

# 对通过 Expressway 进行的企业到企业呼叫的最常见问题进行故障排除

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[常见问题](#)

- [1. 错误“//SIP/SIPTcp/wait SdlReadRsp : 忽略大消息。仅允许最多 5000 个字节。重置连接。”](#)
- [2. 如果另一个呼叫服务器转接呼叫，媒体流将停止。](#)
- [3. CUCM 中未配置顶级域。](#)
- [4. CUCM 证书必须应用客户端身份验证属性。](#)
- [5. 交互工作问题。](#)
- [6. 从 CUCM 收到的 ACK 消息未发送到 VCS-E/Expressway E。](#)
- [7. CUCM 丢弃入站呼叫中的 TCP 会话](#)
- [8. VCS 无法正确解析 FQDN 或查询 SRV 记录失败。](#)

[Related Information](#)

## Introduction

本文档介绍企业到企业 (B2B) 部署中最常见的问题。如何通过 Expressway 对 B2B 呼叫进行故障排除。

## Prerequisites

### Requirements

Cisco 建议您了解以下主题：

- Expressway C (Exp-C)
- Expressway-E
- 思科统一呼叫管理器 (CUCM)
- 网真视频通信服务器-C (VCS-C)

### Components Used

本文档中的信息基于以下软件和硬件版本：

- Expressway C 和 Expressway E X8.1.1 或更高版本
- 统一通信管理器 (CUCM) 10.0 或更高版本

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. 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。

## 常见问题

### 1. 错误“//SIP/SIPTcp/wait\_SdlReadRsp：忽略大消息。仅允许最多 5000 个字节。重置连接。”

由 VCS 中注册的网真端点发出，且通过会话初始协议 (SIP) 中继呼入到 CUCM 中的呼叫出现以下错误“/ SIP/SIPTcp/wait\_SdlReadRsp：忽略大消息。仅允许最多 5000 个字节。重置连接。”

Expressway C/VCS-C 中的呼叫路由配置正确，呼叫发送到 CUCM。SIP Invite 消息发送到 CUCM，但 SDL 日志中没有任何 SIP 消息。可以在 SDL 日志中看到此错误：

```
""|AppInfo|SIPTcp - 忽略来自 xxx.xxx.xxx.xxx:[27469] 的大消息。仅允许最多 5000 个字节。重置连接。”
```

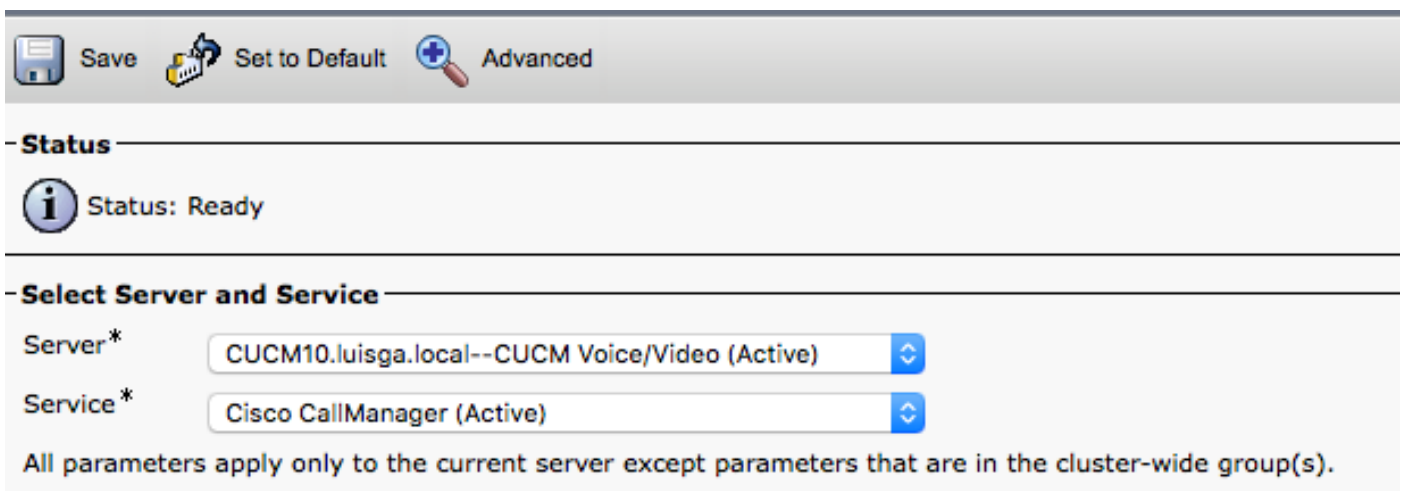
在 CUCM 8.6 及更低版本中，SIP 最大传入消息大小的默认值为 5000，在 CUCM 9.X 之后的版本中，该值更改为 11000。但是，如果从第 8 版或更低版本升级到第 9 或 10 版，会保留之前软件版本中的默认值 (5000)。

### 解决方案

此问题与 [CSCts00642](#) 漏洞有关。

将 CUCM 高级服务参数 **SIP 最大传入消息大小** 从默认值 5000 增加到合适的大小，使其足以应对这些类型的呼叫。11000 是一个理想选择，能适应预期的大多数客户场景。

在 CUCM 管理页面，导航至 **服务参数** 并选择您的 **CUCM 服务器** 和 **CallManager 服务**：



Save Set to Default Advanced

**- Status -**  
i Status: Ready

**- Select Server and Service -**  
Server\* CUCM10.luisga.local--CUCM Voice/Video (Active)  
Service\* Cisco CallManager (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

选择高级选项并搜索 **SIP 最大传入消息大小**：

SIP Max Incoming Message Size *	11000	11000
SIP Max Incoming Message Headers *	100	100

### 2. 如果另一个呼叫服务器转接呼叫，媒体流将停止。

在移动和远程访问 (MRA) 呼叫以及 B2B 呼叫中会出现这种情况。

这会导致在转接呼叫后，单向无声音或出现噪音（与您尝试播放音频加密的捕捉时听到的噪音相同）。出现这种情况的原因是在呼叫设置中选择了转接目的端点不支持的加密套件。

您可以比较呼叫转接前后的 SIP 协商。在 VCS 或 CUCM 日志中的首次协商中，可以看到来自 VCS 的 200 OK 消息中的加密行：

```
m=audio 54582 RTP/SAVP 9 96 97 0 8 18 101
a=rtpmap:9 G722/8000
a=rtpmap:96 G7221/16000
a=fmtp:96 bitrate=32000
a=rtpmap:97 G7221/16000
a=fmtp:97 bitrate=24000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
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:ckXijkT3CcVY+xlof3ozX/TjHPz05OzEdY49rAHA|2^48
a=sendrecv
a=rtcp:54583 IN IP4 10.1.201.7
m=video 54658 RTP/SAVP 96 97
b=TIAS:4000000
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e01e;max-fs=1621;packetization-mode=1;max-rcmd-nalu-size=32000;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42e01e;max-fs=1621;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:S8BJvGB/2l6F7XP8izXxId443Xd9f27oUI/4gxSt|2^48
```

在第一个呼叫中接受了加密行，但在第二个呼叫中，您可以看到 ACK 消息删除了加密行：

```
m=audio 24826 RTP/AVP 0
c=IN IP4 10.1.231.30
a=ptime:20
a=rtpmap:0 PCMU/8000
m=video 0 RTP/AVP 126
c=IN IP4 10.1.98.80
b=TIAS:448000
a=label:11
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42E01F;packetization-mode=1;max-fs=3601;max-rcmd-nalu-size=32000;level-asymmetry-allowed=1
a=content:main
```

VCS 会尝试使用在开头协商的加密行，即使呼叫转接的目的端点不支持加密。

## 解决方案

此问题与 [CSCuv11790](#) 漏洞有关。

要修复此问题，请将 VCS/Expressway 升级到 x8.6.1 版本。

## 3. CUCM 中未配置顶级域。

如果未设置顶级域企业参数，则 CUCM 会将入站呼叫路由到自己的域，并且使用 SIP 路由模式。这可能会导致环路，因为呼叫最有可能发回到 Exp-C，也可能出现“404 未找到错误”。

## 解决方案

从 CUCM 管理页面上，导航至系统 > 企业参数，更改此设置

<b>Clusterwide Domain Configuration</b>	
<a href="#">Organization Top Level Domain</a>	<input type="text"/>
<a href="#">Cluster Fully Qualified Domain Name</a>	<input type="text"/>

## 4. CUCM 证书必须应用客户端身份验证属性。

当 Exp-C 和 CUCM ( 开启 TLS 验证 ) 之间设置了安全连接时，则会根据呼叫的方向，由特定呼叫服务器发起 SSL 握手。这意味着，两台服务器的证书中必须有客户端和服务端身份验证。如果不存在此属性，则 VCS/Expressway 日志中会出现此错误：

```
Line 190: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,060"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connecting"
Line 239: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,071"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Established"
Line 249: 2015-05-07T07:34:01-04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCTime="2015-05-07 11:34:01,081"
Module="network.tcp" Level="DEBUG": Src-ip="10.50.47.16" Src-port="45215" Dst-ip="10.50.47.51"
Dst-port="5061" Detail="TCP Connection Closed" Reason="no certificate returned"
```

## 解决方案

您可以在 VCS 证书指南中找到有关如何使用 Web 客户端和服务端属性配置模板的详细信息

[http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config\\_guide/X8-7/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-7.pdf](http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-7/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-7.pdf)

## 5. 交互工作问题。

VCS/Expressway 版本 X8.6.x 的交互工作流程存在一些问题。

与问题相关的漏洞：

如果您从 VCS/Expressway 检查关于被拒视频 m 行的诊断日志，则会检测到缺陷 [CSCUw85626](#)：

在协商 H323 流 TCS 部分中的媒体行时，会显示此错误消息。

媒体行索引：1

已拒绝：为 true，方向：SDP\_MEDIA\_DIR\_SENDRECV

类型：video / SDP\_MF\_AU\_VID

缺陷 [CSCUw85715](#) 是类似的，但在这种情况下，VCS/Expressway 日志会说明原因是 dataTypeNotSupported：

```
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCtime="2015-10-29 05:49:00,197"
Module="network.h323" Level="INFO": Action="Sent" Dst-ip="XXXXXXXXXXXXXXXXXX" Dst-port="49162"
Detail="Sending H.245 OpenLogicalChannelRejResponse "
2015-10-29T09:49:00+04:00 XXXXXXXXXXXXXXXXXXXX tvcs: UTCtime="2015-10-29 05:49:00,197"
Module="network.h323" Level="DEBUG": Dst-ip="XXXXXXXXXXXXXXXXXX" Dst-port="49162"
Sending H.245 PDU:
value MultimediaSystemControlMessage ::= response : openLogicalChannelReject :
{
forwardLogicalChannelNumber 3,
cause dataTypeNotSupported : NULL
}
```

## 解决方案

升级到 X8.7 或更高版本。

## 6. 从 CUCM 收到的 ACK 消息未发送到 VCS-E/Expressway E。

当配置的遍历区域未指向正确的 VCS Expressway/Expressway E IP 地址时，通常会出现这个问题。

在 ( Expressway/Edge 上的 ) 单个 NIC 部署中，Control/Core 上的遍历客户端区域需要指向遍历服务器的公共 IP 地址。

在双 NIC 部署中，遍历客户端需要指向遍历服务器的内部 IP 地址 ( 内部 NIC 通常是 LAN1，但可以是 LAN2 )。请记住，这是内部局域网的内部 IP 地址。

## 解决方案

有关不同网络部署的详细信息和图表，请参阅[思科 VCS Expressway 和 VCS Control - 基本配置附录 4](#)。

## 7. CUCM 丢弃入站呼叫中的 TCP 会话

如果呼叫是从 VCS Control/Expressway Core 转发的，CUCM 可能会通过丢弃 TCP 会话拒绝此呼叫。

当相邻区域和 SIP 中继安全配置文件之间的端口不匹配或配置为 5060/5061 时，可能会出现这种情况。

B2B 呼叫使用中继通信，但 MRA 使用的是内联通信，而 CUCM 不允许内联通信和中继通信通过同一端口。由于大多数情况下 MRA 是自动配置的，因此 B2B 部署需要使用不同的端口。


## 解决方案

为了做到这一点，相邻区域中给 ( VCS-C/Expressway C 上的 ) CUCM 配置的目的地端口不能为 5060/5061，通常是 5065，但也可以使用其他端口。配置的端口必须与在 CUCM 上分配给此服务器 SIP 中继的 SIP 安全配置文件中配置的端口匹配。

在 CUCM 管理页面，导航至设备 > 中继。

端口为 5065 的 SIP 中继安全配置文件

**Status**

 Status: Ready

---

**SIP Trunk Security Profile Information**

Name\*

Description

Device Security Mode

Incoming Transport Type\*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)\*

X.509 Subject Name

Incoming Port\*

SIP 中继目标端口可以是 5060/5061，如图所示。

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="14.80.86.72"/>	<input type="text"/>	<input type="text" value="5060"/>

VCS/Expressway 相邻区域中的 SIP 端口必须与 SIP 中继安全配置文件中配置的端口匹配，如图所示。

在 Expressway 管理页面，导航至配置 > 协议 > SIP

**SIP**

Mode

Port \*

Transport

Accept proxied registrations

Media encryption mode

ICE support

Preloaded SIP routes support

VCS 没有这种限制或限制不适用于此场景，这意味着 SIP 中继可以配置为 5060/5061。

## 8. VCS 无法正确解析 FQDN 或查询 SRV 记录失败。

对于从 CUCM 发起的 B2B 呼叫，CUCM 处理和路由呼叫的方式可能会引入一个问题。

当 CUCM 将呼叫转发给 VCS 服务器时，CUCM 往往会在被叫 URI 末尾添加 : 5060 或 : 5061 ( 具体取决于配置 ) ， ( 即 test@lab.local >> test@lab.local:5060 ) ，当呼叫到达 Expressway 并满足至 DNS 区域的搜索规则时，VCS 不会查询 SRV 记录，而是仅查询 A 或 AAAA 记录。您可以在 VCS/Expressway 的诊断日志中确认这一点。

## 解决方案

要解决此问题，只需创建一个转换，在到达 DNS 区域之前删除末尾的端口 ( 无论在哪台服务器上均可，这一点并不重要 ) 。

在 Expressway 管理页面，导航至 **配置 > 拨号方案 > 转换 y 配置 > 拨号方案 > 转换**

转换示例：

**Create transform**

Configuration

Priority: 1

Description:

Pattern type: Regex

Pattern string: \*(?!.\*@%localdomains%)(.\*)(:5060|5061)

Pattern behavior: Replace

Replace string: \\1

State: Enabled

**Create transform**

Configuration

Priority: 1

Description:

Pattern type: Regex

Pattern string: \*(.)(:5060|5061)

Pattern behavior: Replace

Replace string: \\1

State: Enabled

如果由于某种原因不能创建转换，还可以通过搜索规则来解决这个问题，但建议通过转换来解决问题。

在 Expressway 管理页面，导航至 **配置 > 拨号方案 > 转换 y 配置 > 拨号方案 > 搜索规则**

## Related Information

- [思科 VCS Expressway 和 VCS Control - 基本配置](#)