

# 通过与 CUCM 集成的 Expressway 配置企业到企业音视频呼叫

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[第 1 步：CUCM 和 Expressway C 之间的 SIP 中继](#)

[a. 添加一个新的 SIP 中继安全配置文件。](#)

[b. 在 CUCM 上配置 SIP 中继。](#)

[c. 在 Expressway-C 上配置邻居区域](#)

[d. 检查证书。](#)

[第 2 步：配置 Expressway C 和 Expressway E 之间的遍历区域](#)

[a. 在 Expressway C 上配置面向 B2B 流量的遍历区域](#)

[b. 在 Expressway E 上配置面向 B2B 流量的遍历区域](#)

[第 3 步：在 Expressway E 上配置 DNS 区域](#)

[第 4 步：配置拨号方案](#)

[a. 转换和/或在 Expressway-C 和 E 上搜索规则](#)

[b. CUCM 中的 SIP 路由模式](#)

[c. 对于 SIP 呼叫路由，必须在公共 DNS 服务器上创建 SRV 记录。](#)

[d. 在 CUCM 中配置集群完全限定域名。](#)

[e. 在 Expressway C 上创建转换，将端口从接收的 URI \(源自 CUCM 的 Invite 消息\) 中移除。](#)

[第 5 步：上传富媒体许可证到 Expressway](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文档介绍如何通过与思科统一呼叫管理器 (CUCM) 集成的 Expressway 集成/配置企业到企业 (B2B) 部署，以便进行音视频通话。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Expressway C (Exp-C)
- Expressway E (Exp-E)
- 思科统一呼叫管理器 (CUCM)
- 思科 Unity Connection (CUC)
- 网真视频通信服务器-C (VCS-C)
- Jabber 电话
- 思科网真系统 (CTS)
- EX 电话
- 会话初始协议 (SIP)
- 超文本传输协议 (HTTP)
- 可扩展消息传送和网真协议 (XMPP)
- 思科 Unified IM and Presence
- 证书

## 使用的组件

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

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

以下步骤详细介绍如何通过 CUCM 集成的 Expressway 集成/配置音视频通话 B2B 部署，从而能够向其他公司（域）发起呼叫或接听来自他们的呼叫。

具有移动远程访问(MRA)功能的Expressway提供企业网络外部的Jabber和TC终端的无缝注册，如网络图所示。

同一架构还可在不同企业（即企业到企业集成）之间提供无缝集成/呼叫，这适用于音频、视频和 IM&P(B2B)

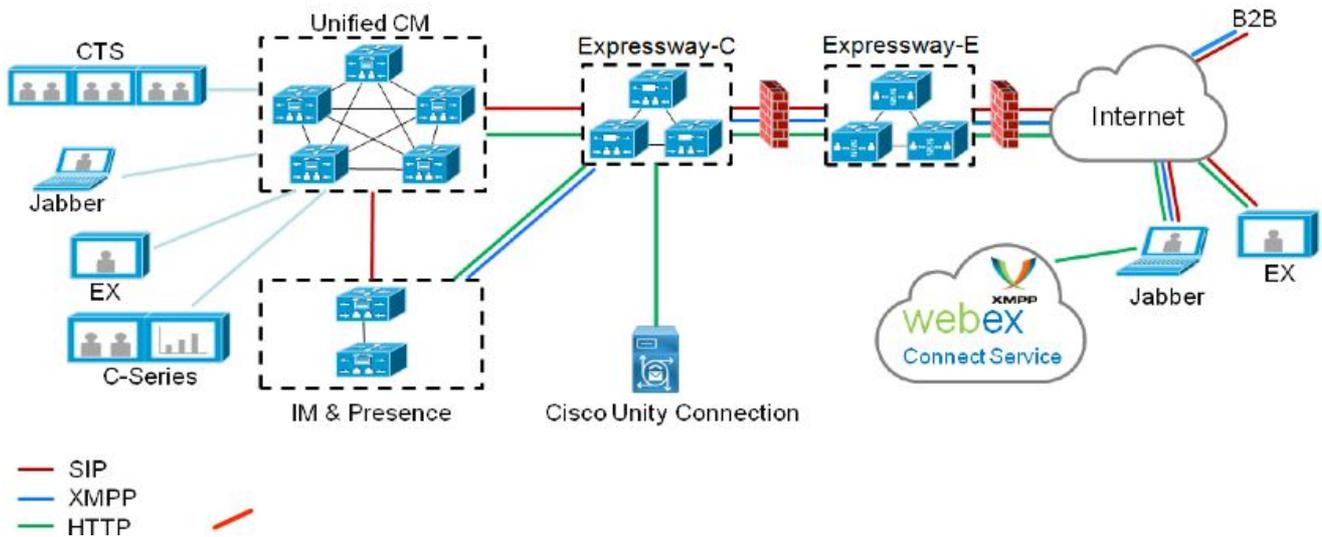
本文档未介绍 IM&P 部分以及 H.323 集成。

在继续之前，您需要确保为域创建相关DNS服务(SRV)，其他公司会使用这些记录来查找 Expressway的位置。

## 配置

### 网络图

下图为网络图示例



## 第 1 步：CUCM 和 Expressway C 之间的 SIP 中继

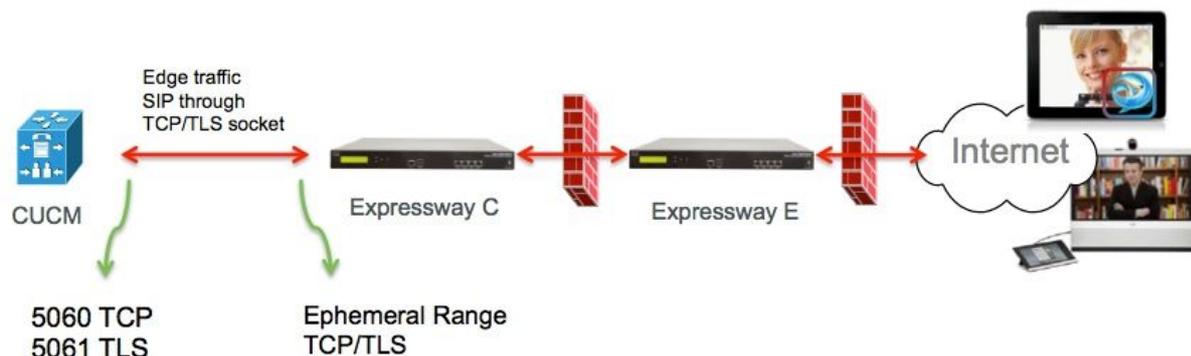
在Expressway-C完成CUCM发现后，会为每个节点自动配置相邻区域，并发现传输协议。

当CUCM集群在混合模式下配置时，对于目标端口为5060的非安全流量，有一个区域用于传输控制协议(TCP)，对于目标端口为5061的安全流量，有一个区域用于TLS (传输层安全)。这些端口不能更改。

这两个区域用于进出边缘终端的所有边缘呼叫。

来自边缘端点的呼入呼叫会使用这些自动添加区域的路由，因此会发往 CUCM 上的 TCP 5060 或 TLS 5061 端口。

边缘终端通过已建立的套接字进行注册以及发起/接收呼叫。



对于B2B呼叫，请在CUCM中配置指向Expressway-C的SIP中继，其中CUCM通常在端口5060或5061上侦听来自此网关的入站流量。

由于边缘流量来自与端口 5060/5061 相同的源 IP 地址，因此需要为 CUCM 中的该中继使用不同的侦听端口。否则，边缘流量将路由到CUCM中的SIP中继设备，而不是路由到终端设备 (CSF或EX)。

对于 Expressway C 端，为会话初始协议 (SIP) TCP/TLS 使用端口 5060 和 5061。

下图展示了 CUCM 在端口 6060/6061 侦听该中继的入站流量的示例



以下为此部署的不同配置步骤，包括安全和非安全部署。

a. 添加一个新的 SIP 中继安全配置文件。

在 CUCM 管理页面，导航至 > 设备 > 中继。

配置与5060/5061不同的传入端口，此处使用6060作为TCP，使用6061作为TLS

非安全 SIP 中继配置文件

## - SIP Trunk Security Profile Information

Name*	B2B SIP TRUNK EXPRESSWAY None Secure
Description	Non Secure SIP Trunk Profile for B2B Expressway
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	6060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

## 安全 SIP 中继配置文件

对于TLS，您还需要配置与Expressway-c提供的证书的CN匹配的X.509使用者名称。此外，还将Expressway-C或CA证书（颁发Expressway-C证书）上传到CUCM证书信任库。

## - SIP Trunk Security Profile Information

Name*	B2B SIP TRUNK EXPRESSWAY SECURE
Description	Secure SIP Trunk Profile for B2B Expressway
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	expresswayc.cisco.com
Incoming Port*	6061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

### b.在 CUCM 上配置 SIP 中继。

通过此中继，所有B2B呼叫都流入和流出CUCM。

SIP 中继配置参数是 CUCM VCS 部署的标准参数。

确保关联在第 1 步中创建的安全配置文件。

### c.在Expressway-C上配置邻居区域

需要在Expressway-C 上配置指向 CUCM 的相邻区域。

此区域用于将入站 B2B 流量路由到 CUCM。

此配置为标准配置，唯一的例外是必须确保配置的目的端口与分配给 CUCM SIP 中继的 SIP 中继安全配置文件中配置的侦听端口相对应。

在本示例中，SIP/TCP使用的目标端口为6060,SIP/TLS使用的目标端口为6061。（请参阅步骤1），如图所示

从Expressway管理页面，导航至 **Configuration > Dial Plan > Transforms y Configuration**

SIP TCP 相邻区域：

**Configuration**

Name  ⓘ

Type

Hop count  ⓘ

**H.323**

Mode  ⓘ

**SIP**

Mode  ⓘ

Port  ⓘ

Transport  ⓘ

Accept proxied registrations  ⓘ

Media encryption mode  ⓘ

ICE support  ⓘ

**Authentication**

Authentication policy  ⓘ

SIP authentication trust mode  ⓘ

**Location**

Peer 1 address  ⓘ SIP: Reachable: 10.48.79.105:6060

Peer 2 address  ⓘ

Peer 3 address  ⓘ

Peer 4 address  ⓘ

Peer 5 address  ⓘ

Peer 6 address  ⓘ

**Advanced**

Zone profile  ⓘ

## SIP TLS 相邻区域 - TLS 验证模式已启用

TLS 验证模式设置为启用时，必须确保对等体地址匹配 CUCM 所提供证书的 CN 或 SAN。通常，在 TLS 验证模式下，为对等地址配置 CUCM 节点的完全限定域名(FQDN)。

从“Expressway管理”页，导航至配置>拨号方案>转换y配置

Configuration	
Name	CUCMZONE
Type	Neighbor
Hop count	20

H.323	
Mode	Off

SIP	
Mode	On
Port	6061
Transport	TLS
TLS verify mode	On
Accept proxied registrations	Deny
Media encryption mode	Auto
ICE support	Off

Authentication	
Authentication policy	Do not check credentials
SIP authentication trust mode	Off

Location	
Peer 1 address	cucm.cisco.com
Peer 2 address	
Peer 3 address	
Peer 4 address	
Peer 5 address	
Peer 6 address	

SIP: Reachable: 10.48.79.105:6060

Advanced	
Zone profile	Cisco Unified Communications Manager (8.6.1 or later)

## SIP TLS 相邻区域 - TLS 验证模式已关闭

当TLS验证模式设置为关闭时，对等体地址可以是CUCM节点的IP地址、主机名或FQDN。

从Expressway管理页面，导航至 **Configuration > Dial Plan > Transforms y Configuration**

Configuration		
Name	CUCMZONE	
Type	Neighbor	
Hop count	20	

H.323		
Mode	Off	

SIP		
Mode	On	
Port	6061	
Transport	TLS	
TLS verify mode	Off	
Accept proxied registrations	Deny	
Media encryption mode	Auto	
ICE support	Off	

Authentication		
Authentication policy	Do not check credentials	
SIP authentication trust mode	Off	

Location		
Peer 1 address	10.48.79.105	SIP: Reachable 10.48.79.105:6050
Peer 2 address		
Peer 3 address		
Peer 4 address		
Peer 5 address		
Peer 6 address		

Advanced		
Zone profile	Cisco Unified Communications Manager (8.6.1 or later)	

#### d.检查证书。

对于 TLS，确保以下几点：

- Expressway C 服务器证书或 CA 根证书（用于签署证书）已上传到 CUCM 集群所有服务器上的 CUCM 信任库。
- Callmanager 证书或 CA 根证书（用于签署证书）已上传到 Expressway-C 服务器上的受信任 CA 证书列表。

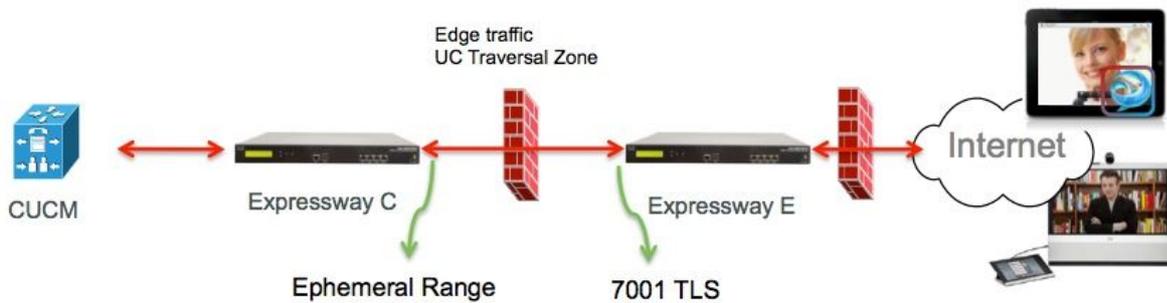
### 第 2 步：配置 Expressway C 和 Expressway E 之间的遍历区域

必须配置单独的穿越区域，以便在 Expressway-C 和 Expressway-E 之间路由 B2B 流量。

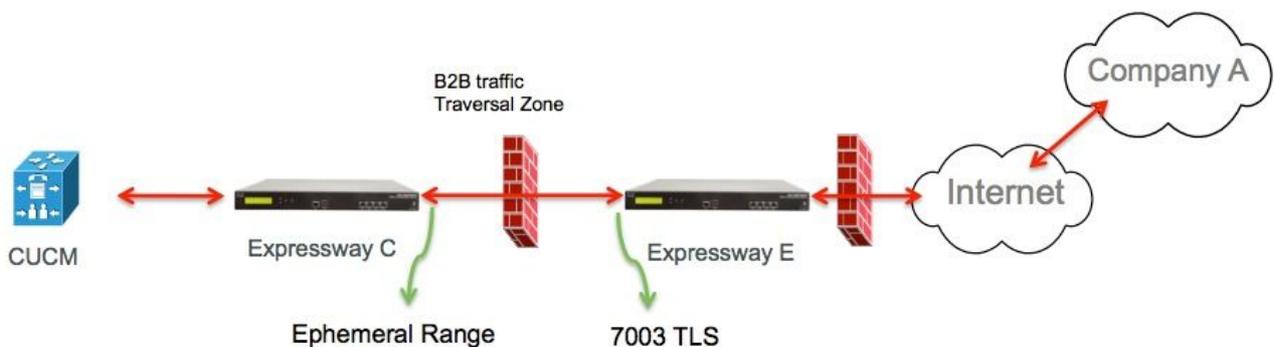
这是标准的穿越区域配置，但与 CUCM 上的 SIP 中继类似，配置的端口必须不同于面向边缘流量的 UC 穿越区域所用的端口。

UC 穿越区域的标准端口为 7001。对于 B2B 遍历区域，例如配置 7003。

面向边缘流量的 UC 穿越区域（如图所示）



面向 B2B 流量的穿越区域（如图所示）



#### a.在 Expressway C 上配置面向 B2B 流量的遍历区域

Expressway-C是穿越区域客户端，在本例中，目标端口为7003

TLS 验证模式设置为启用时，确保配置的对等体地址与 Expressway E 所提供证书的 CN 或 SAN 匹配。

从“Expressway管理”页，导航至配置>拨号方案>转换y配置

The screenshot displays the configuration page for a dial plan conversion, organized into several sections:

- Configuration:**
  - Name:
  - Type:  (highlighted with a red box)
  - Hop count:
- Connection credentials:**
  - Username:
  - Password:  (highlighted with a red box)
- H.323:**
  - Mode:
  - Protocol:
- SIP:**
  - Mode:
  - Port:  (highlighted with a red box)
  - Transport:
  - TLS verify mode:  (highlighted with a red box)
  - Accept proxied registrations:
  - Media encryption mode:
  - ICE support:
  - SIP poison mode:
- Authentication:**
  - Authentication policy:
- Client settings:**
  - Retry interval:
- Location:**
  - Peer 1 address:  (highlighted with a red box)
  - Peer 2 address:
  - Peer 3 address:

b.在 Expressway E 上配置面向 B2B 流量的遍历区域

Expressway-E是穿越区域服务器，在本例中，侦听端口为7003。

TLS 验证模式设置为启用时，确保配置的 TLS 验证主题名称与 Expressway C 所提供证书的 CN 或 SAN 匹配。

从“Expressway管理”页，导航至**配置>拨号方案>转换y配置**

**Configuration**

Name \*  ⓘ

Type Traversal server

Hop count \*  ⓘ

---

**Connection credentials**

Username \*  ⓘ

Password [Add/Edit local authentication database](#)

---

**H.323**

Mode  ⓘ

Protocol  ⓘ

H.460.19 demultiplexing mode  ⓘ

---

**SIP**

Mode  ⓘ

Port \*  ⓘ

Transport  ⓘ

TLS verify mode  ⓘ

TLS verify subject name \*  ⓘ

Accept proxied registrations  ⓘ

Media encryption mode  ⓘ

ICE support  ⓘ

SIP poison mode  ⓘ

---

**Authentication**

Authentication policy  ⓘ

### 第 3 步：在 Expressway E 上配置 DNS 区域

要路由B2B流量，请在Expressway-E上配置DNS区域。

对于发往此区域的流量，Expressway-E对ether\_sip或\_sip执行DNS SRV查找，并对从SIP URI的域部分派生的域执行DNS SRV查找。

DNS 服务器返回的 SRV 目标用于路由 SIP 呼叫。

此配置是标准的 DNS 区域配置。

从Expressway管理页，导航至**配置>区域**

**Create zone** You are here: [Configuration](#) > [Zones](#) > [Zones](#) > [Create zone](#)

**Configuration**

Name  ⓘ

Type  ⓘ

Hop count  ⓘ

**H.323**

Mode  ⓘ

**SIP**

Mode  ⓘ

TLS verify mode  ⓘ

Fallback transport protocol  ⓘ

Media encryption mode  ⓘ

ICE support  ⓘ

**Advanced**

Include address record  ⓘ

Zone profile  ⓘ

## 第 4 步：配置拨号方案

### a. 转换和/或在Expressway-C和E上搜索规则

从Expressway管理页面，导航至 **Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform or Search Rules**

有关详细信息，请参阅[VCS部署指南](#)(Control with Expressway)，该章节的“路由配置”：

## b.CUCM 中的 SIP 路由模式

有关详细信息，请参阅《CUCM 系统和管理指南》（拨号方案部署指南）

## c.对于SIP呼叫路由，必须在公共DNS服务器上创建SRV记录。

如图所示，它列出了所需的SRV记录，以及本文档中未讨论的H323 B2B呼叫。请注意，Expressway 上默认禁用 SIP UDP。

### DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
example.com.	h323cs	tcp	10	10	1720	expe.example.com.
example.com.	h323ls	udp	10	10	1719	expe.example.com.
example.com.	sip	tcp	10	10	5060	expe.example.com.
example.com.	sip	udp *	10	10	5060	expe.example.com.
example.com.	sips	tcp	10	10	5061	expe.example.com.

## d.在 CUCM 中配置集群完全限定域名。

可以输入多个以逗号分隔的条目。



Clusterwide Domain Configuration

Organization Top Level Domain:

Cluster Fully Qualified Domain Name:

## e.在 Expressway C 上创建转换，将端口从接收的 URI ( 源自 CUCM 的 Invite 消息 ) 中移除。

有关详细信息，请查看本文档[VCS Expressway上从CUCM到DNS区域的呼叫发送到错误的IP地址](#)

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



Configuration

Priority: 5

Description: Remove port from URI for outbound calls to vngtp.lab

Pattern type: Regex

Pattern string: (\*).@vngtp.lab(:.\*)?

Pattern behavior: Replace

Replace string: !1@vngtp.lab

State: Enabled

SRND 还包含详细介绍拨号方案的章节。

## 第 5 步：上传富媒体许可证到 Expressway

富媒体许可证（亦称遍历区域许可证）必须上传到每个 Expressway 服务器。

其目的在于防止呼叫丢失或由于配置不正确而导致释放呼叫并出现以下错误消息：“已达到呼叫许可证限值：您已达到并发穿越呼叫许可证的许可证限值”

## 验证

当前没有可用于此配置的验证过程。

## 故障排除

有关B2B的进一步故障排除信息，请参阅本文档[“通过Expressway排除企业到企业呼叫的最常见问题”](#)

## 相关信息

- [思科网真视频通信服务器 \(VCS\)](#)
- [技术支持和文档 - Cisco Systems](#)