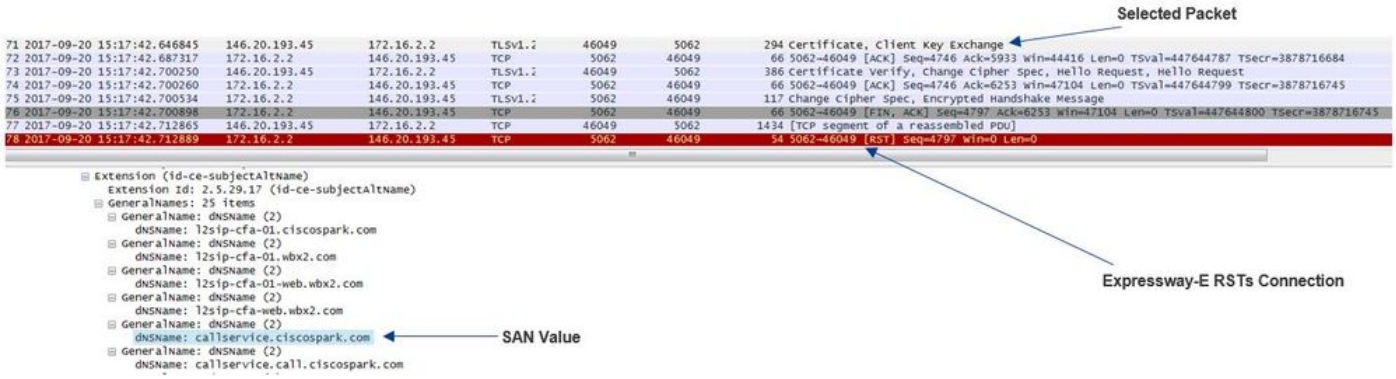
问题 2 TLS 主体名称不正确，验证 Expressway E Cisco Webex 混合 DNS 区域中的名称

作为双向 TLS 握手的一部分，混合呼叫服务连接使用 TLS 验证。这意味着，除了信任Cisco Webex CA证书外，Expressway还通过检查所显示证书的使用者备用名称(SAN)字段来验证证书，以确保其具有**callservice.ciscospark.com等**值。如果此值不存在，则入站呼叫将失败。

在此特定场景中，Cisco Webex服务器将其证书呈现给Expressway-E。证书实际上有 25 个不同的SAN。假设Expressway-E检查callservice.ciscospark.com SAN的证书，但未找到该证书。在这种情况下，您会在诊断日志记录找中看到与以下类似的错误：

```
2017-09-20T11:17:42.701-04:00 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"
2017-09-20T11:17:42.701-04:00 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"
```

如果您使用 Wireshark 分析此证书握手，您会发现 Cisco Webex 提供证书后，Expressway 会立即重置连接（如图所示）。



要确认此值的配置，您可以转到为此解决方案配置的 Webex 混合 DNS 区域。如果您有 Expressway E xConfiguration，您可以查看区域配置章节，确定已配置 TLS 验证主体名称的方式。对于 xConfiguration，请注意，区域顺序为区域 1 排在第一个。以下为上述问题环境的 xConfiguration。

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

如示例所示，TLS验证主题名称设置为**calllservice.ciscospark.com，而**不是**callservice.ciscospark.com**。（请注意额外的“l”）。

解决方案：

为解决此问题，必须修改 TLS 验证主体名称：

- 登录到 Expressway E
- 导航到**配置 > 区域 > 区域**
- 选择 **Webex 混合服务 DNS 区域**
- 将TLS验**证主题名称**设置为**callservice.ciscospark.com**
- 选择**保存**

> **注意**：有关基线日志记录行为，请参阅。此章节介绍 Expressway 的证书验证过程以及到 Webex 混合 DNS 区域的映射。

> **注意**：自Expressway代码x12.5及更高版本起，新的“Webex”区域已发布。此Webex区域预填充与Webex通信所需区域的配置。这意味着您不必再设置TLS主题验证模式和TLS验证主题名称。为简化配置，如果您运行的是x12.5或更高版本的Expressway代码，建议使用Webex区域。

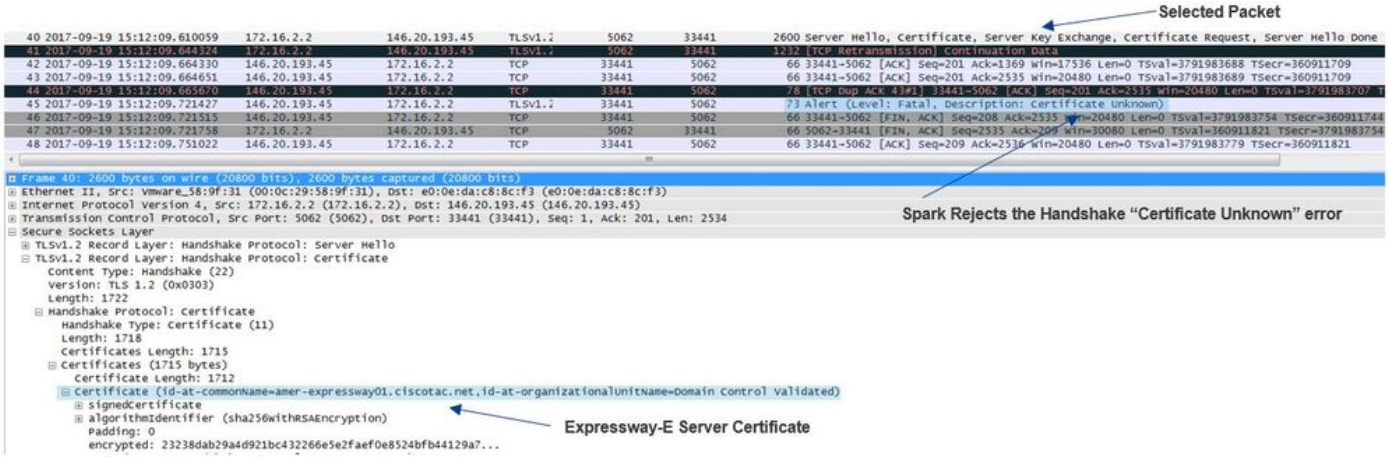
问题 3 Expressway E 未向 Cisco Webex 发送完整证书链

作为双向 TLS 握手的一部分，Cisco Webex 必须信任 Expressway E 证书。Cisco Webex 拥有受信任公共 CA 的完整列表。通常，如果您的 Expressway E 证书由 Cisco Webex 支持的公共 CA 签署，TLS 握手都会成功。根据设计，Expressway-E仅在TLS握手期间发送其证书，尽管它由公共CA签名。要发送完整的证书链（根和中间），必须将这些证书添加到Expressway-E自身的受信任CA证书存储中。

否则，Cisco Webex 会拒绝 Expressway E 的证书。要对与此问题匹配的情况进行故障排除，您可以使用 Expressway E 的诊断日志和 tcpdump。在分析 Expressway E 诊断日志时，您将看到与以下类似的错误：

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" UTCTime="2017-09-19 15:12:09,721"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721" Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)" Method="::TTSSLErrorOutput" Thread="0x7fc67c6ec700": TTSSL_continueHandshake: **Failed to establish SSL connection** iResult="0" error="1" bServer="true" localAddress="['IPv4''TCP''172.16.2.2:5062']" remoteAddress="['IPv4''TCP''146.20.193.45:33441']" ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:**sslv3 alert certificate unknown**"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721" Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2" Dst-port="**5062**" Detail="**TCP Connection Closed**" Reason="**Got EOF on socket**"

从 Wireshark 角度进行分析时，您将看到 Expressway E 提供了它的证书。展开数据包，您可以看到仅发送了服务器证书。随后，Cisco Webex 拒绝了此 TLS 握手并提示未知 CA 错误消息（如图所示）。

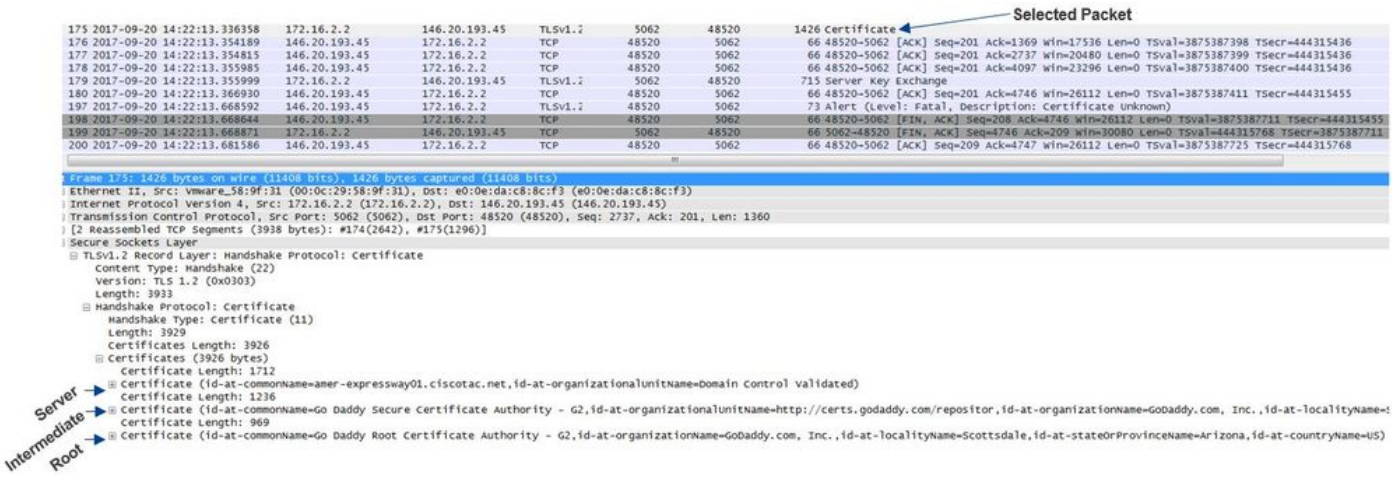


解决方案：

为了解决此问题，您必须将 Expressway E 证书签名中涉及的中间 CA 和根 CA 上传到受信任 CA 证书库中：

第 1 步： 登录到 Expressway E。
第 2 步： 导航到**维护 > 安全 > 受信任 CA 证书**。
第 3 步： 在用户界面底部附近的“上传”菜单中，选择**选择文件。**
第 4 步： 选择 Expressway E 证书签名涉及的 CA 证书。
第 5 步： 选择**添加 CA 证书**。
第 6 步： 对 Expressway E 证书签名涉及的所有 CA 证书（中间证书和根证书）重复以上步骤。
第 7 步： 选择**添加 CA 证书**。

完成此过程后，您将看到密钥交换中包含 Expressway E 服务器证书签名涉及的完整证书链。以下为使用 Wireshark 分析数据包捕获时您会看到的内容示例。



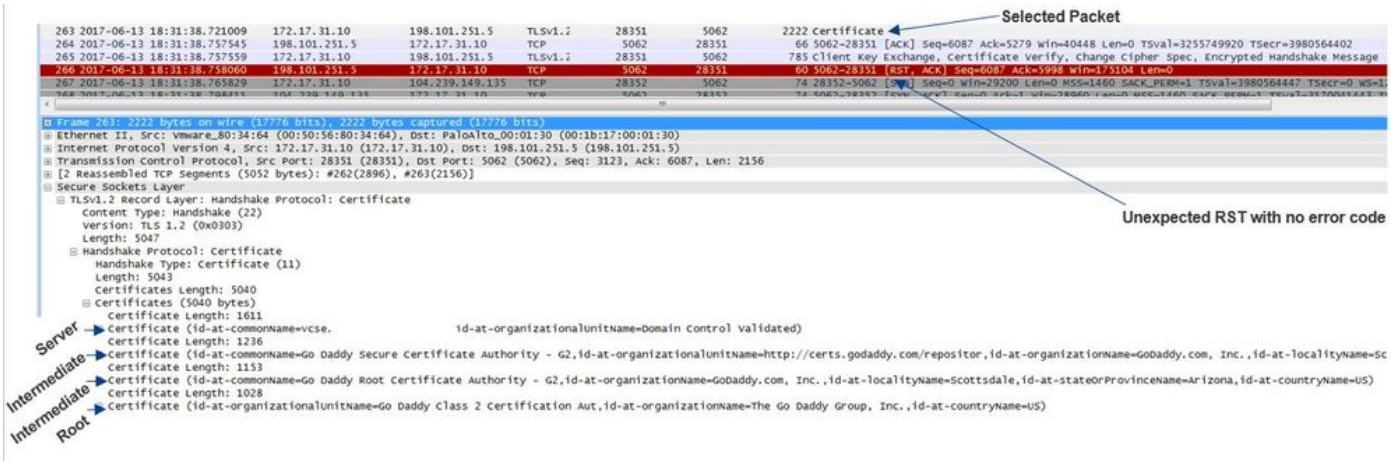
问题 4 防火墙终止双向 TLS 握手

Expressway解决方案通常与防火墙连接。很多时候，适用于此解决方案的内联防火墙会运行某些类型的应用层检测。通常，使用Expressway解决方案时，当防火墙运行应用层检查时，管理员会看到不良结果。此问题可帮助您确定防火墙的应用层检测在何时突然断开了连接。

您可以在 Expressway 诊断日志中查找已尝试的双向 TLS 握手。如前所述，在端口 5062 上建立 TCP 连接后会立即进行此握手。在此场景中，当防火墙终止连接时，您将可在诊断日志记录中看到这些错误。

```
Thread="0x7f6496669700": TTSSL_continueHandshake: Failed to establish SSL connection iResult="-
1" error="5" bServer="false" localAddress="['IPv4''TCP''172.17.31.10:28351']"
2017-06-13T13:31:38.760-05:00 vcse tvcs: Event="Outbound TLS Negotiation Error" Service="SIP"
Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062" Detail="No SSL
error available, probably remote disconnect" Protocol="TLS" Common-
name="callservice.ciscospark.com" Level="1" UTCTime="2017-06-13 18:31:38,758"
2017-06-13T13:31:38.760-05:00 vcse tvcs: UTCTime="2017-06-13 18:31:38,758" Module="network.tcp"
Level="DEBUG":  Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062"
Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

从数据包捕获的角度来看，您会发现 Expressway E 向 Cisco Webex 提供了它的证书。您会看到存在来自 Cisco Webex 方向的 TCP RST（如图所示）。



乍一看，您可能认为 Expressway E 的证书存在错误。要解决此问题，您首先需要回答以下问题：

- Expressway E 证书是由 Cisco Webex 信任的公共 CA 签署吗？
- 是否已将 Expressway E 证书以及 Expressway E 证书签名涉及的所有证书手动上传到 Cisco

Webex Control Hub (https://admin.ciscospark.com) ？

在此情形中，解决方案不是使用 Cisco Webex Control Hub 管理 Expressway E 的证书。这表示 Expressway E 证书必须由 Cisco Webex 信任的公共 CA 签署 。通过选择 Wireshark 捕获中的证书数据包（如上图所示），您可以看到，证书是由公共 CA 签署，且已向 Cisco Webex 发送完整的证书链。因此，此问题应该与 Expressway 证书无关。

此时，如果有必要进行进一步隔离，您需要从防火墙的外部接口上移除数据包捕获。但是，诊断日志中不存在 SSL 错误是一个重要的数据点。如前所述（问题 3），*如果 Cisco Webex 不信任 Expressway E 的证书，您必定会看到 SSL 断开的原因。*然而在这种情况，没有显示任何 SSL 错误。

> **注意：**如果您从防火墙外部接口上移除数据包捕获，您将不会看到来自 Cisco Webex 环境的 TCP RST。

解决方案

对于此解决方案，您的合作伙伴或客户必须依赖于您的安全团队。安全团队必须调查他们是否对 Expressway 解决方案应用了任何类型的应用层检测，如果他们使用了应用层检测，则应禁用此检测。**《VCS 控制和 Expressway 部署指南 》**附录 4 给出了建议客户关闭此功能的原因。

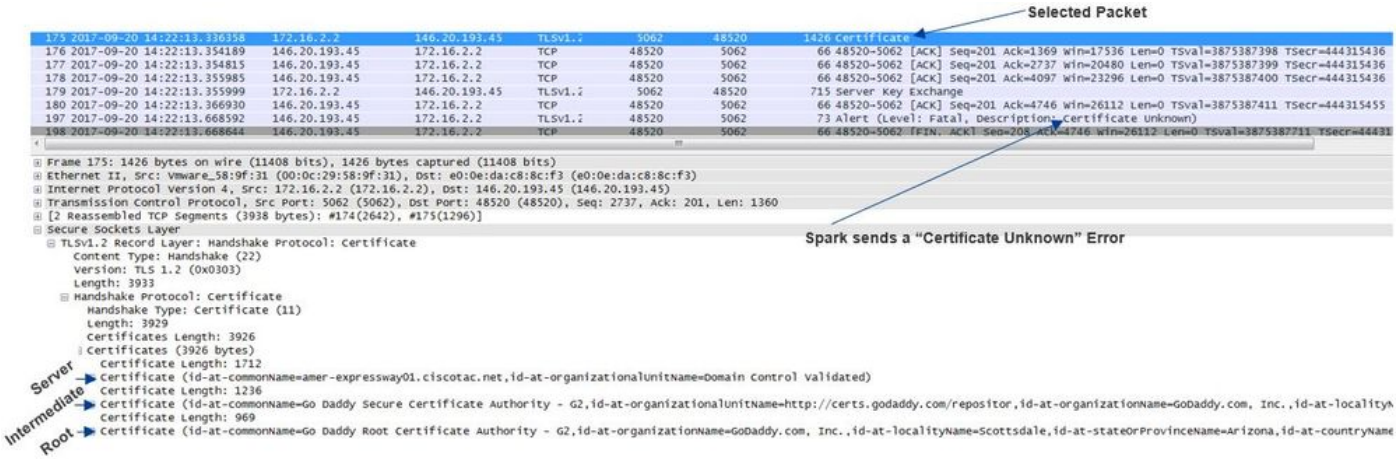
问题 5 Expressway E 由公共 CA 签署，但 Cisco Webex Control Hub 已加载备用证书

当您从零开始部署 Expressway 解决方案且 Expressway E 证书最初不是由公共 CA 签署时，常常会出现这种情况。在这种情况下，您将 Expressway E 服务器证书（已由内部签署）上传到 Cisco Webex Control Hub，以便您可以成功完成双向 TLS 协商。然后，您的 Expressway E 证书最终由公共 CA 签署，但您忘了从 Cisco Webex Control Hub 中移除服务器证书。要知道，当证书上传到 Cisco Webex Control Hub 后，此证书将优先于 Expressway 在 TLS 握手过程中提供的证书和证书链。

从Expressway E诊断日志记录的角度来看，此问题可能类似于Cisco Webex不信任Expressway E证书时遇到的日志记录签名 — 例如，Expressway E未发送其完整链或Expressway E证书未由Cisco Webex信任的公共CA签名。以下为 TLS 握手过程中 Expressway E 日志记录示例：

```
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-20
14:22:13,668"
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:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="network.tcp" Level="DEBUG":  Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

从Wireshark的角度来看，您可以在此看到Expressway E在行项目175中显示其证书。稍后，Cisco Webex环境会拒绝证书，但证书未知错误如图所示。



如果您选择 Expressway E 发送的证书数据包，您可以展开证书信息，以确定 Expressway E

1.是由 Cisco Webex 信任的公共 CA 签署的，以及

2.它是否包括签名涉及的完整证书链。

在此情况下，这两个条件均符合。这表明 Expressway E 证书没有任何错误。

解决方案

第 1 步： 登录到 Cisco Webex Control Hub。
第 2 步： 从左侧窗格中选择**服务。**

第 3 步： 在“混合呼叫”卡片下选择**设置。**

第 4 步： 滚动至“呼叫服务连接”部分，在“加密 SIP 呼叫的证书”下查看列表中是否存在不需要的证书。如果是，点击证书旁边的垃圾桶图标。

第 5 步： 选择**删除。**

> **注意：**在删除证书之前，必须进行分析并确定客户未在使用上传到 Webex Control Hub 的证书。

有关在 Cisco Webex Control Hub 中上传 Expressway E 证书的详细信息，请查看《混合呼叫部署指南》中的此章节。

问题 6 Expressway 未将入站呼叫映射到 Cisco Webex 混合 DNS 区域

入站 TLS 映射功能与 TLS 验证主体名称配合使用，两者均在混合呼叫 DNS 区域配置。此场景详细说明了在x12.5之前Expressway发现的问题和挑战。在x12及之后，实施了名为“Webex”区域的新区域类型。此区域预填充与Webex集成所需的所有配置。如果运行x12.5并部署Webex混合呼叫，建议使用**Webex** 区域类型，以便为您自动配置混合呼叫服务域(callservice.webex.com)。此值与Webex证书的使用者备用名称匹配，该名称在相互TLS握手期间显示，并允许连接和入站映射成功到Expressway。

如果您使用的代码版本低于x12.5，或者未使用Webex区域，您将希望继续下面的说明，说明如何识别并纠正Expressway未将入站呼叫映射到Webex混合DNS区域的问题。

该功能分为三个步骤：

1. Expressway E 接受 Cisco Webex 证书。
2. Expressway E 检查 Cisco Webex 证书，以确定是否有匹配 TLS 验证主体名称的备用主体名称：callservice.ciscospark.com。
3. Expressway E 通过 Cisco Webex 混合 DNS 区域映射入站连接。

如果身份验证不成功，则表明证书验证失败。如果 Expressway E 配置了企业到企业场景，则呼叫会进入默认区域并会根据企业到企业场景的搜索规则进行路由。

像其他场景一样，您必须使用诊断日志记录和数据包捕获来确定故障情况，然后使用数据包捕获查看是哪一端发送 RST。以下为尝试并建立 TCP 连接的示例。

```
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"
```

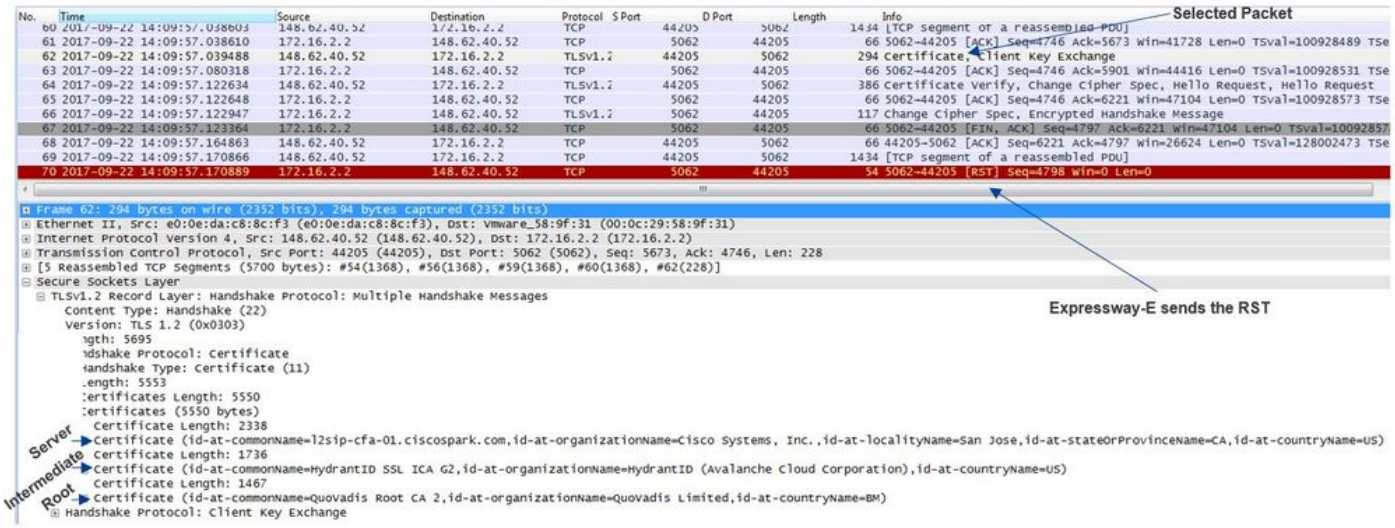
成功建立 TCP 可为 TLS 握手提供保障。您会发现，开始握手后不久就出现了错误。

```
2017-09-22T10:09:57.044-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,044"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f044e7cc700":  Detail="Handshake in progress"
Reason="want read/write"
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"
UTCTime="2017-09-22 14:09:57,123"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,123"
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 Closed" Reason="Peer's TLS certificate identity was
unacceptable"
```

从 pcap 的角度分析此情况，您能够更好地了解

- 谁发送 RST，以及
- 传递了哪种证书，以确定它们是否正确。

在分析此特定的捕获时，您可以看到是 Expressway E 发送了 RST。在查看传递的 Cisco Webex 证书时，您可以看到它了发送完整的链。此外，您可以根据诊断日志中的错误消息进行判断，您可以排除 Expressway E 不信任 Cisco Webex 公共 CA 的场景。否则，您会看到类似于“**证书链中村子自签名证书**”的错误。 您可以深入查看数据包详细信息（如图所示）。



单击Webex服务器证书并展开该证书以查看使用者备用名称(dnsName)，您可以验证以确保其列**有callservice.ciscospark.com**。

导航到 Wireshark：**证书 > 扩展名 > 常规名称 > GeneralName > dNSName:callservice.ciscospark.com**

可通过这一点确认 Webex 证书无任何问题。

您现在可以确认 TLS 验证主体名称是正确的。如前所述，如果您有 xConfiguration，您可以查看区域配置章节，确定已配置 TLS 验证主体名称的方式。有关 xConfiguration 注意的一点是，区域顺序为首先创建区域 1。以下为上述问题环境的 xConfiguration。显然 TLS 验证主体名称无任何错误。

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

那么接下来需要查看 **TLS 验证入站映射**。这能够确认您是否正确地将 TLS 连接映射到了 Webex 混合 DNS 区域。xConfiguration 也可用于此分析。在 xConfiguration **中，TLS 验证入站映射被称为 DNS ZIP TLS 验证 InboundClassification**。在此示例中，该值设置为“关”。

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "Off"
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
```

如果此值设置为“关闭”，则这意味着VCS被阻止尝试将入站TLS连接映射到此区域。如果在Expressway-E上配置了企业到企业方案，则呼叫会进入默认区域，并根据为企业到企业方案提供的搜索规则进行检查和路由。

解决方案

要解决此问题，您需要将混合呼叫DNS区域上的TLS验证入站映射设置为“打开”。以下是完成该操作的步骤。

1. 登录到 Expressway E
2. 导航到**配置 > 区域 > 区域**
3. 选择**混合呼叫 DNS 区域**
4. 对于 **TLS 验证入站映射**，选择**开**
5. 选择**保存**

注意：有关基线日志记录行为，请参阅。此章节介绍 Expressway 的证书验证过程以及到

Webex 混合 DNS 区域的映射。

问题 7 Expressway E 使用默认自签名证书

在一些新的混合呼叫服务连接部署中，Expressway E 证书签名被忽略或认为可以使用默认服务器证书。有些人认为，这可能是因为 Cisco Webex Control Hub 让您将自定义证书加载到门户中了。（**服务 > 设置（在混合呼叫卡片下）> 上传（在已加密呼叫证书下）**）

如果您密切关注**加密 SIP 呼叫证书的措辞，您会看到：**“请使用 Cisco Collaboration 默认信任列表中提供的证书或上传您自己的证书。如果您使用自己的证书，请确保主机名位于已验证的域中。”该语句的关键点在于**“请确保主机名位于已验证的域中。”**

当您对与此情形匹配的问题进行故障排除时，请记住，故障现象取决于呼叫的方向。如果呼叫由内部电话发出，则 Cisco Webex 应用程序不会振铃。此外，如果您尝试在 Expressway 搜索历史记录中跟踪该呼叫，您会发现该呼叫到达了 Expressway E 并就此停止。如果呼叫是由 Cisco Webex 应用程序发往现场设备，内部电话不会振铃。在这种情况下，Expressway E 和 Expressway C 搜索历史记录将不显示任何内容。

在此特定场景中，呼叫由内部电话发出。根据 Expressway E 搜索历史记录，您可以确定该呼叫到达了服务器。此时，您可以深入分析诊断日志记录，确定发生的情况。要开始进行此分析，请首先查看是否已尝试并且通过端口 5062 建立 TCP 连接。通过在 Expressway E 诊断日志中搜索“TCP 连接”并搜索包含“Dst-port=5062”标记的行项目，*您可以确定是否建立了连接。*

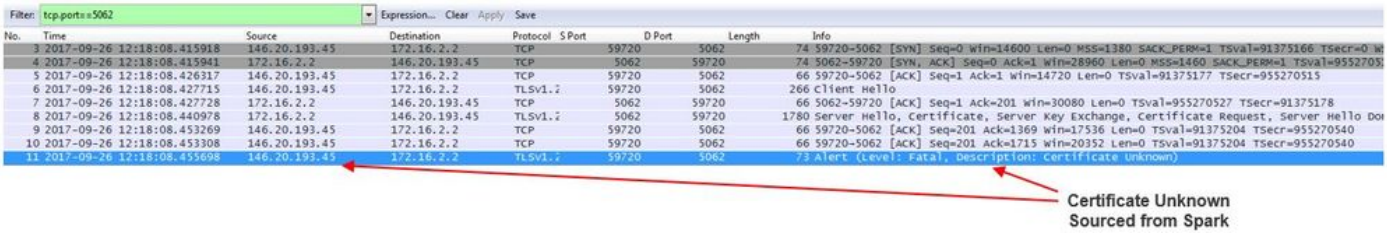
```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG":  Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG":  Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

在确认已建立 TCP 连接后，您便可以对随后立即发送的 TLS 握手进行分析。如以下代码段所示，握手失败且证书为未知证书**(Detail="sslv3 alertcertificate unknown")**

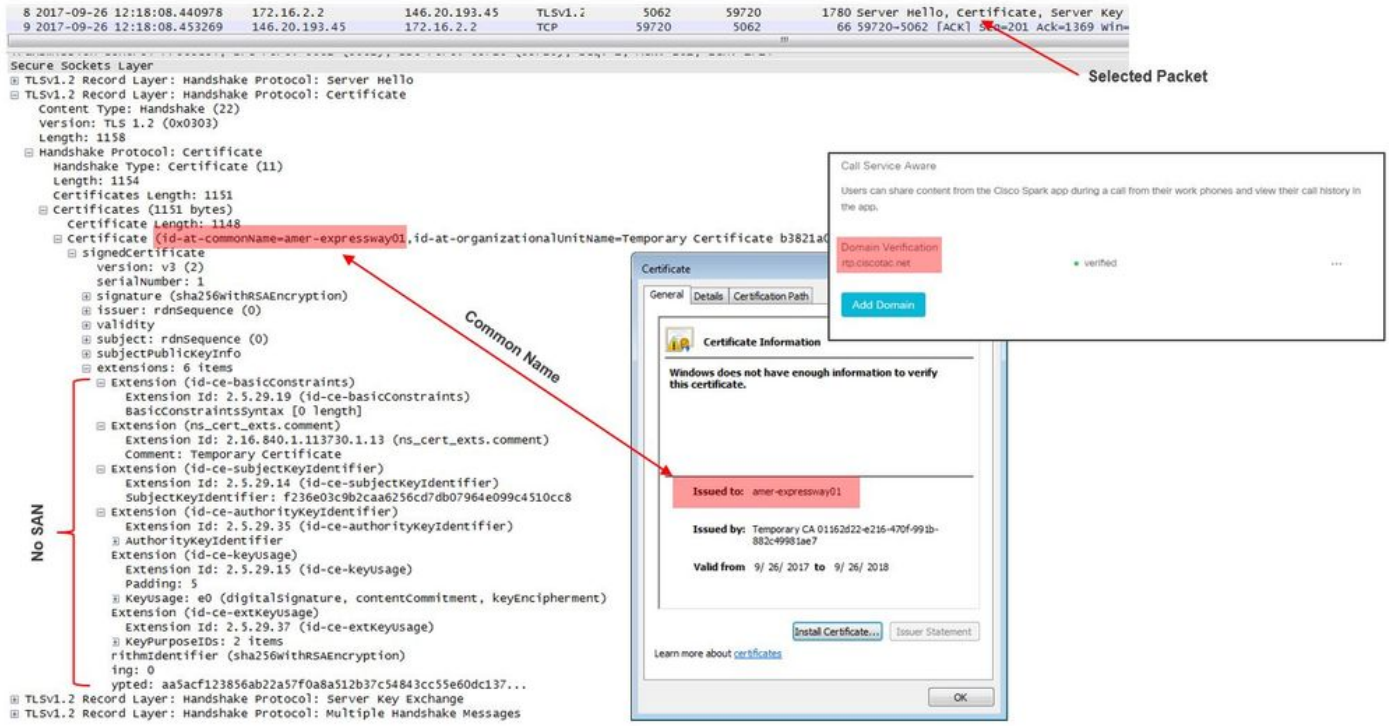
```
2017-09-26T08:18:08.441-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,441"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700":  Detail="Handshake in progress"
Reason="want read/write"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-26
12:18:08,455"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1997)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700":  Detail="Handshake Failed"
Reason="want error ssl"
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSLErrorOutput" Thread="0x7f930adab700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4''TCP''172.16.2.2:5062']" remoteAddress="['IPv4''TCP''146.20.193.45:59720']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"

2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="network.tcp" Level="DEBUG":  Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

仔细查看 Expressway E 诊断日志记录中提供的数据包捕获，您可以看到，证书未知错误源自 Cisco Webex 的方向（如图所示）。



如果您检查来自 Expressway E 的默认服务器证书，您可以看到“常用名”和“备用主体名”不包含“已验证的域” **(rtp.ciscotac.net)。** 通过这些证据，您便能找打导致此问题的原因（如图所示）。



此时，您确认 Expressway E 服务器证书需要由公共 CA 或内部 CA 签署。

解决方案

您可以通过两种方法解决此问题：

1. 使用 Cisco Webex 信任的公共 CA 签署 Expressway E 证书。
   登录到 Expressway。导航到**维护 > 安全 > 服务器证书**。选择**生成 CSR**。输入所需的证书信息并确保**额外的备用名称字段包含 Webex Control Hub 中列出的验证域。**点击**生成 CSR**。将 CSR 提供给第三方公共 CA 进行签名。证书返回后，立即导航到**维护 > 安全 > 服务器证书**。在**选择服务器证书文件旁边的上传新证书**部分，选择**选择文件并选择签名证书**。选择**上传服务器证书数据**。导航到**维护 > 安全 > 受信任 CA 证书**。在**选择包含受信任 CA 证书的文件**旁边的**上传部分，选择选择文件**。选择任何根和中间 CA 证书提供公共的 CA。选择**添加 CA 证书**。重新启动 Expressway E。
2. 使用内部 CA 签署 Expressway E 证书，然后将内部 CA 和 Expressway E 证书上传到 Cisco Webex Control Hub。
   登录到 Expressway导航到**维护 > 安全 > 服务器证书**。选择**生成 CSR**输入所需的证书信息并确保*额外的备用名称字段包含 Webex Control Hub 中列出的***验证域。**点击**生成 CSR**将 CSR

提供给第三方公共 CA 进行签名证书返回后，立即导航到*维护 > 安全 > 服务器证书*在*选择服务器证书文件旁边的上传新证书*部分，选择**选择文件并选择签名证书。**选择**上传服务器证书数据。**导航到**维护 > 安全 > 受信任 CA 证书。**在**选择包含受信任 CA 证书的文件旁边的上传部分，选择选择文件**。选择任何根和中间 CA 证书提供公共的 CA。选择**添加 CA 证书**。重新启动 Expressway E。

2a.将内部 CA 和 Expressway E 证书上传到 Cisco Webex Control Hub

1. 以管理员身份登录到 Cisco Webex Control Hub。
2. 选择**服务**。
3. 在“混合呼叫服务”卡片下选择**设置。**
4. 在“加密SIP呼**叫的证书”部分，选**择**上传**。
5. 选择内部 CA 和 Expressway E 证书。

入站:从 Cisco Webex 到本地

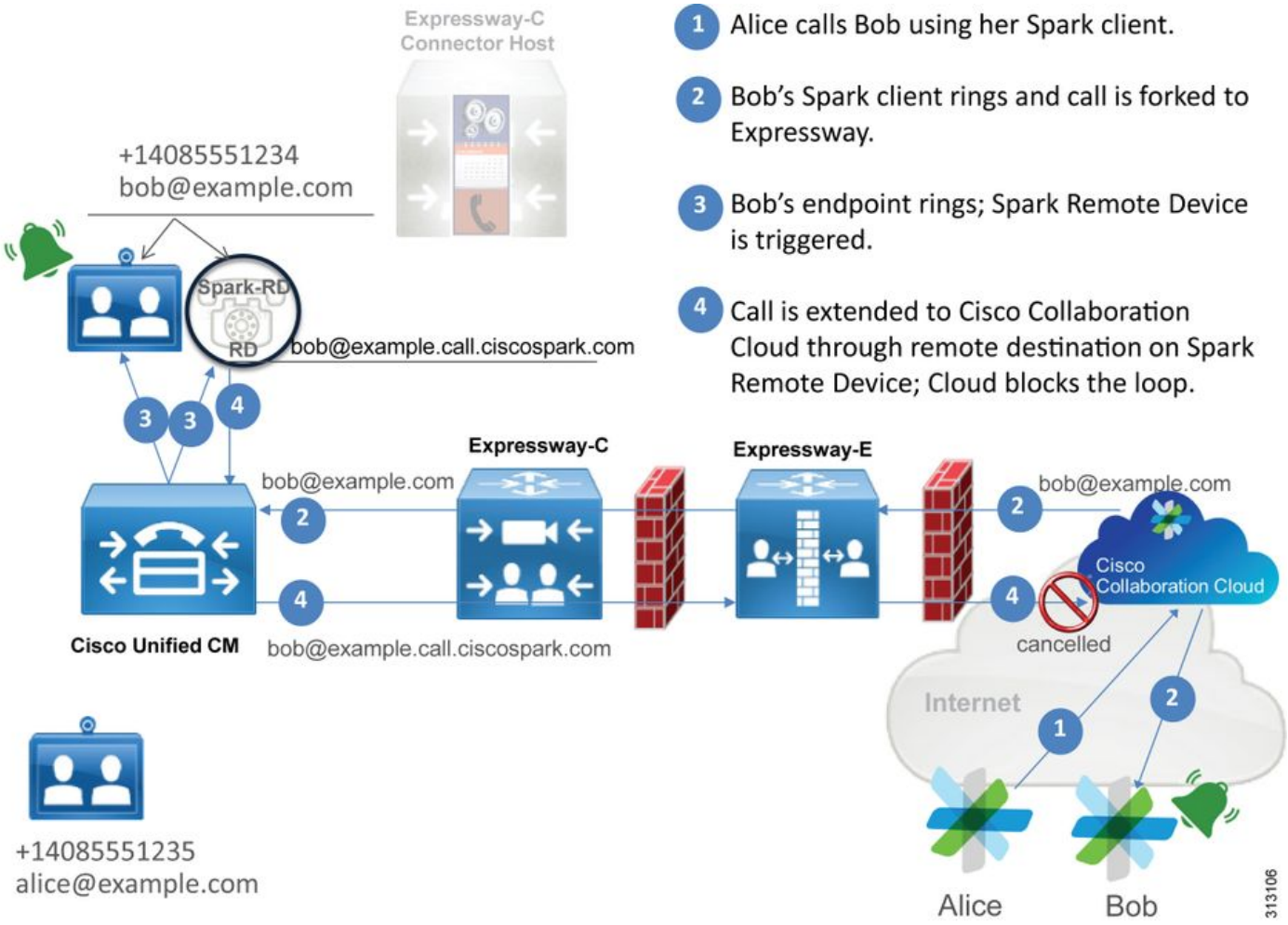
几乎所有从 Cisco Webex 到本地的入站故障都会导致相同的故障报告：“当我从 Cisco Webex 应用程序向另一个同事的应用程序发出呼叫时，同事的应用程序会振铃，但内部电话不会。” 为了解决此问题，您会发现了解呼叫流程以及在发出此类型呼叫时所使用的逻辑会很有帮助。

高级逻辑流

1. 主叫方的 Cisco Webex 应用程序发起呼叫
2. 被叫方的应用程序振铃
3. 呼叫被分配到 Cisco Webex 环境
4. Cisco Webex 环境必须根据 Cisco Webex Control Hub 中客户配置的 SIP 目的地执行 DNS 查询
5. Cisco Webex 环境尝试通过端口 5062 连接到 Expressway
6. Cisco Webex 环境尝试执行双向 TLS 握手
7. Cisco Webex 环境向 Expressway 发送 SIP INVITE 消息，此消息被向下传递到内部协作终端/IP 电话
8. Cisco Webex 和企业完成 SIP 协商
9. Cisco Webex 和企业开始发送和接收介质。

呼叫流

导航到 Cisco Webex 应用 > Cisco Webex 环境 > Expressway E > Expressway C > 内部协作终端/IP 电话（如图所示）。



以下是与从 Webex 到内部基础设施的入站呼叫相关的一些常见问题。

问题 1 Cisco Webex 无法解析 Expressway E DNS SRV/主机名

在思考从 Cisco Webex 到内部设施的呼叫流程时，按照逻辑，Cisco Webex 首先会思考如何联系内部 Expressway。如上文所述，Cisco Webex 将根据配置的 **SIP 目的地（在** Cisco Webex Control Hub 混合呼叫服务设置页面列出）通过执行 SRV 查询尝试连接到内部 Expressway。

如果您尝试从 Expressway E 诊断日志的角度对此情况进行故障排除，您不会看到任何来自 Cisco Webex 的流量。如果您尝试搜索 TCP 连接，您不会看到 Dst-port=5062，也不会看到任何后续 MTLS 握手或来自 Cisco Webex 的 SIP Invite。

在这种情况下，您必须检查 Cisco Webex Control Hub 中的 **SIP 目的地是如何配置的。**您还可以使用**混合连接测试工具协助排除故障。**该工具可检查是否存在有用的 DNS 地址，Cisco Webex 是否可以连接到 SRV 查询中返回的端口，以及内部 Expressway E 是否有 Cisco Webex 信任的有效证书。

1. 登录到 Cisco Webex Control Hub。
2. SelectServices
3. 在混合呼叫卡中选择 Settingslink。
4. 在呼叫服务连接部分验证 SIP 目的地字段中用于公共 SIP SRV 地址的域。
5. 如果已正确输入记录，请点击**测试，查看记录是否有效。**
6. 如下图所示，您可以清楚地看到公共域没有与其关联的 SIP SRV 记录。

选择**视图测试结果**，您可以看到故障的详细信息（如图所示）。

另一种方法是，您也可以使用nslookup查找SRV记录。以下是您可以运行的命令，以验证SIP目标是否存在。

```
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
```

您可以在上述代码块中看到，系统启动了 nslookup 命令，然后服务器被设置为 8.8.8.8，即公共的 Google DNS 服务器。最后，您将要查找的记录类型设置为 SRV 记录。此时，您可以发布您想要查找的完整 SRV 记录。最终结果是请求超时。

解决方案

1. 为用于托管公共域名的现场 Expressway E 配置公共 SIP SRV 地址。
2. 配置将解析为 Expressway E 的公共 IP 地址的主机名
3. 配置 SIP 目的地，以列出用于在第 1 步中创建的 SIP SRV 地址的域。 登录到 Cisco Webex Control Hub选择**服务**选择*混合呼叫卡中的***设置链接**在呼叫服务连接部分，在 **SIP 目的地字段输入**用于公共 SIP SRV 地址的域。 选择保存

   注意：如果您想要使用的 SIP SRV 记录已被用于企业到企业通信，我们建议在 Cisco Webex Control Hub 中指定企业域的一个子域作为 SIP 发现地址（如下所示）：

服务和协议：_sips._tcp.mtls.example.com
优先级：1
重量：10
端口号：5062
目标：us-expe1.example.com

可直接从《Cisco Webex 混合设计指南》中查找以上建议。

备选解决方案

如果客户没有（且未计划创建）SIP SRV 记录，它们也可以列出后缀为 ":5062" 的 Expressway 公共 IP 地址。 这样，Webex环境将不会尝试SRV查找，而是直接连接到 **%Expressway_Pub_IP%:5062。**(示例：64.102.241.236:5062）

1. 将SIP目标配置为**%Expressway_Pub_IP%:5062。** *（示例： 64.102.241.236:5062）* 登录到 Cisco Webex Control Hub选择**服务**选择*混合呼叫卡中的***设置链接**在呼叫服务连接部分，在 **SIP 目的地字段输入 %Expressway_Pub_IP%:5062。** 选择保存

有关必须设置的 SIP 目的地地址和/或 SRV 记录的详细信息。请参阅《 Cisco Webex 混合呼叫服务部署指南》或《Cisco Webex 混合设计指南 》中的《为您的组织启用混合呼叫服务》部分。

问题 2 套接字失败：端口 5062 阻止至 Expressway 的入站流量

在完成 DNS 解析后，Cisco Webex 环境会尝试通过端口 5062 建立到 DNS 查询中返回的 IP 地址的连接。此 IP 地址将成为内部 Expressway E 的公共 IP 地址。如果 Cisco Webex 环境无法建立此 TCP 连接，此前往内部设备的入站呼叫将会失败。在这种情况下，故障表现与其他所有 Cisco Webex 入站呼叫失败的表现都相同：内部电话不振铃。

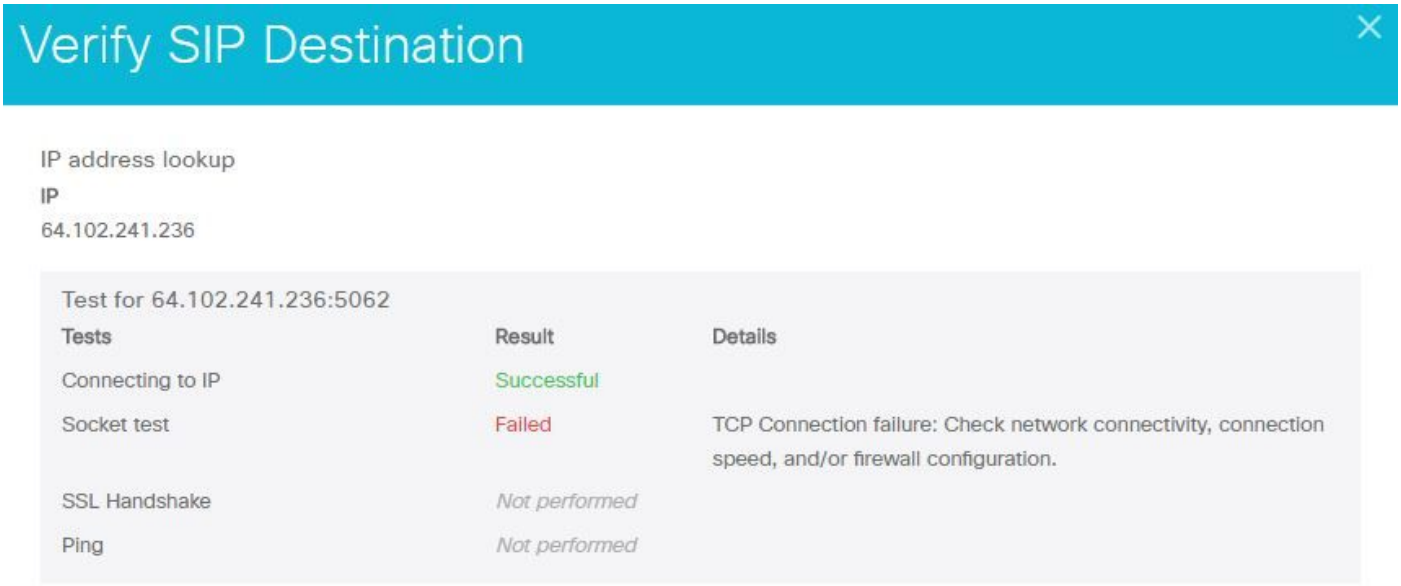
如果您正在使用 Expressway 诊断日志对此问题进行故障排除，您将不会看到来自 Cisco Webex 的任何流量。如果您尝试搜索 TCP 连接，您不会看到 Dst-port=5062 的任何连接尝试，也不会看到任何后续 MTLS 握手或来自 Cisco Webex 的 SIP Invite。由于在这种情况下，Expressway E 诊断日志记录无任何作用，您可以使用以下几种验证方法：

1. 从防火墙外部接口移除数据包捕获
2. 使用端口检查实用程序
3. 使用混合连接测试工具

由于混合连接测试工具内置在 Cisco Webex Control Hub 中，并模拟 Cisco Webex 环境尝试连接到内部 Expressway，因此它是最理想的验证方法。要测试到组织的 TCP 连接，请执行以下操作：

1. 登录到 Cisco Webex Control Hub。
2. SelectServices
3. 在混合呼叫卡中选择 Settingslink。
4. 在呼叫服务连接部分，确保 SIP 目的地中输入的值正确
5. 点击“测试”（如图所示）。

6.由于测试失败，您可以单击“查看测**试结果”**链接，以检查详细信息，如图所示。



如上图所示，在尝试连接到 64.102.241.236:5062 时套接字测试失败。除 Expressway 诊断日志 /pcap 外，此数据也未显示任何连接尝试，这足以说明您需要调查防火墙 ACL/NAT/路由配置。

解决方案

由于此问题不是由 Cisco Webex 环境或内部协作设备导致的，因此您需要关注防火墙配置。由于您不一定能够预测您将会应对的防火墙类型，您需要向熟悉此设备的人寻求帮助。此问题可能与防火墙 ACL、NAT 或路由配置错误有关。

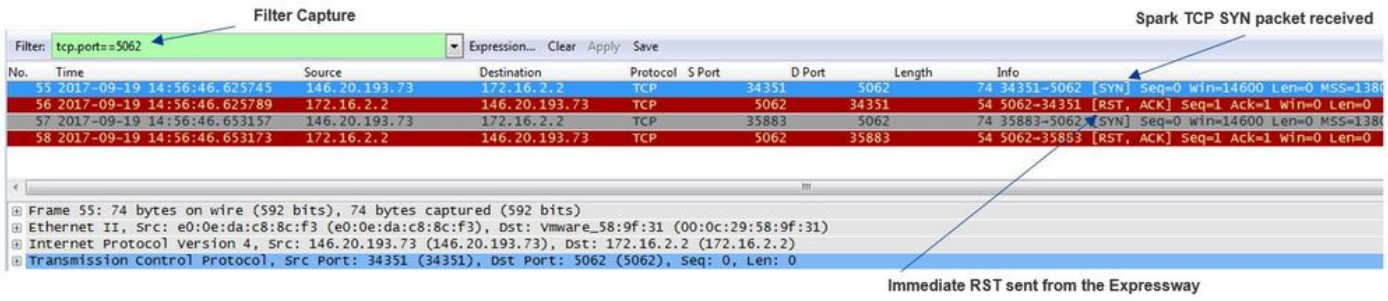
问题 3 套接字失败：Expressway E 未侦听端口 5062

此问题通常会被错误地诊断。很多时候，会假设防火墙是导致端口 5062 上的流量被阻止的原因。要解决此问题，您可以使用上文“端口 5062 上到 Expressway 的入站流量被阻止”场景中的技巧。您会发现用于检查端口连接的混合连接测试工具及任何其他工具将会出现故障。首先会假设防火墙阻止了流量。大多数人然后会重新检查 Expressway E 的诊断日志记录，以确定是否可以看到尝试建立的 TCP 连接。他们会查找与下图所示日志行项目类似的日志行项目。

```
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"
```

在这种情况下，上述日志条目不存在。因此，许多人会错误地诊断此问题，并假设原因在于防火墙。

如果诊断日志记录中包含数据包捕获，您便可以确定原因不在防火墙。以下为 Expressway E 未侦听端口 5062 的场景下的数据包捕获示例。使用 tcp.port==5062 作为过滤器对此捕获进行过滤（如图所示）。



在从 Expressway E 获取的数据包捕获中可以看到，防火墙未阻止通过 TCP 端口 5062 的流量，未被防火墙阻止，但事实上此流量并未到达。在编号为 56 的数据包中，您可以看到，初始 TCP SYN 数据包到达后 Expressway E 立即发送了 RST。根据此信息，您可以得出以下结论：问题存在于 Expressway E 接收数据包的过程中；您必须从 Expressway E 的角度来进行故障排除。鉴于此，请思考 Expressway E RST 数据包的可能原因。导致此行为的两种可能原因为：

1. Expressway-E设置了某些类型的防火墙规则，这些规则可能会阻止流量

2. Expressway-E未侦听相互TLS流量和/或未侦听端口5062上的流量。

Expressway E 防火墙功能在*系统 > 保护 > 防火墙规则 > 配置*中。在此环境中勾选这一项时，则不存在防火墙配置。

有多种方法可以用于验证 Expressway 是否侦听通过端口 5062 的双向 TLS 流量。您可以通过 Web 界面或 CLI 以根用户的身份执行此操作。

从 Expressway 根中，如果您发出 **netstat-an | grep ':5062' ，您应**该得到一些类似于下面所示的输出。

```
~ # 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      0 127.0.0.1:5062          0.0.0.0:*               LISTEN
tcp        0      0 ::1:5062                :::*                    LISTEN
```

也可通过 Expressway E Web 界面来获得此信息。请参阅以下步骤来收集此信息

1.登录Expressway-E

2.导航至“**维护工具”>“端口使用”>“本地入站端口”**

3.搜索类型SIP和IP端口5062。（如图所示，以红色突出显示）

既然您知道您会看到哪些内容，您便可以将其与当前环境进行比较。从 CLI 角度看，当您运行 **netstat-an | grep ':5062',**输出如下所示：

```
~ # netstat -an | grep ':5062'
tcp        0      0 127.0.0.1:5062          0.0.0.0:*               LISTEN
tcp        0      0 ::1:5062                :::*                    LISTEN
~ #
```

此外，Web UU 不会显示在本地入站端口上侦听的双向 TLS 端口

Local inbound ports

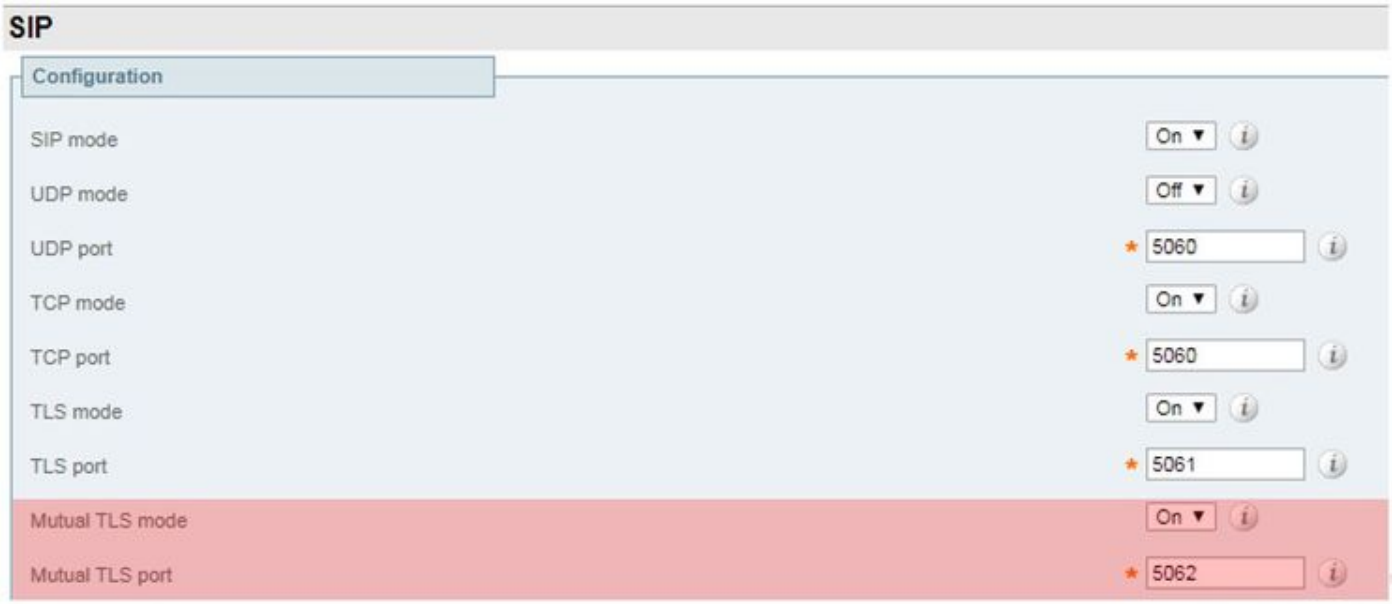
Type	Description	Protocol	IP address	IP port	Transport
H.323	Call signaling port range	H.323	192.168.1.6	15000-19999	TCP
H.323	Call signaling port range	H.323	172.16.2.2	15000-19999	TCP
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP
SIP	TCP port	SIP	192.168.1.6	5060	TCP
SIP	TCP port	SIP	172.16.2.2	5060	TCP
SIP	TLS port	SIP	192.168.1.6	5061	TCP
SIP	TLS port	SIP	172.16.2.2	5061	TCP

根据此数据，您可以得出以下结论：Expressway E 不侦听双向 TLS 流量。

解决方案

要解决此问题，您必须确保双向 TLS 模式已启用且 Expressway E 上的双向 TLS 端口设置为 5062：

1. 登录到 Expressway E
2. 导航到**配置 > 协议 > SIP**
3. 确保双向 TLS 模式设置为**开**
4. 确保双向 TLS 端口设置为 **5062**
5. 点击**保存**（如图所示）。



问题 4 Expressway E 或 Expressway C 不支持预加载 SIP 路由报头

使用混合呼叫服务连接时，将根据**路由报头**完成呼叫路由。会根据此解决方案 Call Service Aware（Expressway 连接器）部分提供给 Cisco Webex 的信息填充路由报头。Expressway 连接器主机在 Unified CM 查询启用了呼叫服务的用户并拉出他们的**目录 URI 和 Unified CM 主集群的集群 FQDN**。请参阅以下示例（以 Alice 和 Bob 之间的呼叫为例）：

目录 URI	**目标路由报头**
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

如果 Alice 或 Bob 进行呼叫，呼叫被路由到其内部 Unified CM，以便可以在将呼叫路由到被叫用户之前，将其固定到他们的思科 WebexRD。

如果 Alice 呼叫 Bob，呼叫将路由到 *Alice 的 Unified CM 主集群 FQDN (us-cucm.example.com)*。如果您分析一下 Cisco Webex 向 Expressway E 发送的入站 SIP INVITE，您会在 SIP 标头中找到以下信息

请求 URI SIP：bob@example.com
路由报头 sip:us-cucm.example.com;lr

从Expressway的角度来看，搜索规则配置为路由呼叫，而不是由请求URI**，而是由路由报头(us-cucm.example.com)** — 在此例中为Alice的Unified CM主集群。

有了此基础设置，您可以对故障排除情况有更好的了解，在此情况下，Expressway 配置错误，这导致以上逻辑无法正常工作。由于几乎所有其他入站混合呼叫服务连接的呼叫设置都失败了，故障表现为*内部电话不振铃*。

在分析 Expressway 上的诊断日志之前，请思考如何识别此呼叫：

1. SIP 请求 URI 为被叫方的**目录 URI**。
2. SIP FROM字段的格式将为“**主叫方**”列**为“名字姓氏”<sip:WebexDisplayName@subdomain.call.ciscospark.com>**

有了此信息，您可以根据**被叫方目录 URI、主叫方第一个和最后一个名称或主叫方的 Cisco Webex SIP 地址**搜索诊断日志。如果您没有任何此信息，可以搜索“INVITE SIP:**”，该**搜索查找在Expressway上运行的所有SIP呼叫。一旦您识别了入站呼叫的 SIP INVITE，您便可以找到并复制 SIP 呼叫 ID。获得此值后，您只需根据呼叫 ID 搜索诊断日志，以便查看与此呼叫分支相关联的所有消息。

为了帮助隔离路由问题，另一件需要做的事是确定呼叫进入企业的路由路径有多长。您可以尝试在 Expressway C 上搜索上文所述信息，以查看呼叫的路由路径是否有那么长。如果是，您将有可能想要就此进行调查。

在此场景中，您可以看到，Expressway C 收到了 Expressway E 发送的 INVITE。

```
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-ip="192.168.1.5" Local-port="26847"
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;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-
id=a82052ef-6fd7-4506-8173-e73af6655b5d;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8ad97fff3c240124;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;egress-
zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769
6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstojano test"



        ;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
```

Route:

Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-e73af6655b5d@192.168.1.6:7003;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-e73af6655b5d@192.168.1.6:5061;transport=tls;lr>

重要的一点是，路由报头（集群 FQDN）仍然保持不变。但是，没有根据路由报头（群集 FQDN）cucm.rtp.ciscotac.net 执行任何搜索逻辑。相反，您将看到消息立即被拒绝，提示 **404 未找到**错误。

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="**Call Attempted**" Service="SIP" Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" **Src-alias="sip:pstojano-test@dmzlab.call.ciscospark.com"** Dst-alias-type="SIP" **Dst-alias="sip:jorobb@rtp.ciscotac.net"** Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Protocol="TLS" Auth="NO" Level="1" UTCTime="2017-09-19 18:16:15,832"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="**Search Attempted**" Service="SIP" Src-alias-type="SIP" **Src-alias="pstojano-test@dmzlab.call.ciscospark.com**" Dst-alias-type="SIP" **Dst-alias="sip:jorobb@rtp.ciscotac.net"** Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="searchtype:INVITE" Level="1" UTCTime="2017-09-19 18:16:15,834"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="**Search Completed**" **Reason="Not Found"** Service="SIP" Src-alias-type="SIP" **Src-alias="pstojano-test@dmzlab.call.ciscospark.com"** Dst-alias-type="SIP" **Dst-alias="sip:jorobb@rtp.ciscotac.net"** Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" **Detail="found:false**, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-19 18:16:15,835"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="**Call Rejected**" Service="SIP" Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" **Src-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net"** Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" **Detail="Not Found"** Protocol="TLS" **Response-code="404"** Level="1" UTCTime="2017-09-19 18:16:15,835"
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="INFO": Action="Received" Local-ip="192.168.1.5" Local-port="26847" Src-ip="192.168.1.6" Src-port="7003" Detail="Receive Request Method=INVITE, CSeq=1, **Request-URI=sip:jorobb@rtp.ciscotac.net**, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-Tag=872524918, To-Tag=, Msg-Hash=11449260850208794722, Local-SessionID=daf7c278732bb5a557fb57925dffcbf7, Remote-SessionID=00000000000000000000000000000000"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,836" Module="network.sip" Level="INFO": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-ip="192.168.1.6" Dst-port="7003" Detail="**Sending Response Code=404**, Method=INVITE, CSeq=1, **To=sip:jorobb@rtp.ciscotac.net**, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-Tag=872524918, To-Tag=96b9a0eaf669a590, Msg-Hash=254718822158415175, Local-SessionID=00000000000000000000000000000000, Remote-SessionID=daf7c278732bb5a557fb57925dffcbf7"

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,836" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-ip="192.168.1.6" Dst-port="7003" Msg-Hash="254718822158415175"
SIPMSG:
|**SIP/2.0 404 Not Found**
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-id=a82052ef-6fd7-4506-8173-e73af6655b5d;received=192.168.1.6;rport=7003;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8ad97fff3c240124;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;egress-zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769

6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: **9062bca7eca2afe71b4a225048ed5101**@127.0.0.1
CSeq: 1 INVITE
From: **"pstojano test"**

;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>;tag=96b9a0eaf669a590
Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.5:5061 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=daf7c278732bb5a557fb57925dffcbf7
Content-Length: 0

与工作场景比较，您会发现，在正常工作场景中，会根据路由报头（集群 FQDN）执行搜索逻辑

2017-09-22T13:56:02.215-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="**Search Attempted**" Service="SIP"
Src-alias-type="SIP" **Src-alias="pstojano-test@dmzlab.call.ciscospark.com"** Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf" Tag="8bd936da-f2ab-4412-96df-d64558f7597b" Detail="searchtype:INVITE" Level="1"
UTCTime="2017-09-22 17:56:02,215"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,217"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<routed> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<location clear="yes" url="sip:cucm.rtp.ciscotac.net;lr" diversion="" dest-url-for-
message="sip:jorobb@rtp.ciscotac.net" sip-route-set="" dest-service=""> added
sip:cucm.rtp.ciscotac.net;lr to location set "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<proxy stop-on-busy="no" timeout="0"/> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound MS to CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'multiway' did not match destination
alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'WebEx Search Rule' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'ISDN Inbound' ignored due to source
filtering"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'recalls into CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'CEtcp-rtp12-tpdmz-118-ucmpub' did
not match destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Conference Factory' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"

```
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound B2B Calling' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Cisco Webex' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'as is local' towards
target 'LocalZone' at priority '1' with alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.219-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Hybrid Call Service
Inbound Routing' towards target 'CUCM11' at priority '2' with alias 'cucm.rtp.ciscotac.net;lr'"
```

然后，您会看到 Expressway C 将呼叫正确转发到了 Unified CM (192.168.1.21)。

```
2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-
ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TCP 192.168.1.5:5060;egress-
zone=CUCM11;branch=z9hG4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b
5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-
id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;ingress-
zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-
service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbed5b79c6cffad9ecd84cc8
337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005
Via: SIP/2.0/TLS
192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbeff9819;received=148.62.40.64;rport=36
149;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-
8c648a16c2c5d7b85fa5c759d59aa190;rport=47732
Call-ID: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstojano test" <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=567490631
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 14
Route:
```

```
Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf@192.168.1.5:5060;transport=tcp;lr>
Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-
e2d2bb6fec77@192.168.1.6:7003;transport=tls;lr>
Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-
e2d2bb6fec77@192.168.1.6:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
```

分析完诊断日志记录，将问题隔离到 Expressway C 和特定错误（404 未找到）后，您便可以专注于分析导致此行为的原因了。需要考虑以下事项：

1. 呼叫会按照搜索规则进入和离开 Expressway 上的区域。

2. Expressway 使用被称为预加载 SIP 路由支持的逻辑，来处理包含路由器报头的 SIP INVITE 请求。可在 Expressway C 和 Expressway E 上的各区域（遍历服务器、遍历客户端和邻居）中开启或关闭此值。

您现在可以使用 xConfiguration 查看 Expressway E 遍历服务器和 Expressway C 客户端区域的配置，尤其是为混合呼叫服务连接设置的配置。除了区域配置外，您还可以分析为了将呼叫从一个区域传递到另一个区域而配置的搜索规则。您还知道 Expressway E 确实将呼叫传递给 Expressway C 了，因此此处的遍历服务器区域配置很可能设置正确。

从以下 xConfig 我们可以了解到，此区域的名称为**混合呼叫服务遍历**，这属于 **TraversalServer 区域类型。**它通过 SIP TCP 端口 **7003** 与 Expressway C 通信。

混合呼叫服务的关键之处在于，它必须开启预加载 SIP 路由支持。在 Expressway Web 界面，此值为**预加载 SIP 路由支持，而在 xConfiguration 中，其显示为 SIP PreloadedSipRoutes 接受**

```
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"
*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: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On"
*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 TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Type: "TraversalServer"
```

您还可以确定，此区域已绑定到搜索规则 3（Webex 混合）。实质上，搜索规则发送了经由混合呼叫服务 DNS 区域的“Any”别名，并将其传递到上述区域，即混合呼叫服务遍历。不出所料，Expressway E 上的搜索规则和遍历服务器区域均配置正确。

```
*c xConfiguration Zones Policy SearchRules Rule 3 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Description: "Calls to VCS-C"
*c xConfiguration Zones Policy SearchRules Rule 3 Mode: "AnyAlias"
*c xConfiguration Zones Policy SearchRules Rule 3 Name: "Webex Hybrid"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Behavior: "Strip"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern String:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Type: "Prefix"
*c xConfiguration Zones Policy SearchRules Rule 3 Priority: "15"
*c xConfiguration Zones Policy SearchRules Rule 3 Progress: "Stop"
```

```
*c xConfiguration Zones Policy SearchRules Rule 3 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 3 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 3 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 3 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 3 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Type: "Zone"
```

如果您关注 Expressway C 的 xConfiguration，您可以首先查找 Webex 混合的遍历客户端区域。一种简单的查找方法是，搜索您从 Expressway E xConfiguration 获知的端口号（**SIP 端口："7003"**）。 这能帮助您快速确定 xConfiguration 中的正确区域。

和以前一样，您可以了解区域名称（混合呼叫服务遍历）、类型（遍历客户端），以及为 SIP PreloadedSipRoutes 接受（预加载 SIP 路由支持）部署的配置。 从此 xConfiguration 您可看到，此值设置为“关”。根据《Cisco Webex 混合呼叫服务部署指南》，此值应为设置为“开”。

此外，根据预加载 SIP 路由支持的定义，如果此值设置为“关”，且 INVITE 包含以下路由报头，则 Expressway C 应该拒绝消息：“**如果您希望此区域拒绝包含此报头的 SIP INVITE 请求，交换机预加载 SIP 路由支持将关闭。**”

```
Expressway-C
*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/1lYDd76O/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"
```

此时，您已经将问题归结于 Expressway C 的遍历客户端区域配置错误。您必须将预加载 SIP 路由支持切换到“开”。

解决方案

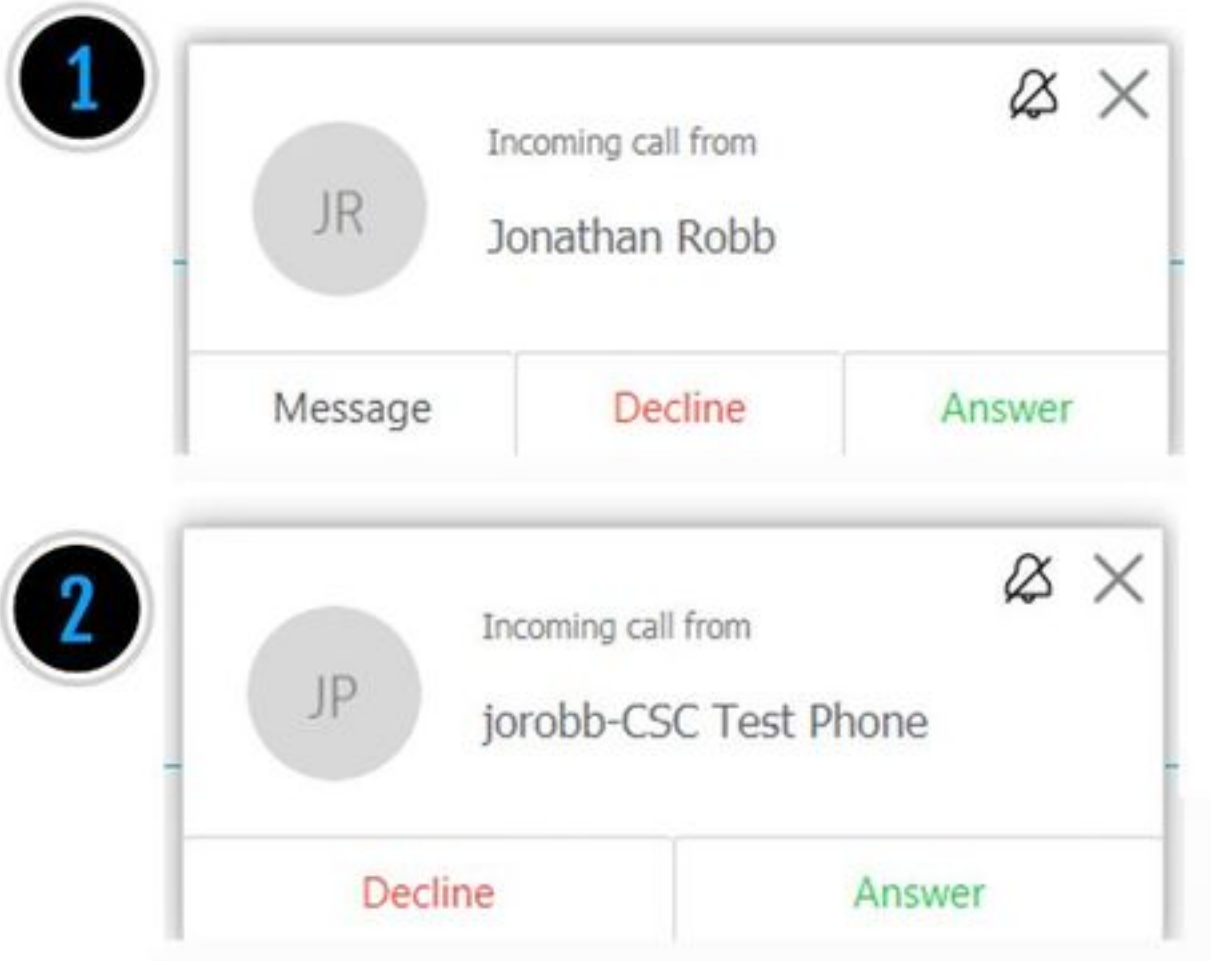
要正确设置预加载 SIP 路由支持，请执行以下操作：

1. 登录到 Expressway C
2. 导航到**配置 > 区域 > 区域**
3. 选择混合呼叫服务遍历客户端区域（各个客户采用的命名可能不同）
4. 将**预加载 SIP 路由支持**设置为**开**
5. 选择**保存**

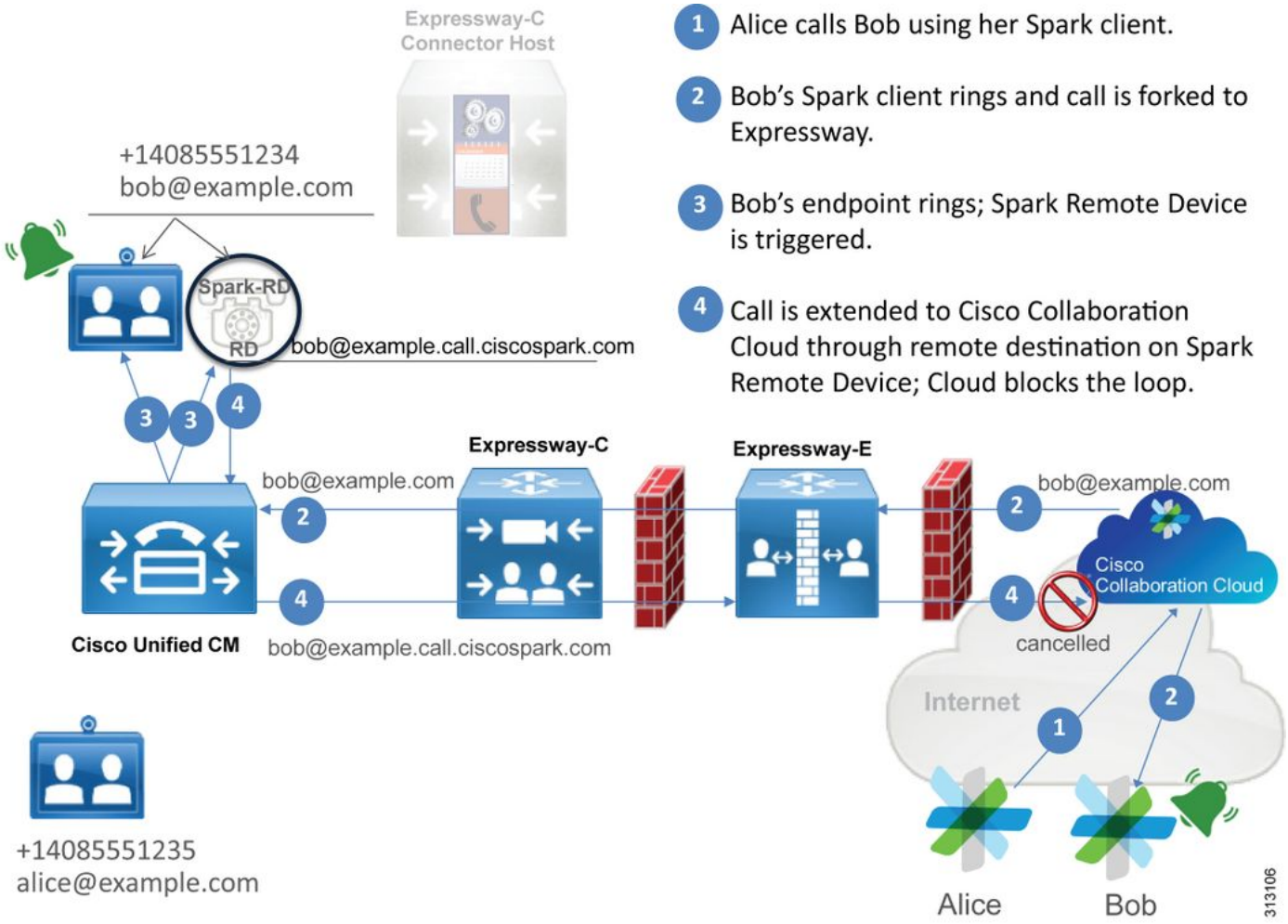
注意：尽管此场景显示 Expressway C 出现了故障，但如果 Webex 混合呼叫遍历服务器区域的**预加载 SIP 路由支持设置为"关"，也可能会在 Expressway E 上看到相同的诊断日志记录错误。**在这种情况下，您将永远不会看到呼叫到达 Expressway C，且 Expressway E 将一直拒绝该呼叫并发送 404 未找到错误消息。

问题 5 Cisco Webex 应用程序接收两个呼叫通知 (toasts)

此问题是唯一不会导致丢弃呼叫的入站呼叫场景。出现此问题时，收到呼叫的人（被叫方）会在 Cisco Webex 应用程序中收到发起呼叫（主叫方）发出的两个通知 (toasts)。 第一个通知从 Cisco Webex 生成，第二个通知来自内部基础设施。以下是两个通知的示例（如图所示）。



第一个通知 (toast) 由发起呼叫的人（主叫方）从 Cisco Webex 端发出。在这种情况下，主叫 ID 是发起呼叫的用户的显示名称。第二个通知 (toast) 来自内部 CTI 或分配给发起呼叫的用户的 Cisco Webex RD。起初，此行为看上去十分异常。但是，如果您查看（《Cisco Webex 混合呼叫设计指南》中的）入站呼叫图，您便知道此行为其实时合理的（如图所示）。



您可以从图中看到，Alice 正在从自己的 Cisco Webex 应用程序呼叫 Bob，且呼叫被分配到了内部设备。此呼叫应与分配给 Bob 的电话的目录 URI 相匹配。问题是，在此设计中，此目录 URI 也分配给了他的 CTI RD 或 Cisco Webex RD。因此，当呼叫被发送到 CTI RD 或 Cisco Webex RD 时，呼叫会返回到 Cisco Webex，因为设备具为 bob@example.call.ciscospark.com 配置了远程目的地。Cisco Webex 处理这种情况的方法是，取消特定呼叫分支。

要正确取消呼叫分支，Cisco Webex 首先需要将在 SIP 报头中添加一个参数，以便它可以通过搜索此参数来取消给定的分支。在 Cisco Webex 的 SIP INVITE 中插入的参数被称为“**call-type=squared”，并且此值还被输入到联系人报头中。**如果从消息中删除了此值，Cisco Webex 将不知道如何取消呼叫。

有了此信息，您可以回顾一下我们在之前讨论过的场景，即当 Cisco Webex 用户 Jonathan Robb 发起呼叫时，用户的 Cisco Webex 应用程序收到两个通知 (toasts)。要对此类问题进行故障排除，您将始终需要从 Expressway C 和 Expressway E 收集诊断日志记录。首先，您可以查看 Expressway E 日志，以确定事实上 SIP INVITE 在发出的初始出站 Cisco Webex INVITE 中提供了 **call-type=squared 值。**这将确保防火墙不会以任何方式篡改消息。以下为此场景中 Expressway E 入站 INVITE 的代码片段示例。

```
2017-09-19T14:01:48.140-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,140"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="172.16.2.2" Local-port="5062"
Src-ip="146.20.193.73" Src-port="40342" Msg-Hash="11658696457333185909"
 SIPMSG:
 |INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
 Via: SIP/2.0/TLS 192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71,SIP/2.0/TLS
127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
 Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
 CSeq: 1 INVITE
```

```
 Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>;call-type=squared
<-- Webex inserted value
 From: "Jonathan Robb"



        ;tag=540300020
 To:
```

联系人报头中存在 **call-type=squared 值。**此时，呼叫必须通过 Expressway 和并离开 Webex 混合遍历服务器区域。我们可以搜索 Expressway E 日志，以确定从 Expressway E 发出呼叫的方式。我们可据此了解 Expressway E 是否以任何方式篡改了 INVITE。

```
2017-09-19T14:01:48.468-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,468"
Module="network.sip" Level="DEBUG":  Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="26686" Msg-Hash="1847271284712495612"
SIPMSG:
INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKec916b02b6d469abad0a30b93753f4b0859;proxy-call-
id=d7372034-85d1-41f8-af84-dffed6d1a9a9;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKd91699370129b4c10d09e269525de00c2;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;egress-
zone=DefaultZone;branch=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdfe078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debcd8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=4
0342;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>     <-- Webex inserted value is now missing
From: "Jonathan Robb"



        ;tag=540300020
To:



Max-Forwards: 15
Route: <sip:cucm.rtp.ciscotac.net;lr>
```

在查看从 Expressway E 发送到 Expressway C 的 SIP INVITE 时，请注意，联系人报头缺少 **call-type=squared**。另一个需要指出的注意事项是，在行项目 4 中，您可以看到 egress-zone 等于 **HybridCallServiceTraversal**。现在，您可以得出以下结论：拨号时，Cisco Webex 应用程序会收到二个通知 (toast) 的原因是 Expressway E 从 SIP INVITE 联系人报头中删除了 **call-type=squared 标记。**要回答的问题是，导致此行为的可能原因。

呼叫必须通过您在 Expressway 设置的混合呼叫服务遍历，因此调查可以从此处开始。如果您有 xConfiguration，您可以看到此区域的配置方式。要在 xConfiguration 中识别区域，您只需使用 Via 行中记录的名称（印在日志中）即可。如前文所述，此名称为 egress-zone=HybridCallServiceTraversal。当名称被印到 SIP 报头的 Via 行时，空格将被删除。从 xConfiguration 角度来看，实际的区域名称将包含空格，并会在混合呼叫服务遍历被格式化。

```
*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 Port: "7003"
*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 TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

识别了混合呼叫服务遍历设置后，您可以查找突出的潜在设置，例如：

- SIP PreloadedSIPRoutes 接受：开启
- SIP ParameterPreservatoin 模式：关闭

使用任何 Expressway 的 Web 界面，您可以看到这些值的定义以及用途。

预加载 SIP 路由支持

将预加载 SIP 路由支持调为“开”，以启用此区域来处理包含路由报头的 SIP INVITE 请求。

“如果您希望此区域拒绝包含此报头的 SIP INVITE 请求，请将预加载 SIP 路由支持设置为“关”。

SIP 参数保留

确定 Expressway 的 B2BUA 是否在通过此区域的 SIP 请求中保留或重写了这些参数。

Onpreserves 在此区域与 B2BUA 之间路由的 SIP 请求 URI 和请求的联系人参数。
Offallows B2BUA 重写在此区域与 B2BUA 之间路由的 SIP 请求 URI 和请求的联系人参数（如有必要）。
根据这些定义、xConfiguration 以及 SIP INVITE“联系人”报头中存在 **call-type=squared 值这一信息，您可以判断，将混合呼叫服务遍历区域中的 SIP 参数保留值设置为“关”是导致标记被删除以及**

Cisco Webex 应用程序收到两个通知的原因。

解决方案

要在 SIP INVITE 联系人报头中保留 call-type=squared 值，您必须确保为处理呼叫过程中涉及的所有区域保留 Expressway 支持 SIP 参数：

1. 登录到 Expressway E
2. 导航到**配置 > 区域 > 区域**
3. 选择用于混合遍历服务器的区域
4. 将 SIP 参数保留值设置为**开**
5. 保存设置。

##########

注意：在此示例场景中，是 Expressway E上的 Webex 混合遍历服务器区域配置错误。请记住，Webex 混合遍历客户端或 CUCM 相邻区域上的 SIP 参数保留值完全有可能被设置为“关” 。这两种配置都将在Expressway-C上完成。如果是这种情况，您可以预期Expressway-E会向Expressway-C发送 **call-type=squared** 值，而Expressway-C会将其剥离。

出站：从本地到 Cisco Webex

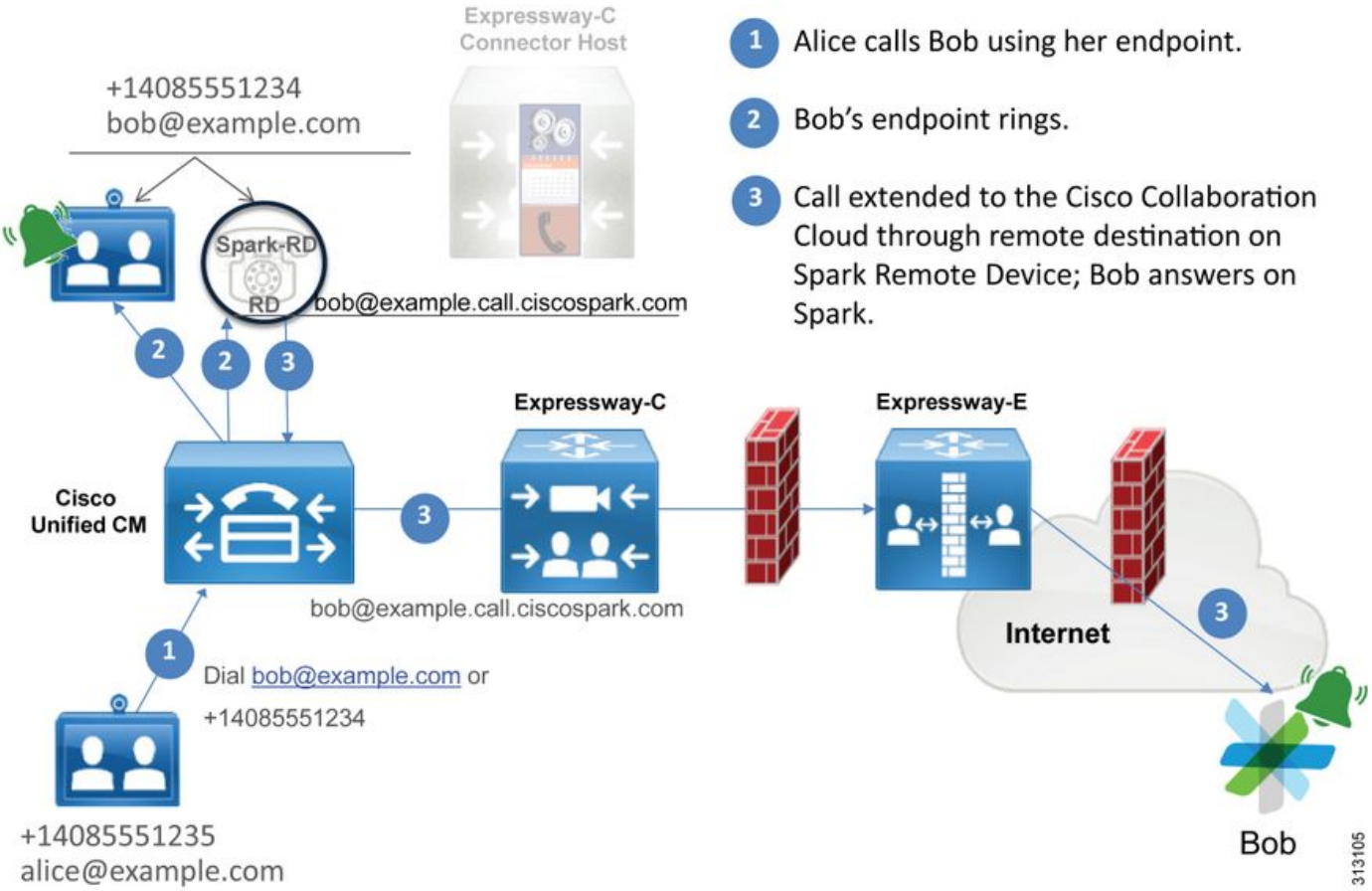
几乎所有从内部设备到 Cisco Webex 的出站呼叫故障都有相同的故障表现：“当我从 Unified CM 注册电话呼叫另一个启用了呼叫服务连接的用户时，其内部电话振铃但其 Cisco Webex 应用程序不振铃。” 对此场景进行故障排除时，您需要了解呼叫流程以及在发出此类型呼叫时所使用的逻辑。

高级逻辑流

1. 用户 A 从内部电话向用户 B 的目录 URI 发起呼叫
2. 用户 B 的内部电话和 CTI RD/Webex RD 收到呼叫
3. 用户 B 的内部电话开始振铃
4. 用户 B 的 CTI-RD/Webex-RD 将呼叫分配到 UserB@example.call.ciscospark.com 的目的地
5. Unified CM 将呼叫传递到 Expressway C
6. Expressway C 将呼叫发送至 Expressway E
7. Expressway-E在callservice.ciscospark.com域上执行DNS查找
8. Expressway E 尝试通过端口 5062 连接到 Cisco Webex 环境。
9. Expressway E 和 Cisco Webex 环境开始双向握手
10. Cisco Webex 环境将呼叫传递给用户 B 的可用 Cisco Webex 应用程序
11. 用户 B 的可用 Cisco Webex 应用程序开始振铃。

呼叫流

导航到**用户 B 内部电话 > Unified CM > CTI RD/Webex RD > Expressway C > Expressway E > Cisco Webex 环境 > Cisco Webex 应用程序**（如图所示）。



注意：图像取自《Cisco Webex 混合设计指南》。

日志分析技巧

如果您对分叉到 Cisco Webex 的出站呼叫出现故障的场景进行故障排除，您会想要收集 Unified CM、Expressway C 和 Expressway E 日志。通过这些日志集，您可以看到呼叫通过环境的方式。另一种了解呼叫进入内部环境的距离是使用 Expressway"搜索历史记录"。 借助 Expressway 搜索历史记录，您可以快速了解经过分叉处理到 Cisco Webex 的呼叫是达到了 Expressway C 或 Expressway E。

要使用搜索历史记录，可以执行以下操作：

1. 登录到 Expressway E
   拨打测试电话
   导航到**状态 > 搜索历史记录**
   验证您是否看到呼叫中包含 Webex SIP URI 目的地地址 (user@example.call.ciscospark.com)
   如果历史记录中未显示 Expressway E 搜索历史记录中的呼叫，请在 Expressway C 上重复此过程

在分析 Expressway 上的诊断日志之前，请思考如何识别此呼叫：

1. SIP 请求 URI 地址将为 Cisco Webex 用户的 SIP 地址
2. SIP FROM字段将格式化为将主叫方列为"名字姓氏"<sip:Alias@Domain>

有了此信息，您可以根据主叫方目录 URI、主叫方第一个和最后一个名称或被叫方的 Cisco Webex SIP 地址搜索诊断日志。如果您没有任何此信息，可以对"INVITE SIP："执行搜索，该搜索将查找在Expressway上运行的所有SIP呼叫。一旦您识别了出站呼叫的 SIP INVITE，您便可以找到并复制 SIP**呼叫 ID**。获得此值后，您只需根据呼叫 ID 搜索诊断日志，以便查看与此呼叫分支相关联的所有消息。

以下是从 Unified CM 注册电话到 Cisco Webex 环境的出站呼叫（向启用了呼叫服务连接用户拨打的呼叫）的一些常见问题。

问题1. Expressway无法解析callservice.ciscospark.com地址

Expressway DNS 区域标准操作程序是根据请求 URI 右侧出现的域执行 DNS 查找。请参照以下示例了解原因。如果DNS区域要接收请求URI为**pstojano-test@dmzlab.call.ciscospark.com**的呼叫，则典型的Expressway DNS区域将在请求URI的右侧**dmzlab.call.ciscospark.com**上执行DNS SRV查找逻辑。如果 Expressway 要执行此操作，则预计会发生以下查找和响应。

```
_sips._tcp.dmzlab.call.ciscospark.com.
Response: 5 10 5061 l2sip-cfa-01.wbx2.com.
l2sip-cfa-01.wbx2.com
Response: 146.20.193.64
```

如果仔细看，您会发现 SRV 记录响应提供服务器地址和端口 5061，而非端口 5062。

这表示，端口 5062 上的双向 TLS 握手将不会发生，并会有一个单独的端口用于在 Expressway 和 Cisco Webex 之间传递信令。此处的难点是，*《Cisco Webex 混合呼叫服务部署指南》*未明确呼吁使用端口 5061，因为某些环境不允许企业到企业呼叫。

标准 DNS 区域 SRV 查找逻辑过去的工作方式是，配置 Expressway，使其根据您提供的值执行显式搜索。

在分析此呼叫时，您可以将重点放在 Expressway E 上，因为您确定（使用搜索历史记录）该呼叫最终到达了此处。从进入 Expressway E 的第一个 SIP INVITE 开始，看看它进入哪个区域，使用什么搜索规则，呼叫从哪个区域转出以及是否正确发送到 DNS 区域，以及发生了什么 DNS 查询逻辑。

```
2017-09-19T13:18:50.562-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,556"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26686" Msg-Hash="4341754241544006348"
 SIPMSG:
 |INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK6d734eaf7a6d733bd1e79705b7445ebb46175.1d33be65c99c
56898f85df813f1db3a7;proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf;rport
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK13187594dd412;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: 991f7e80-9c11517a-130ac-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"
<sip: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"
        ;tag=332677~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106860
 To:
```

```
 Max-Forwards: 15
 Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5061;transport=tls;lr>
 Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@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: Tue, 19 Sep 2017 17:18:50 GMT
 Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
 Session-Expires: 1800
 Min-SE: 1800
 Allow-Events: presence
 X-TAATag: 2272025a-ce36-49d0-8d93-cb6a5e90ffe0
 Session-ID: 75957d4fb66a13e835c10737aa332675;remote=00000000000000000000000000000000
 Cisco-Guid: 2568978048-0000065536-0000000148-0352430272
 Content-Type: application/sdp
 Content-Length: 714

<SDP Omitted>
```

在此SIP INVITE中，您可以收集请求URI(pstojano-test@dmzlab.call.ciscospark.com)、**呼叫ID**(991f7e80-9c11517a-130ac-1501a8c0)、**From**("Jonathan Robb" <sip:5010@rtp.ciscotac.net>)、 **to** (sip:pstojano-test@dmzlab.call.ciscospark.com)和**User-Agent** (Cisco-CUCM11.5)。 收到此 INVITE 后，Expressway 必须进行逻辑决策，以确定它是否可以将呼叫路由到另一个区域。Expressway 将执行此基于搜索规则。

```
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG":  Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG":  Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG":  Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG":  Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-
test@dmzlab.call.ciscospark.com'"
```

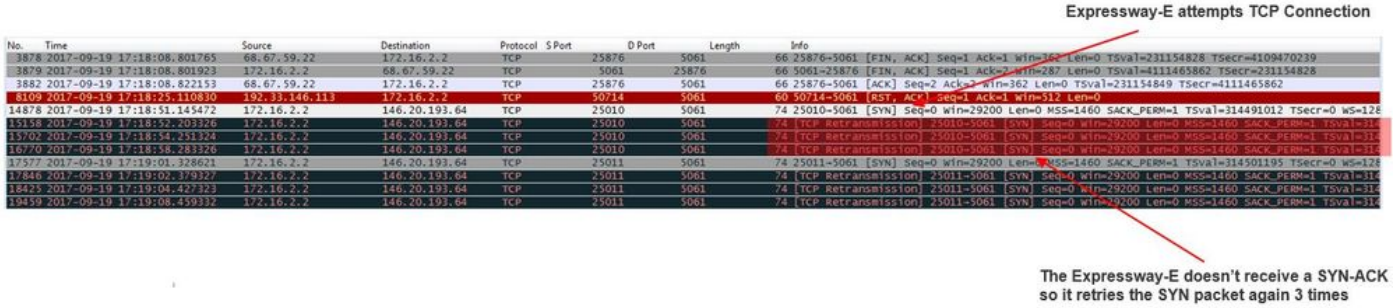
根据上述日志片段，您可以看到，Expressway E 解析了四个搜索规则，但是却只考虑了其中一个规则*（*Webex 混合 - 到 Webex Cloud *）*。搜索规则的优先级为 90，目标是转至混合呼叫服务 DNS 区域。现在，该呼叫被发送到 DNS 区域，您可以查看 Expressway E 上发生的 DNS SRV 查找

```
2017-09-19T13:18:50.565-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,565"
Module="network.dns" Level="DEBUG":  Detail="Sending DNS query"
Name="dmzlab.call.ciscospark.com" Type="NAPTR (IPv4 and IPv6)"
2017-09-19T13:18:50.718-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,718"
Module="network.dns" Level="DEBUG":  Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T13:18:50.795-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,795"
Module="network.dns" Level="DEBUG":  Detail="Resolved hostname to:
['IPv4''TCP''146.20.193.64:5061'] (A/AAAA)  Hostname:'l2sip-cfa-01.wbx2.com' Port:'5061'
Priority:'5' TTL:'300' Weight:'10' (SRV) Number of relevant records retrieved: 2"
```

在上面的代码段中，您可以看到Expressway E根据请求URI(_sips._tcp.dmzlab.call.ciscospark.com)的右侧执行了SRV查找，并且已解析为l2sip-cfa-01.wbx2.com和端口5061的主机名。主机名l2sip-cfa-01.wbx2.com解析为146.20.193.64。使用此信息，Expressway将采取的下一个逻辑步骤是向146.20.193.64发送TCP SYN数据包，以便尝试设置呼叫。从 Expressway E 日志记录中，您可查看是否出现了这种情况。

```
2017-09-19T13:18:51.145-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:51,145"
Module="network.tcp" Level="DEBUG":  Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64"
Dst-port="5061" Detail="TCP Connecting"
2017-09-19T13:19:01.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:19:01,289"
Module="network.tcp" Level="ERROR":  Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64"
Dst-port="5061" Detail="TCP Connection Failed"
```

在上述 Expressway E 诊断日志记录片段中，您可以看到 Expressway E 正在尝试连接到之前在 TCP 端口 5061 上解析的 IP 146.20.193.64，但连接失败。从收集的数据包捕获中，也能看到相同的现象。



从这些结果可以看出，端口 5061 上的流量显然未成功。但是，混合呼叫服务连接会使用 TCP 端口 5062，而非端口 5061。因此，您需要思考为何 Expressway E 不解析返回端口 5062 的 SRV 记录。要回答该问题，您可以检查 Expressway E Webex 混合 DNS 区域是否存在配置问题。

```
*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: "ciscospark.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.ciscospark.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"
```

在 Expressway-E xConfiguration 中，您可以看到有两个特定值与 DNS 查询相关联：**DNSOverride 名称 和 DNSOverride 覆盖**。由于 xConfiguration DNSOverride 覆盖设置为关，因此 DNSOverride 名称将不会生效。要更好地了解这些值执行什么操作，您可以使用 Expressway Web UI 查找值的定义。

修改 DNS 请求 *(在 xConfig 中转换到* DnsOverride 覆盖 *)*

从此区域发出的出站 SIP 呼叫路由到手动指定的 SIP 域，而非拨号目的地中的域。此选项主要用于 Cisco Webex 呼叫服务。请参阅 www.cisco.com/go/hybrid-services。

要搜索的域（在 xConfig 中转换为 DnsOverride 名称）

输入要在 DNS 中查找的 FQDN，而非搜索出站 SIP URI 上的域。原始 SIP URI 不会受到影响。

了解这些定义后，您便会明白这些值（如果设置正确）与我们的 DNS 查找逻辑完全相关。如果将这与《Cisco Webex混合呼叫服务部署指南》中的语句相结合，您会发现“修改DNS请求”必须设置为**On**，而要搜索的域应设置为**callservice.ciscospark.com**。如果您更改这些值，以指定正确信息，则 DNS SRV 查找逻辑将会完全不同。以下是您可以从 Expressway E 诊断日志记录角度看到的代码片段

```
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.ciscospark.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"
```

解决方案

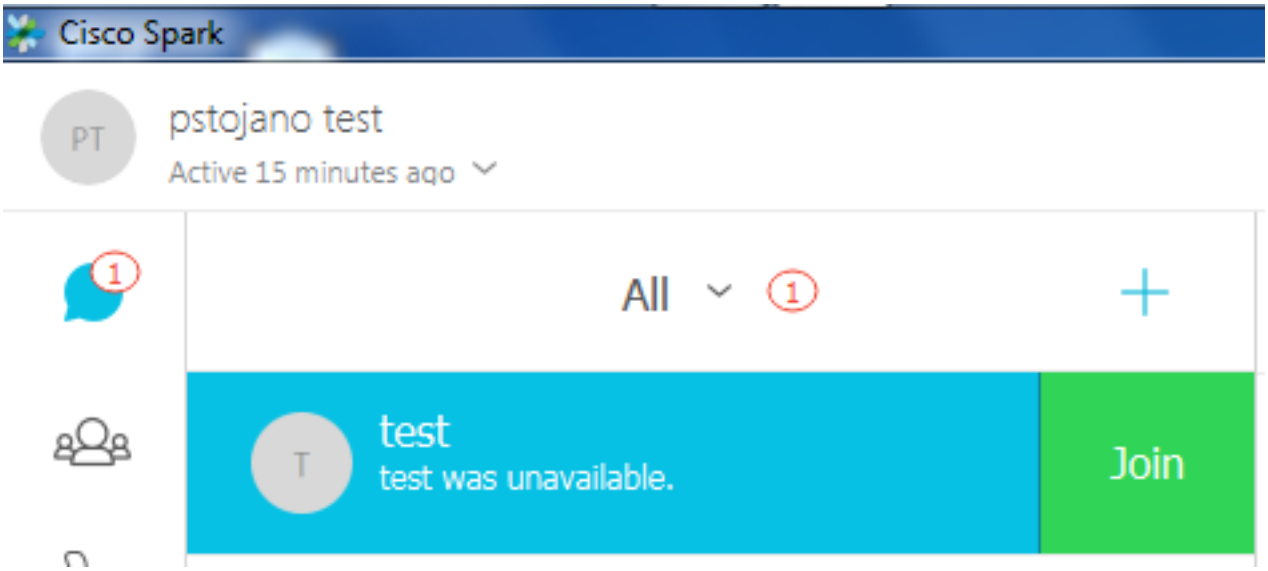
1. 登录到 Expressway E
2. 导航到**配置区域 > 区域**
3. 选择已配置的 Webex 混合 DNS 区域
4. 将“修改 DNS 请求”设置为**开**
5. 将域设置为callservice.ciscospark.com**以搜索值**
6. 保存更改

> **注意**：如果 Expressway 上只使用一个 DNS 区域，应配置一个单独的 DNS 区域，用于可以利用这些值的混合呼叫服务。

问题 2 端口 5062 阻止到 Cisco Webex 的出站流量

Cisco Webex 分叉呼叫失败的独特之处在于，尽管客户端不会振铃，但被叫方的 Cisco Webex 应用程序会显示“加入”按钮。如上述场景类似，您需要再次使用相同的工具和日志记录来准确地定位发生故障的地方。有关隔离呼叫问题和分析日志的技巧，请参阅本文相关部分（如图所示）。

显示“加入”按钮的图示



与出站呼叫问题 #1 类似，您可以首先分析 Expressway E 诊断日志记录，因为您已通过 Expressway 上的搜索历史记录确定呼叫最终到达了 Expressway E。与以前一样，从从Expressway-C进入Expressway-E的初始INVITE开始。请记住，您要查找的内容包括：

1. Expressway-E 是否收到 INVITE
2. 搜索规则逻辑是否将呼叫传递到混合 DNS 区域
3. DNS 区域是否在正确的域上执行 DNS 查找
4. 系统是否在端口 5062 上尝试并正确建立 TCP 握手
5. 双向 TLS 握手是否成功

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,017"
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="3732376649380137405"
 SIPMSG:
 |INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcddfd62f6ff7e09f9939482.899441b6d60c
444e4ed58951d07b5224;proxy-call-id=696f6f1c-9abe-47f3-96a4-e26f649fb76f;rport
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12d4b77c97a64;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: 6a48de80-9c11273a-12d08-1501a8c0@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"
<sip: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"



        ;tag=328867~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106829
 To:



 Max-Forwards: 15
 Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5061;transport=tls;lr>
```

```
 Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@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: Tue, 19 Sep 2017 14:18:34 GMT
 Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
 Session-Expires: 1800
 Min-SE: 1800
 Allow-Events: presence
 X-TAATag: b2967a3b-93fb-4ca4-b0d7-131f75335684
 Session-ID: 75957d4fb66a13e835c10737aa328865;remote=00000000000000000000000000000000
 Cisco-Guid: 1783160448-0000065536-0000000126-0352430272
 Content-Type: application/sdp
 Content-Length: 714
<SDP Omitted>
```

从上述 INVITE 中您可看到，INVITE 接收正常。此为“已接收”操作，且来自 Expressway C 的 IP 地址。您现在可以移至搜索规则逻辑

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG":  Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG":  Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG":  Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG":  Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-
test@dmzlab.call.ciscospark.com'"
```

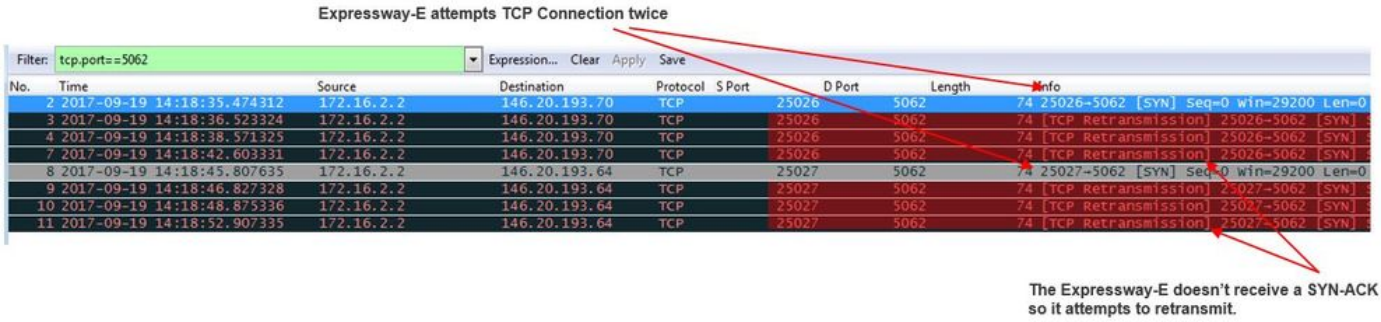
根据上述日志片段，您可以看到Expressway-E通过四个搜索规则进行解析，但只解析了一个*（Webex混合 — 到Webex云）*已考虑。搜索规则的优先级为90，目标是访问 *混合呼叫服务DNS区域*。现在，该呼叫被发送到 DNS 区域，您可以查看 Expressway E 上发生的 DNS SRV 查找所有这些都完全正常。现在您可以重点分析 DNS 查找逻辑

```
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.ciscospark.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"
```

您可以清楚地看到，在本例中，callservice.ciscospark.com SRV记录已解析。响应了四个不同的有效记录，它们都使用端口 5062。这是正常现象。此时，您可以分析下一个 TCP 握手。如前文所述，您可以在诊断日志中搜索“TCP 连接”，并查找列出 Dst-port="5062" 的目的地端口。 以下为您将在此场景中看到的内容的示例：

```
2017-09-19T10:18:35.474-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,474"
Module="network.tcp" Level="DEBUG":  Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connecting"
2017-09-19T10:28:35.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:28:35,289"
Module="network.tcp" Level="ERROR":  Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connection Failed"
```

您还可以使用诊断日志记录捆绑包中包含的 tcpdump 获取有关 TCP 握手的更多详细信息（如图所示）。



此时，您就可以判定 Expressway E 正确路由了呼叫。在此场景的难点在于，不能与 Webex 环境建立 TCP 连接。如果 Webex 环境未响应 TCP SYN 数据包，则可能会出现这种情况，然而，我们不太可能想到处理此连接的服务器在许多客户之间共享。在此场景中，更可能的原因是某些类型的中间设备（防火墙、IPS 等）不允许流量发出。

解决方案

由于这是一个隔离的问题，因此数据应提供给客户的网络管理员。此外，如果他们需要详细信息，您可以边缘设备和/或防火墙的外部接口上移除捕获，以获取更多证据。从 Expressway 角度来看，不需要执行进一步的操作，因为此问题并不在设备上。

问题 3 Expressway 搜索规则配置错误

搜索规则配置错误是 Expressway 上与配置相关的重大问题。搜索规则配置问题可能是双向的，因为入站呼叫和出站呼叫都需要使用搜索规则。当分析此问题时，您会发现，尽管 regex 问题在 Expressway 上相当常见，但它们并不一定总会导致搜索规则问题。在此特定部分，您将会分析失败的出站呼叫。像所有其他分叉出站呼叫场景一样，故障表现是相同的：

- 被叫用户的 Cisco Webex 应用程序显示“加入”按钮
- 主叫电话播放振铃
- 被叫用户的内部话机振铃
- 被叫用户的 Cisco Webex 应用程序不振铃

像所有其他情况一样，您还需要利用 CUCM SDL 跟踪以及 Expressway C 和 Expressway E 诊断日志。与以前一样，您应该参考搜索历史记录使用及在诊断日志中识别呼叫的技巧。与以前一样，根据 Expressway E 搜索历史记录可以确定该呼叫到达了 Expressway E 且失败了。以下是分析的起始阶段，在此阶段，我们查看了 Expressway C 向 Expressway E 发送的初始 SIP INVITE。

```
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.ciscospark.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"
```

```
<sip: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"



        tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972
 To:



 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@192.168.1.5:5060;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 15:26:02 GMT
 Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
 Session-Expires: 1800
 Min-SE: 1800
 Allow-Events: presence
 X-TAATag: 8e8c014d-5d01-4581-8108-5cb096778fc5
 Session-ID: 75957d4fb66a13e835c10737aa505813;remote=00000000000000000000000000000000
 Cisco-Guid: 3582928512-0000065536-0000000240-0352430272
 Content-Type: application/sdp
 Content-Length: 714

<SDP Omitted>
```

使用SIP报头中的呼叫ID(**d58f2680-9c91200a-1c7ba-1501a8c0**)，您可以快速搜索与此对话框关联的所有消息。在查看日志中命中的第三个呼叫 ID 时，您可以看到 Expressway E 立即向 Expressway C 发送了 **404 未找到错误。**

```
2017-09-25T11:26:13.286-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:13,286"
Module="network.sip" Level="DEBUG":  Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="25675" Msg-Hash="12372154521012287279"
 SIPMSG:
 |SIP/2.0 404 Not Found
 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;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal
 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
 From: "Jonathan Robb"



        ;tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972
 To:
```

```
        Server: TANDBERG/4135 (X8.10.2) Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa505813 Content-
Length: 0
```

此数据可告诉您以下两点：

1. Expressway E 从未尝试向 Cisco Webex 发送 INVITE
2. Expressway E 是制定逻辑决策拒绝呼叫（404 未找到错误）的一方。

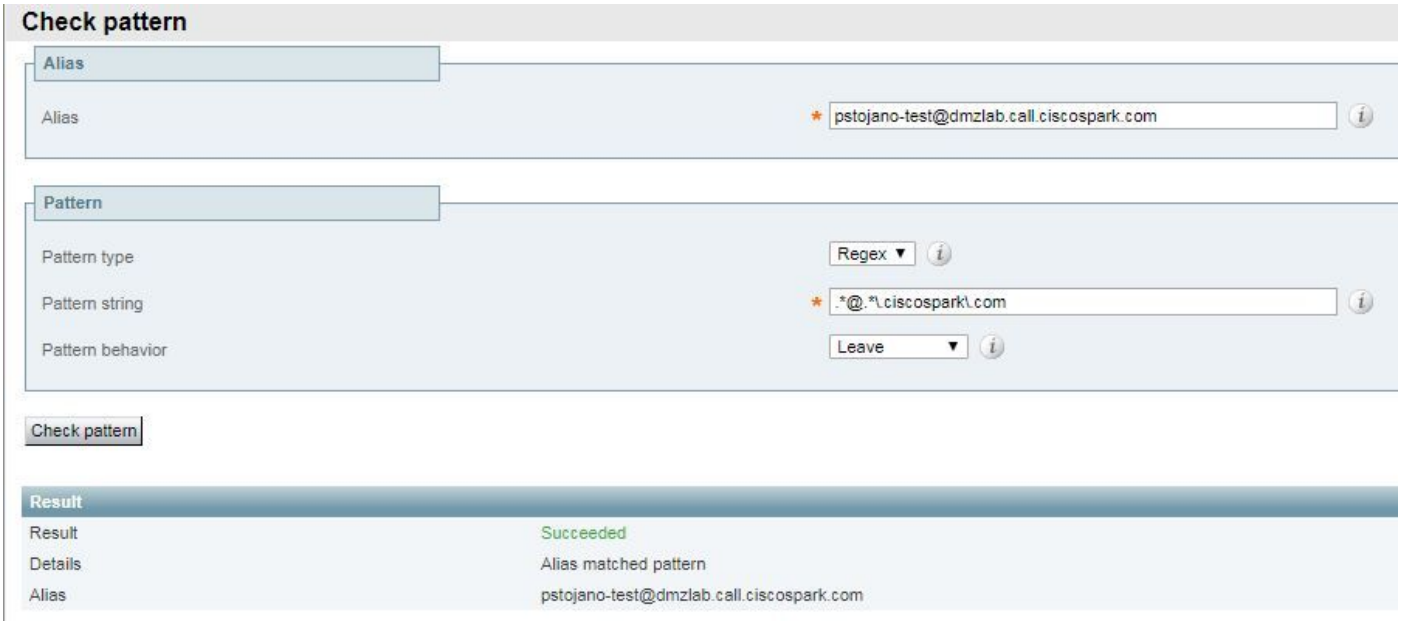
404 未找到错误通常表示 Expressway 无法找到目的地址。由于 Expressway E 使用搜索规则在其自身和其他不同环境之间路由呼叫，您可首先重点分析 Expressway E 的 xConfiguration。您可以在此 xConfiguration 中查找将呼叫传递给 Webex 混合 DNS 区域的搜索规则。要从 xConfiguration 角度查找 Expressway 上配置的搜索规则，您可以搜索“xConfiguration Zones Policy SearchRules Rule”。执行此操作后，您将看到 Expressway 上每个搜索规则的搜索规则配置列表。在“规则”后出现的数量将根据最初创建的标记为1的搜索规则增加。如果您在查找搜索规则时遇到困难。您可以使用常用命名值（例如“*Webex*”）来查找搜索规则。识别规则的另一种方法是查找设置为“.*@.*\.ciscospark\.com”的模式字符串值。 这就是应配置的模式字符串。 *（假设模式字符串配置正确）*在检查 xConfiguration 后，您可以看到，搜索规则 6 是用于将呼叫传递到 Cisco Webex 的正确规则。

```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern String: ".*@.*\.ciscospark\.com"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Type: "Regex"
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 6 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 6 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 6 Source Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 6 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 6 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 6 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Type: "Zone"
```

要测试此模式，我们可以使用中所述的检查模式功能。此处需要声明的是，我们需要配置以下值：维护 > 工具 > 检查模式

- 别名：%Request URI in the initial INVITE%（例如：pstojano-test@dmzlab.call.ciscospark.com)
- 模式类型：Regex
- 模式字符串。*@.*\.ciscospark\.com
- 模式行为：离开

如果规则的 Regex 设置正确，您应该会看到检查模式成功的结果，如下图所示：



在确认搜索规则存在且配置正确后，您可以查看 Expressway 在确定发送 404 未找到错误的 Expressway E 是否受到影响时执行的逻辑。以下是 Expressway 执行的搜索规则逻辑示例。

```
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG":  Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG":  Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG":  Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-25T11:26:02.967-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,967"
Module="network.search" Level="DEBUG":  Detail="Considering search rule 'to DNS' towards target
'DNS' at priority '100' with alias 'pstojano-test@dmzlab.call.ciscospark.com'"

2017-09-25T11:26:02.968-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,968"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="dmzlab.call.ciscospark.com"
Type="NAPTR (IPv4 and IPv6)"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Could not resolve hostname"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"
```

在本示例中，您可以看到 Expressway 处理了四个搜索规则。前三个规则因各种原因而被忽略，第四条规则得到考虑。值得关注的数据片是，在考虑第四条规则后 Expressway 立即直接跳转至 DNS 查询逻辑。回顾我们在 xConfiguration 中看到的内容，为 Webex 混合配置的搜索规则的名称是“Webex Hybrid - to Webex Cloud”，且在上述搜索规则逻辑根本没有考虑此规则。此时，您需要查看被考虑的搜索规则（到 DNS）是如何执行的，以便您可以更好地了解它是否影响了 Webex 混合搜索规则的使用。为此，您可以重新查看 xConfig，这一次查找名为“DNS”的搜索规则

```
*c xConfiguration Zones Policy SearchRules Rule 1 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Description:
*c xConfiguration Zones Policy SearchRules Rule 1 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "(?!.*@%localdomains%.*$).*"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: "Regex"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 1 Protocol: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Mode: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Name: "Please Select"
```

```
*c xConfiguration Zones Policy SearchRules Rule 1 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 1 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Name: "DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Type: "Zone"
```

在检查搜索规则后，您可以得出以下结论：

- 模式字符串与 Cisco Webex 请求 URI 相匹配
- 优先级被设置为 100
- 进度 (Pattern behavior) 被设置为“停止”。

此信息告诉我们，被叫 Cisco Webex 请求 URI 与此规则相匹配，并且如果匹配规则，Expressway 会停止搜索（考虑）其他搜索规则。因此，规则优先级是一个关键因素。Expressway 搜索规则优先级的工作原理是首先尝试优先级最低的规则。以下是示例。搜索规则：本地模式行为：继续第 1 优先级搜索规则：邻居模式行为：继续第 10 优先级搜索规则：DNS模式行为：停止第 50 优先级在本示例中，首先尝试名为“Local”(1) 的搜索规则，如果发现匹配的搜索规则，则会移到名为“Neighbor”的搜索规则 (10)，因为模式行为被设置为“继续”。如果搜索规则“Neighbor”不匹配，则会继续查找搜索规则“DNS” (50)，且就此止步。如果搜索规则“DNS”匹配，则会停止搜索，无论是否存在优先级高于 50 的搜索规则，因为模式行为被设置为停止。 因此，您可以查看“to DNS”和“Webex Hybrid - to Webex Cloud”规则之间的搜索规则优先级。

```
*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"
```

在此，您可以看到“到DNS”规则的优先级低于“到Webex混合 — 到Webex云”规则，因此，将首先尝试“到DNS”规则。由于模式行为（进度）设置为“停止”，因此 Expressway E 绝不会考虑 Webex Hybrid - to Webex Cloud 规则，并且呼叫最终会失败。 解决方案此类问题在混合呼叫服务连接中越来越常见。很多时候，人们在部署解决方案后，会创建一个高优先级规则用于 Cisco Webex 搜索。然而，由于存在优先级更低的匹配规则，此规则很少被调用，并最终导致呼叫失败。Cisco Webex 的入站呼叫和出站呼叫都会发生此问题。要解决此问题，您需要执行以下步骤：

1. 登录到 Expressway E
2. 导航到配置 > 拨号方案 > 搜索规则
3. 查找 Webex 混合搜索规则并点击 *（例如：名称：Webex Hybrid - to Webex Cloud ）*
4. 将优先级值设为低于其他搜索规则，但又足够高，从而不会影响其他人。 *（例如：优先级：99 ）*

搜索规则的惯例是，模式字符串越具体，它在搜索规则优先级列表中位置则越低。通常，DNS 区域配置了模式字符串，用于捕获任何非本地域的数据并将其发送到互联网。因此，我们建议将此类搜索规则设置为高优先级，以便在最后调用它。 问题 4 Expressway CPL 配置错误Expressway 解决方案允许通过使用服务器上可用的呼叫处理语言 (CPL) 逻辑来规避收费欺诈。如果正在部署的 Expressway 解决方案仅用于 Cisco Webex 混合呼叫服务和移动和远程访问，我们强烈建议启用并执行 CPL 策略和规则。尽管 Expressway 上面向 Cisco Webex Hybrid 的 CPL 配置相当直观，如果配置错误，它可以轻松阻止呼叫尝试。以下场景展示了如何使用诊断日志记录找到 CPL 错误配置。像所有其他分叉出站呼叫场景一样，故障表现是相同的：

- 被叫用户的 Cisco Webex 应用程序显示“加入”按钮
- 主叫电话播放振铃
- 被叫用户的内部话机振铃
- 被叫用户的应用程序不振铃

像所有其他情况一样，您可以利用 CUCM SDL 跟踪以及 Expressway C 和 Expressway E 诊断日志。与以前一样，您应参考 用于使用搜索历史记录和诊断日志中识别呼叫的提示。与以前一样，根据 Expressway E 搜索历史记录可以确定该呼叫到达了 Expressway E 且失败了。以下是分析的起始阶段，在此阶段，您可查看 Expressway C 向 Expressway E 发送的初始 SIP INVITE。

```
2017-09-25T16:54:43.722-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,722"
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.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec868343687394302832 56.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;rport
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: c030f100-9c916d13-1cdcb-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"
<sip: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"




         ;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000
 To:




 Max-Forwards: 15
 Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5061;transport=tls;lr>
 Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@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-TAATag: 4fffefed-0512-4067-ac8c-35828f0a1150
 Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
 Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
 Content-Type: application/sdp
 Content-Length: 714

<SDP Omitted>
```

使用 SIP 报头中的呼叫 ID (c030f100 9c916d13 1cdcb 1501a8c0)，您可以快速向下搜索与此对话框关联的所有消息。在查看日志中命中的第三个呼叫 ID 时，您可以看到 Expressway E 立即向 Expressway C 发送了403 Forbidden 错误。

```
2017-09-25T16:54:43.727-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,727"
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="91954361011101346 22"
 SIPMSG:
 |SIP/2.0 403 Forbidden
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec868343687394302832 56.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac;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"




        ;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000
To:




        ;tag=64fe7f9eab37029d
Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa512577
Content-Length: 0
```

要了解Expressway E拒绝此呼叫并向Expressway C发送403禁止错误的原因，您需要分析403禁止和输入Expressway的原始SIP INVITE之间的日志条目。通过分析这些日志条目，您通常可以看到正在做出的所有逻辑决策。请注意，您看不到被调用的搜索规则，但能看到调用了呼叫处理语言 (CPL) 逻辑。以下是代码段。

```
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:




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:




2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"
Module="network.cpl" Level="DEBUG":  Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:




2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:



          "
```

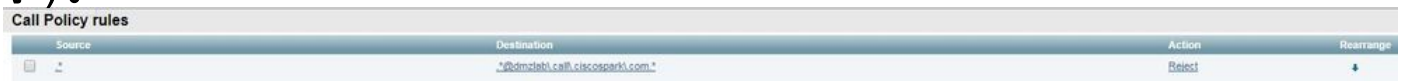
根据上述日志分析，您可以确定 CPL 拒绝了该呼叫。

```
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.ciscospark.com" Call-serial-
number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4fffefed-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"
```

*注意：在此情况下，您不会看到调用的搜索规则，因为 CPL、FindMe 和 Transform 都是在调用搜索规则之前处理的*在大多数情况下，您可以利用 Expressway 的 xConfig 来更好地了解具体情况。但是，对于 CPL，除非启用了策略，否则您不会看到定义的规则。以下 xConfig 部分表明 Expressway E 使用了本地 CPL 逻辑。

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

为了更好地了解规则配置，您需要登录到 Expressway E 并导航至配置 > 呼叫策略 > 规则（如图所示）。



在查看此配置时，您可以看到以下配置：来源：.*目标:.*@dmzlab\.call\.ciscospark\.com.*操作：拒绝您可以发现，与*《Cisco Webex 混合呼叫服务部署指南》*中的介绍相比，源和目标都向后配置。

Field	Setting
Source Type	**From address**
Rule applies to	**Unauthenticated callers**
Source pattern	**.*@example\.call\.ciscospark\.com.***, where **example** is your company's subdomain.
Destination pattern	**.***
Action	**Reject**

解决方案要解决此问题，您需要重新调整CPL规则配置，以便将源设置为。*@%Webex_subdomain%\.call\.ciscospark\.com。*且目标模式为。*

1. 登录到 Expressway E
2. 导航到配置 > 呼叫策略 > 规则
3. 选择为 Cisco Webex 混合呼叫服务设置的规则
4. 输入源模式为。*@%Webex_subdomain%\.call\.ciscospark\.com。*(例如：.*@dmzlab\.call\.ciscospark\.com.*)
5. 输入目标模式。*
6. 选择保存

有关 Webex Hybrid CPL 实施的详细信息，请参阅《Cisco Webex 混合设计指南》。 双向：从 Cisco Webex 到本地或从本地到 Cisco Webex 问题 1 IP 电话/协作端点提供 G.711、G.722 或 AAC-LD 以外的音频编解码器。混合呼叫服务连接支持三种不同的音频编解码器：G.711、G.722 和 AAC-LD。要成功建立与 Cisco Webex 环境呼叫，必须使用这些音频编解码器之一。本地环境可以设置为使用多种类型的音频编解码器，但同时也可以设置为限制它们。通过在Unified CM上使用自定义和/或默认区域设置，这可能会有意或无意地发生。对于此特定行为，记录模式可能会因呼叫的方向以及Unified CM是否配置为使用 Early Offer 或 Delayed Offer 而有所不同。以下是这种行为可能出现的几种不同情况的例子：

1. Cisco Webex 发送提供 G.711、G.722或 AAC-LD 的入站 INVITE w/ SDP。Expressway-C 将发送此消息到 Unified CM，但 Unified CM 配置为仅允许G.729 进行此呼叫。因此，由于没有可用的编解码器，Unified CM 将拒绝该呼叫。
2. Unified CM 的会尝试作为呼出电话 *Early Offer 加入 Cisco Webex，这意味着初始 INVITE 发送到 Expressway-C 将包含仅支持 G.729 音频的 SDP*。然后，Cisco Webex会发送200 OK w/SDP，该SDP将从音频(*m=audio 0 RTP/SAVP*)中零，因为它不支持G.729。一旦Expressway-C将此INVITE传递到Unified CM，Unified CM将终止呼叫，因为没有可用的编解码器。
3. Unified CM 的会尝试将出战呼叫作为Cisco Webex 的 *Delayed Offer，这意味着初始 INVITE 发送到 Expressway-C 将不包含 SDP*。Cisco Webex 然后发送一个包含其支持的所有音频编解码器的 200 OK w/ SDP。Expressway-C 将该 200 OK 发送到 Unified CM，但Unified CM 仅被配置为只允许G.729进行该呼叫。因此，由于没有可用的编解码器，Unified CM 将拒绝该呼叫。

如果您尝试识别与此问题匹配的混合呼叫服务连接呼叫失败，除了Unified CM SDL跟踪外，您还必须获取Expressway日志。下面的示例日志片段与Unified CM尝试将出站呼叫作为Early Offer进行的

#2情况相符。因为我们知道呼叫到达 Cisco Webex，所以日志分析从 Expressway-E 开始以下是Cisco Webex初始INVITE out的代码段。您可以看到首选音频编解码器设置为 G.729（有效负载 18）。 101 用于双音多频，对于此特殊场景不相关。

```
2017-09-19T10:46:10.488-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:10,488"
Module="network.sip" Level="DEBUG":  Action="Sent" Local-ip="172.16.2.2" Local-port="25034" Dst-
ip="146.20.193.64" Dst-port="5062" Msg-Hash="4309505007645007056"
SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aedea256d2;rport
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=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
CSeq: 101 INVITE
Remote-Party-ID: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;privacy=off;screen=no;party=calling
Contact: <sip:172.16.2.2:5073;transport=tls>;video;audio
From: "Jonathan Robb"




Max-Forwards: 14
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aedea256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aedea256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
Supported: X-cisco-srtp-fallback,replaces,timer
Session-Expires: 1800;refresher=uac
Min-SE: 500
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000
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
t=0 0
m=audio 52668 RTP/SAVP 18 101  <-- CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
```

```
UNENCRYPTED_SRTCP
a=sendrecv
a=rtcp:52669 IN IP4 64.102.241.236
m=video 52670 RTP/SAVP 126 97
b=TIAS:384000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801e;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=content:main
a=label:11
a=rtcp:52671 IN IP4 64.102.241.236
```

在此初始 INVITE 的响应，Cisco Webex 使用 200 OK 消息作为响应。如果您仔细看看这条消息，你会发现音频编解码器已归零。此处有问题，因为未分配音频端口，呼叫将不能以协商该音频流。

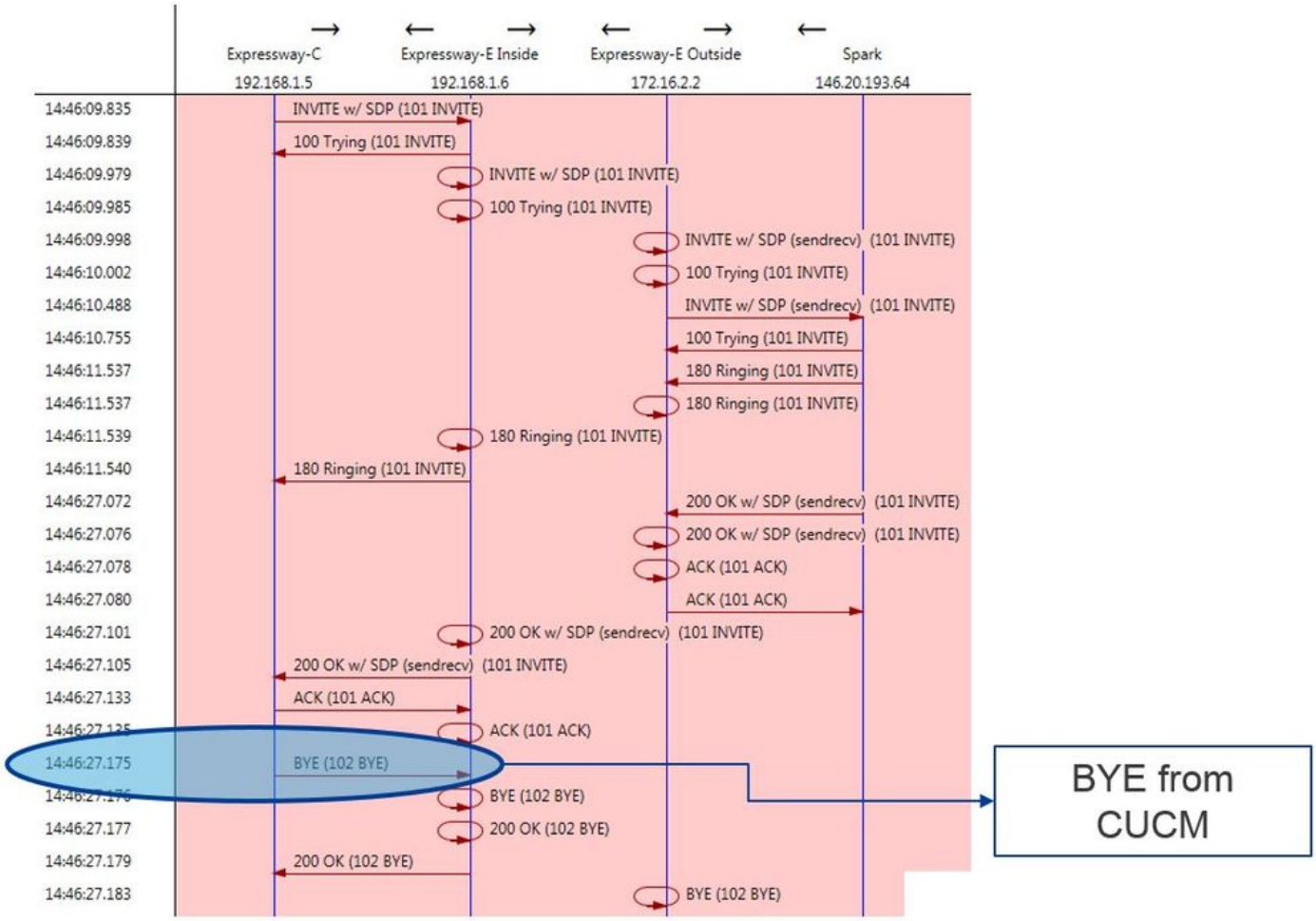
```
2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
SIPMSG:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aedea256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS
172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS
192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-
zone=HybridCallServiceTraversal,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
CSeq: 101 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>
From: "Jonathan Robb"

Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aedea256d2@64.102.241.236:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aedea256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE
User-Agent: Cisco-L2SIP
Supported: replaces
Accept: application/sdp
Allow-Events: kpml
Session-ID: ed35426ed3ade6fdc3b058792333df2b;remote=75957d4fb66a13e835c10737aa329445
Locus: 4711a33f-9d49-11e7-9bf6-dea12d0f2127
Locus-Type: CALL
Content-Type: application/sdp
```

```
Content-Length: 503

v=0
o=linus 0 1 IN IP4 146.20.193.109
s=-
c=IN IP4 146.20.193.109
b=TIAS:384000
t=0 0
m=audio 0 RTP/SAVP *      <-- Webex is zeroing this port out
m=video 33512 RTP/SAVP 108
c=IN IP4 146.20.193.109
b=TIAS:384000
a=content:main
a=sendrecv
a=rtpmap:108 H264/90000
a=fmtp:108 profile-level-id=42001E;packetization-mode=1;max-mbps=40500;max-fs=1620;max-
fps=3000;max-br=10000;max-dpb=3037;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....................................
a=label:200
```

您现在可以使用 TranslatorX 查看其余对话框。您可以看到对话框本身以确认完成。问题在对话框完成后立即出现一个BYE，该BYE来自Expressway-C的方向，如图所示。



以下是BYE消息的详细示例。您可以清楚地看到，用户代理是 Cisco-CUCM11.5，这意味着该消息是由 Unified CM 生成的。需要指出的另一点是，原因代码设置为cause=47。此代码的常见转换是“无可用资源”。

```
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-
```

```
zone=HybridCallServiceTraversal;branch=z9hG4bK90a666b3461356f8cd605cec91e4538240575.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-c60a8b17a8bd;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12ddd10269d39;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 102 BYE
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=329447~c9cc7ddc-9592-49e8-a13c-
79e26f48eebc-30106833
To: <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=f3734601fb0eb541
Max-Forwards: 69
Route: <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:7003;transport=tls;lr>,<sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:5061;transport=tls;lr>
User-Agent: Cisco-CUCM11.5
Date: Tue, 19 Sep 2017 14:46:09 GMT
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Reason: Q.850 ;cause=47
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=ed35426ed3ade6fdc3b058792333df2b
Content-Length: 0
```

由于Cisco Webex组件已将此呼叫示例的音频编解码器归零，因此重点必须是：a.所以重点必须放在发送给 Cisco Webex 的初始 INVITE 以及b.Cisco Webex 用于端口清零的逻辑。现在，了解初始INVITE的独特之处，可以注意到它仅包含G.729。了解此信息，请查阅《Cisco Webex混合呼叫服务部署指南》，并具体查看准备环境一章，其中“完成混合呼叫服务连接的先决条件”部分的步骤5调出了支持的特定编解码器。那里我们会看到以下内容：Cisco Webex 支持以下编解码器：

- 音频 — G.711、G.722、AAC-LD
- 视频 — H.264

注意：Opus不用于Cisco Webex混合呼叫的内部部署。 用手上此信息，您可以得出以下结论：Unified CM 将发送不受支持的音频编解码器是 Cisco Webex 从端口归零的原因。 解决方案：要解决此特殊情况，您可能需要检查Cisco Webex RD（将呼叫锚定在本地）和Expressway-C的SIP中继之间的区域配置。为此，请确定这两个元素所在的设备池。设备池包含到区域的映射。 要确定 Expressway C SIP 中继的设备池，请执行以下操作：

1. 登录Unified CM。
2. 导航至Device > Trunk。
3. 搜索中继名称或单击Find。
4. 选择 Expressway C 中继.
5. 记录设备池的名称。

要确定锚定呼叫的CTI-RD或Cisco Webex-RD的设备池，请执行以下操作：

1. 导航至Device > Phone。
2. 搜索时，您可以选择Device Type contains Webex或CTI Remote Device（取决于客户使用的内容）。
3. 记录设备池的名称。

确定连接到每个设备池的区域：

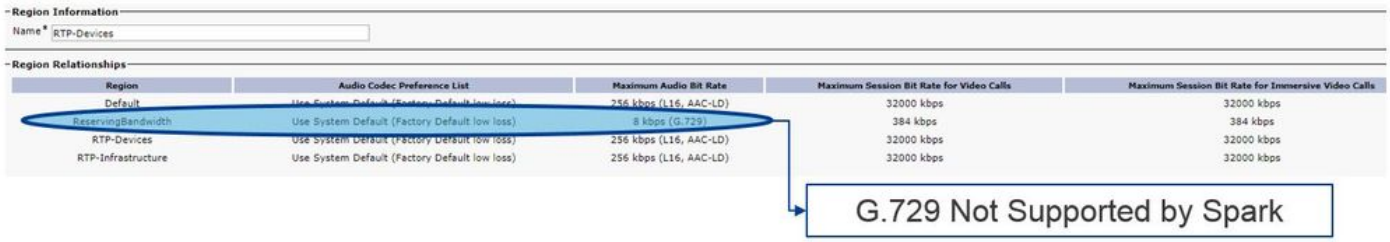
1. 导航到System > Device Pool。
2. 搜索用于 Expressway C SIP 中继的设备池.
3. 单击“Device Pool(设备池)”。
4. 记录区域名称。
5. 搜索用于 Webex-RD 或 CTI-RD 的设备池.
6. 单击“Device Pool(设备池)”。
7. 记录区域名称。

确定区域关系：

1. 导航至系统>区域信息>区域。
2. 搜索确定的一个区域。

3. 确定使用G.729的两个区域之间是否存在区域关系。

此时，如果您确定使用 G.729 的区域之间存在区域关系，您需要调整该关系以支持 Cisco Webex 使用的受支持的音频编解码器或使用一个不同的设备池，该设备池包含一个支持这种关系的区域。在上述记录的场景下，确定以下内容：Expressway-C 中继区域：ReservingBandwidthWebex-RD 区域：RTP 设备下面是RTP设备和ReservingBandwidth区域之间关系的图示，如图所示。



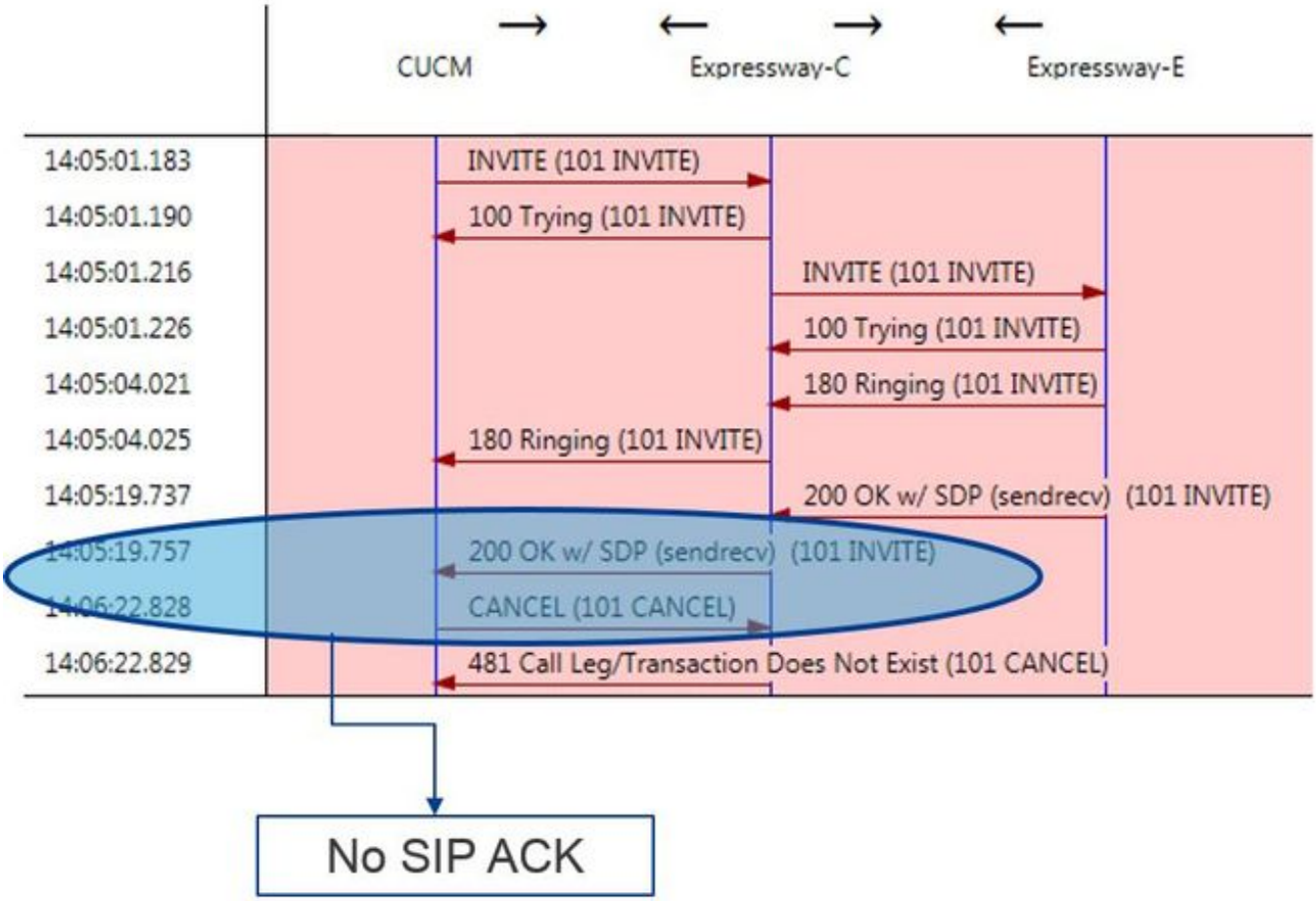
您可以通过更改 Expressway-C 中继所在的设备池来更改区域关系。新设备池有一个区域设置至 RTP-基础设施，因此 Cisco Webex-RD 和 Expressway-C 中继之间的新区域关系是 RTP-设备和 RTP-基础设施之间的关系。如图所示，您可以看到此关系支持AAC-LD，AAC-LD是Cisco Webex支持的音频编解码器之一，因此呼叫将正确设置。 问题 2 超过了 Unified CM 的最大传入消息大小因为在企业中视频应用越来越普遍，包含 SDP 的 SIP 消息尺寸已大幅增长。处理这些消息的服务器必须配置为能够接受大数据包。对于许多呼叫控制服务器，采用默认值即可。对于思科 Unified Communications Manager (Unified CM)，在之前的版本中，采用默认值处理包含 SDP 的较大 SIP 消息不再可行。在Unified CM的更高版本中，SIP消息允许的值大小已增加，但此值仅在新安装时设置，而不是升级时设置。因此，升级Unified CM的旧版本以支持混合呼叫服务连接的客户可能会受到Unified CM上最大传入消息大小过低的影响。如果您试图确定符合此问题描述的混合呼叫服务连接呼叫故障，除了 Unified CM SDL 跟踪数据之外，您还需要获取 Expressway 日志。为了确定故障，首先要了解发生的情况，然后了解发生故障的场景类型。要回答发生什么的问题，您必须知道，一旦Unified CM收到过大的SIP消息，它只会关闭TCP套接字，而不会响应Expressway-C。因此，该故障发生的场景和方式有许多：

1. Cisco Webex 发送一条过大的带 SDP 的入站 INVITE 消息。Expressway-C 会将此消息传递到 Unified CM，Unified CM 关闭 TCP 套接字，然后 SIP 对话将超时。

2. Unified CM 会以 Early Offer 尝试向 Webex 发起出站呼叫，这意味着发送到 EXPRESSWAY-C 的初始 INVITE 消息包含 SDP。Cisco Webex 然后发送一条带 SDP 的 200 OK 响应消息，从 Expressway-C 发送至 Unified CM 的 200 OK 响应消息过大。 Unified CM 关闭 TCP 套接字，然后 SIP 对话将超时。

3. Unified CM 会以 Delayed Offer 尝试向 Webex 发起出站呼叫，这意味着发送到 Expressway-C 的初始 INVITe 消息不包含 SDP。Cisco Webex 然后发送一条带 SDP 的 200 OK 消息，从 Expressway-C 发送至 Unified CM 的 200 OK offer 消息过大。Unified CM 关闭 TCP 套接字，然后 SIP 对话将超时。

查看此特定条件的 Expressway-C 日志可帮助您了解消息流。如果您要使用TranslatorX等程序，您会看到Expressway-C正在将带SDP的Cisco Webex 200 OK(OK)传递到Unified CM。问题是 Unified CM 永远不会回复 SIP ACK 消息，如图所示。



由于 Unified CM 是未响应的根源，因此，有必要检查 SDL 跟踪数据以查看 Unified CM 如何处理这种情况。在此场景中，您会发现Unified CM忽略来自Expressway-C的大消息。将打印类似此的日志行项目。

```
CUCM Traces
53138762.000 |09:05:19.762 |AppInfo  |SIPSocketProtocol(5,100,14,707326)::handleReadComplete
send SdlReadRsp: size 5000
53138763.000 |09:05:19.762 |SdlSig   |SdlReadRsp                                  |wait
|SIPTcp(5,100,71,1)               |SdlTCPConnection(5,100,14,707326)
|5,100,14,707326.4^10.36.100.140^*        |*TraceFlagOverrode
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.
```

在SIP对话超时后，Cisco Webex将向Expressway-E发送入站SIP 603拒绝消息，如日志示例中所述。

```
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="2483073756671246315" SIPMSG: SIP/2.0 603 Decline
```

如前所述，您可以在三种不同的场景中看到此行为。为清楚起见，此处提供的日志样本与第 3 种场景相符，在这一场景下，出站呼叫以 Delayed offer 发送至 Cisco Webex。 解决方案：

1. 登录Unified CM。
2. 导航至系统>服务参数。
3. 选择正在运行 Call Manager 服务的服务器.
4. 当提示选择服务时，选择Cisco Call Manager服务。

5. 选择高级选项。
6. 在集群范围参数（设备-SIP）设置页面，更改SIP 最大传入消息大小值为 18000。
7. 选择Save。
8. 为运行 Cisco Call Manager 服务的每个 Unified CM 节点重复此过程。

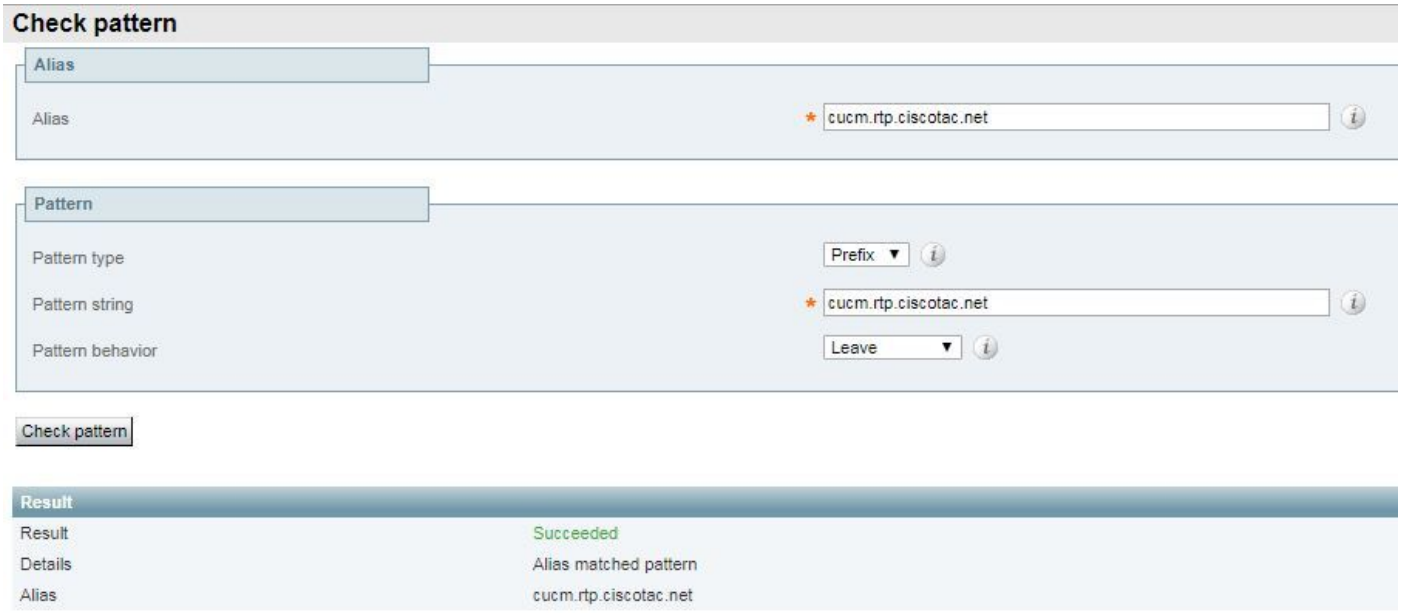
注意：为便于 IP 电话、 协作端点和/或 SIP 中继使用此设置，必须重新启动。这些设备可以单独重新启动，以最大程度地减少对环境的影响。请勿重置CUCM上的每台设备，除非您知道这样做绝对可以接受。Appendix Expressway 故障排除工具选中模式实用程序Expressway具有模式检查实用程序，当您想测试模式是否与特定别名匹配并以预期方式进行转换时，该实用程序非常有用。您可以在维护 > 工具 > 检查模式菜单选项下的 Expressway 上找到该实用程序。通常，如果要测试搜索规则正则表达式是否将别名与模式字符串正确匹配，然后选择性地对字符串执行成功操作，则使用此选项。对于混合呼叫服务连接，您还可以通过测试确定 Unified CM 集群 FQDN 将与您为其设置的模式字符串相匹配。使用此实用程序时，请记住，该呼叫将根据路由报头中的 Unified CM 集群 FQDN 参数而不是目标 URI 进行路由。有关示例，如果以下邀请进入 Expressway，测试复选模式功能根据 cucm.rtp.ciscotac.net 而非 jorobb@rtp.ciscotac.net 来测试选中模式功能。

```
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-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;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;egress-
zone=DefaultZone;branch=z9hG4bK524f89592d00ffc45b7b53000271676c370.88b5177ac4d7cfcae1eb8f8be78da
055;proxy-call-id=2db939b2-a49b-4307-8d96-23716a2c090b;received=172.16.2.2;rport=25010
Via: SIP/2.0/TLS
192.168.4.150:5062;branch=z9hG4bK92f9ef952712e6610c3e6b72770c1230;received=148.62.40.63;rport=39
986;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-313634-
3d27a6f914badee6420287903c9c6a45;rport=45939
Call-ID: 3e613afb185751cdf019b056285eb574@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>
From: "pstojano test" <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=145765215
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

要使用检查模式测试混合呼叫服务连接路由报头搜索规则路由，请执行以下步骤：

1. 导航至维护>工具>检查模式。
2. 对于别名，输入Unified CM集群FQDN。
3. 将Pattern Type设置为Prefix。
4. 将模式字符串设置为Unified CM集群FQDN。
5. 将“模式”行为设置为“离开”。
6. 选择“检查模式”。

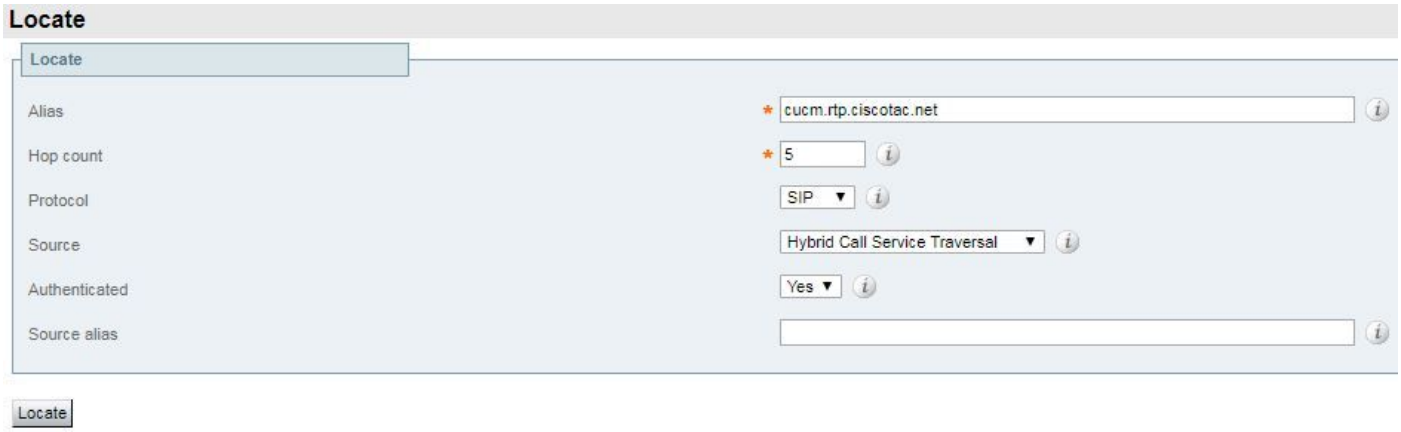
如果 Expressway 上的搜索规则配置正确，您会看到结果返回一条成功消息。 以下是如图所示的成功检查模式测试示例。



成功的原因是此别名(cucm.rtp.ciscotac.net)与(cucm.rtp.ciscotac.net)的前缀模式字符串匹配。 为了了解根据这些结果如何路由呼叫，您可以使用描述的Expressway定位实用程序。定位实用程序如果您想要测试 Expressway 是否可以根据给定的别名将呼叫路由到特定区域，那么 Expressway 的定位实用程序非常有用。您无需定位实际呼叫，就能完成所有这一切。您可以在维护 > 工具 > 定位菜单下的 Expressway 上找到定位实用程序。。您将看到一些说明，了解如何使用Expressway-C上的“定位”功能来确定服务器是否可以根据SIP路由报头中的Unified CM集群FQDN路由呼叫。

1. 导航至维护>工具>定位。
2. 在“别名”字段中输入Unified CM集群FQDN。
3. 选择SIP作为协议。
4. 为源选择Cisco Webex Hybrid Traversal Client Zone。
5. 选择Locate。

界面的底部将显示搜索结果。以下是运行与匹配结果的示例测试示例，如图所示。



以下是查找结果。粗体表示兴趣的价值。结果表明：

- 可以对别名进行路由的事实 (True)
- 源信息 （ 区域名称/类型 ）
- 目标信息 （ 被路由的别名 ）
- 匹配的搜索规则（ 混合呼叫服务的入站路由 ）
- 呼叫将发送到的区域(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
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
```

诊断日志当您为遍历 Expressway 解决方案的呼叫解决主叫方或媒体问题故障时，任何时候都必须使用诊断日志记录。此 Expressway 功能为工程师提供大量的详细信息，用于 Expressway 通过的所有逻辑决策。您可以看到完整的 SIP 消息正文，Expressway 如何传递该呼叫，以及 Expressway 如何设置媒体通道。诊断日志记录有许多不同的模块需要添加日志信息。日志记录级别可进行调整，以显示致命错误 (FATAL)、普通错误 (ERROR)、警告信息 (WARN)、一般信息 (INFO)、调试信息 (DEBUG) 和跟踪信息 (TRACE)。默认情况下，所有内容都设置为INFO，它几乎捕获诊断问题所需的所有内容。有时，您可能需要将某个模块的日志记录级别从一般信息 (INFO) 调整为调试信息 (DEBUG)，以更好地了解当前情况。以下步骤说明您可以如何调整 developer.ssl 模块的日志记录级别，该模块负责为 TLS （相互）握手提供信息。

1. 登录到Expressway服务器（必须在Expressway-E和C上完成）。
2. 导航至维护>诊断>高级>支持日志配置。
3. 滚动至您想要调整的模块，在本例中，滚动至 developer.ssl 模块并单击它。
4. 在“级别”参数旁，从菜单中选择“调试”。
5. Click Save.

此时，您已准备好开始捕获诊断日志记录：

1. 登录Expressway服务器（必须在Expressway-E和C上完成）。
2. 导航至维护>诊断>诊断日志记录。
3. 单击“Start New Log(启动新日志)”(确保选中tcpdump选项)。
4. 重现问题.
5. 单击“Stop Logging(停止日志记录)”。
6. 单击Download Log。

对于 Expressway 诊断日志记录，请记住，您将同时从 Expressway C 和 Expressway E 开始日志记录：首先，在Expressway-E上开始登录，然后转至Expressway-C并启动。此时，您可以重现问题。注意：目前，Expressway/VCS诊断日志捆绑包不包含有关Expressway服务器证书或受信任CA列表的信息。如果您曾因此功能而受益，请在此缺陷后附上您的案例。

相关信息

- 《Cisco Webex 混合呼叫服务部署指南》
- 《Cisco Webex 混合设计指南》

- 《Cisco Expressway 管理员指南 》
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。