在多域部署下配置基于 Expressway/VCS 的移动和远程访问

目录

简介

本文档介绍在使用多个域的情况下，应如何配置思科网真视频通信服务器 (VCS) 来实现移动远程访问 (MRA)。

在仅使用一个域时，MRA 的设置相对简单，只需按照部署指南中提供的步骤操作即可。但是，在使用了多个域的情况下，MRA 部署会变得更加复杂。本文档不作为配置指南提供，仅用于介绍在多域环境下部署 MRA 的重要注意事项。有关具体配置步骤的说明，请参阅思科网真视频通信服务器 (VCS) 部署指南。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

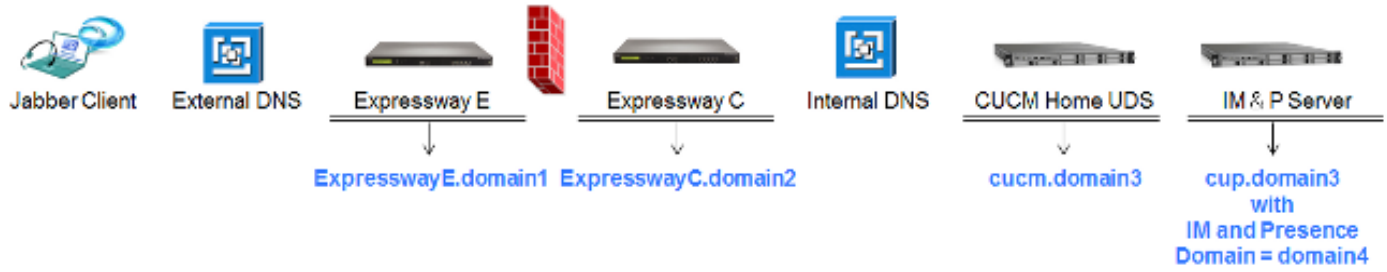
本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

请参阅本节提供的信息配置 VCS。

网络图

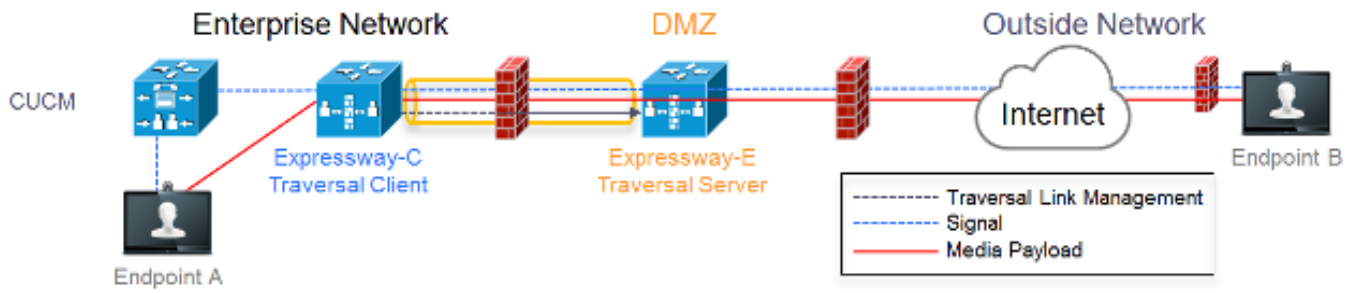


下面是对不同域的简要描述：

- **domain1 - 供客户端使用的边缘域。客户端通过该域发现边缘服务器的位置，进而通过边缘服务器发现用户数据服务 (UDS)。**
- **domain2 和 domain3 - 用于服务器发现的域。**
- **domain4 - 即时消息传输和在线状态 (IM&P) 域，用于可扩展通信平台 (XCP) 和可扩展消息传送和网真协议 (XMPP) 流量。**

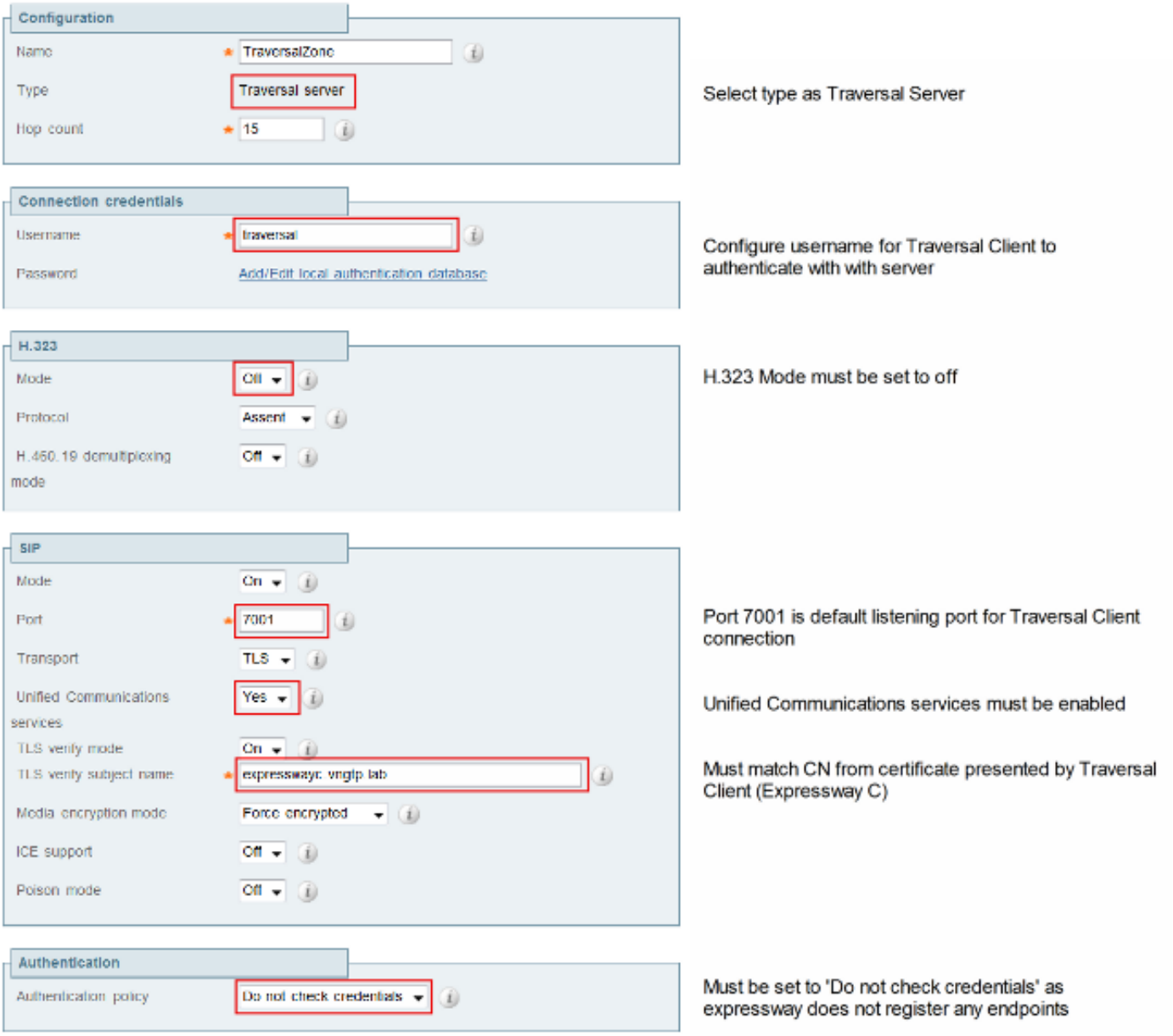
穿越区域

穿越区域由位于隔离区 (DMZ) 的穿越服务器 (**expresswayE**) 和位于网络内部的穿越客户端 (**expresswayC**) 组成：



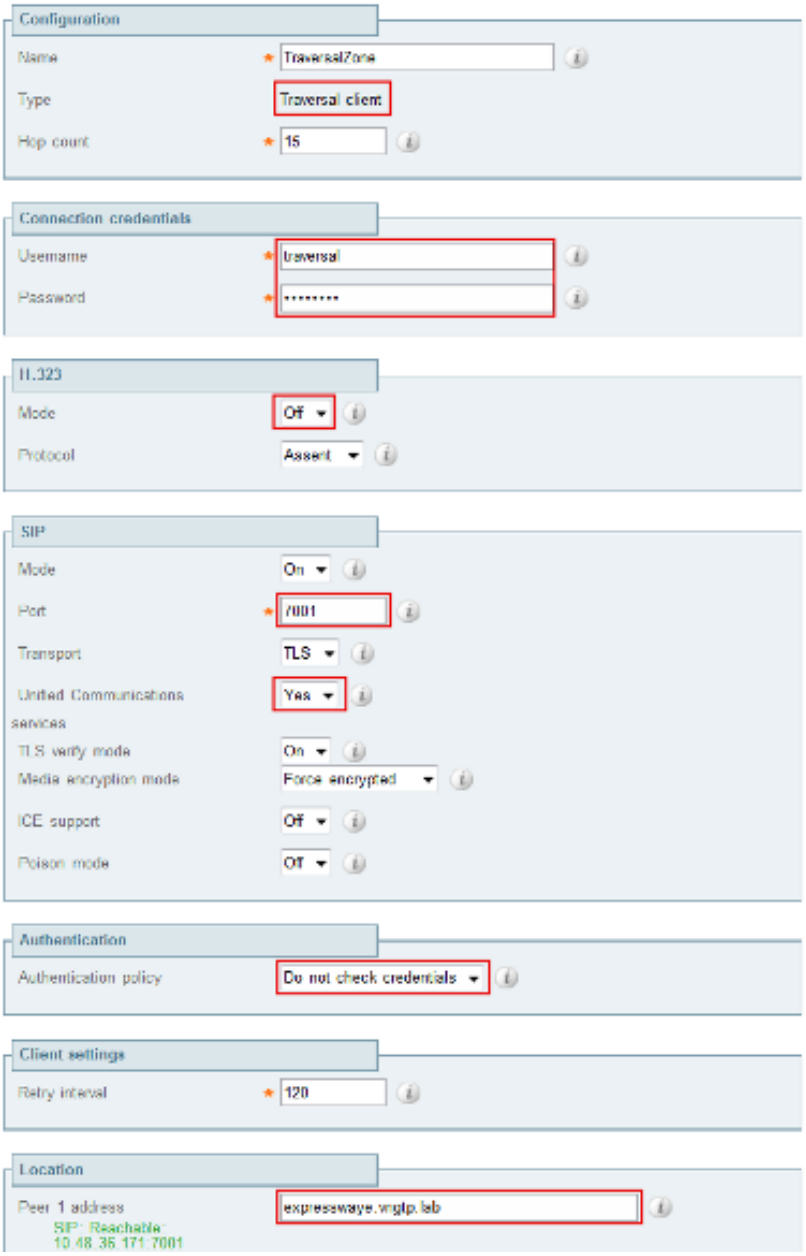
穿越服务器

穿越服务器位于 Expressway E 中配置的区域：



穿越客户端

穿越客户端位于 Expressway C 中配置的区域：



语音服务域

用户通常使用 **userid@domain4** 登录，因为内部用户与外部用户在用户体验上应该没有差异。这意味着如果 **domain1 与 domain4** 不同，则必须在 Jabber 客户端上配置语音服务域。这是因为系统会使用登录名中的域名部分执行服务 (SRV) 记录查找，以发现协作边缘服务。

客户端会针对 **_collab-edge._tls.<domain>** 执行域名系统 (DNS) SRV 记录查询。因此，如果登录用户 ID 中的域名与 Expressway E 中配置的域不同，就必须使用语音服务域配置。Jabber 使用此配置来发现协作边缘和 UDS。

此配置可以通过多种方式来实现：

1. 在通过媒体服务接口 (MSI) 安装 Jabber 时，添加如下参数：

```
msiexec /i CiscoJabberSetup.msi VOICE_SERVICES_DOMAIN=domain1 CLEAR=1
```

2. 导航至 **%APPDATA% > 思科 > 统一通信 > Jabber > CSF > 配置**，然后在此目录中创建如下 **jabber-config-user.xml 文件：**

```
<?xml version="1.0" encoding="utf-8"?>
<config version ="1.0">
<Policies> <VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
</config>
```

注意：此方法仅作为实验性方法提供，并非思科正式推荐的方法。

3. 修改 **jabber-config.xml 文件。**此方法要求客户端先进行内部登录。Jabber配置文件生成器可用于以下操作：

```
<Policies>
<VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
```

4. 除此之外，也可以事先通过语音服务域对 Jabber 移动客户端进行配置，使其无需进行内部登录。具体操作详见《部署和配置指南》的服务发现一章。要使用此方法，您必须创建用户所需点击的配置 URL：

```
ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1
```

注意：之所以需要使用语音服务域，是因为您必须确保对外部域 (**domain1**) 执行协作边缘 SRV 记录查找。

DNS 记录

本节介绍外部和内部 DNS 记录的配置设置。

外部

类型	条目	解析结果
SRV 记录	_collab-edge._tls.domain1	ExpresswayE.domain1
A 记录	ExpresswayE.domain1	IP 地址 ExpresswayE

需要重点指出的是：

- SRV 记录返回的是完全限定域名 (FQDN)，而不是 IP 地址。
- SRV 记录返回的 FQDN 必须与 Expressway-E 的实际 FQDN 相符，或者 SRV 记录的目标为 CNAME，但别名指向与 Expressway-E 位于同一域内的服务器（详见未解决的思科错误 ID CSCuo82526）。

存在上述要求的原因是，Expressway-E 会使用自己的域 (**domain1**) 为客户端设置 Cookie，如果该域与 FQDN 返回的域不一致，客户端不会接受这种情况。我们已记录了思科错误 ID CSCuo83458，以解决这个情况。

内部

类型	条目	解析结果
SRV 记录	_cisco-uds._tcp.domain1	cucm.domain3
A 记录	cucm.domain3	IP 地址 CUCM

由于语音服务域设置为 **domain1**，Jabber 会在经过格式转换以用于执行协作边缘配置发现 (**get edge_config) 的 URL 中嵌入 domain1。** 在收到此信息后，Expressway-C 会对 **domain1 执行 SRV**

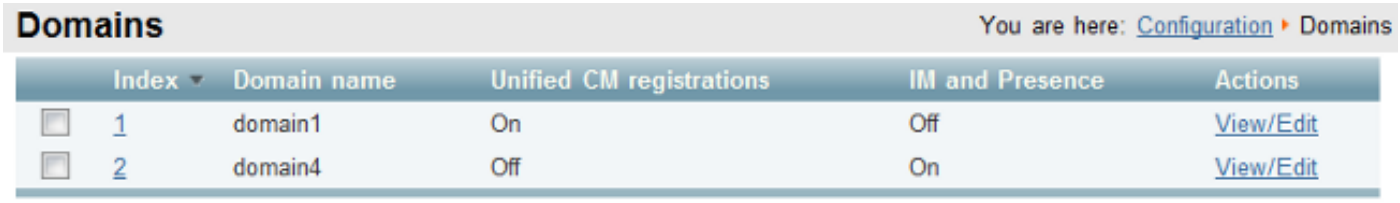
UDS 记录查询，并在 200 OK 消息中返回相关的记录。

类型	条目	解析结果
SRV	_cisco-uds._tcp.domain4	cucm.domain3
A 记录	cucm.domain3	IP 地址 CUCM

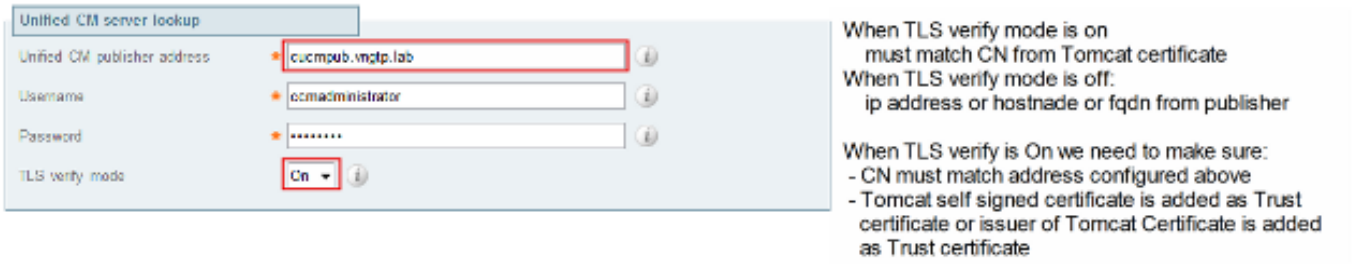
当客户端位于网络内部时，系统会对 **domain4** 执行 SRV UDS 记录发现。

Expressway-C 中的 SIP 域

您必须为 MRA 添加并启用 Expressway-C 中的下列会话初始协议 (SIP) 域：



主机名/IP 地址 CUCM 服务器



在配置思科统一通信管理器 (CUCM) 服务器时，您会遇到两种场景：

- 如果 Expressway-C (**domain2**) 与 CUCM 服务器 (**domain3**) 配置了相同的域，您可以使用以下参数配置 CUCM 服务器（**系统 > 服务器**）：

  IP 地址主机名FQDN
- 如果 Expressway-C (**domain2**) 与 CUCM 服务器 (**domain3**) 配置了不同的域，您必须使用以下参数配置 CUCM 服务器：

  IP 地址FQDN

存在上述要求的原因是，当 Expressway-C 发现 CUCM 服务器并获得返回的主机名后，会对 **hostname.domain2** 执行 DNS 查找；如果 **domain2 与 domain3 不同，则会导致查找无效。**

证书

除了遵循一般证书要求外，还应在证书的使用者替代名称 (SAN) 中添加其他一些内容：

- Expressway-C

  必须添加 IM&P 服务器上配置的聊天节点别名。此要求仅适用于需要同时使用传输层安全 (TLS) 和群组聊天的统一通信 XMPP 联合部署。如果 IM&P 服务器已发现该别名，该别名会自动添加到证书签名请求 (CSR) 中。

必须添加 CUCM 的所有电话安全配置文件中配置用于加密 TLS 并供请求远程访问的设备使用的名称（FQDN 格式）。
注意：仅当证书颁发机构 (CA) 不支持 SAN 中的主机名语法时，才需要使用 FQDN 格式。

- Expressway-E

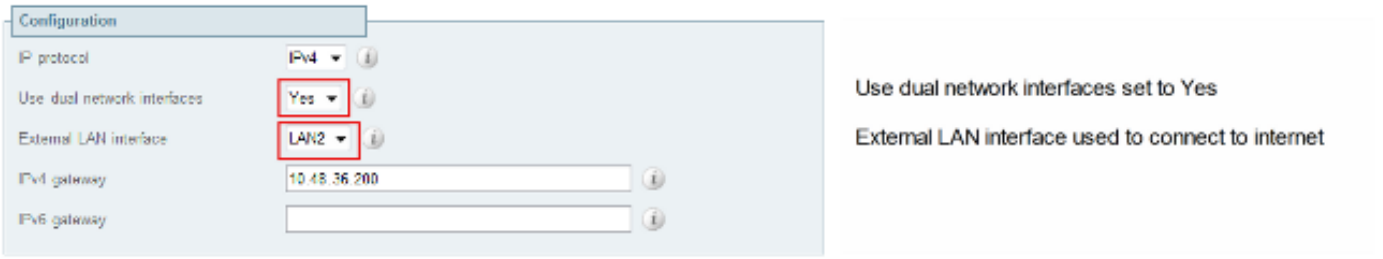
必须添加用于执行服务发现的域 (**domain1**)。 必须添加 XMPP 联合域。必须添加 IM&P 服务器上配置的聊天节点别名。此要求仅适用于需要同时使用 TLS 和群组聊天的统一通信 XMPP 联合部署。这些信息可以从 Expressway-C 生成的 CSR 中复制。

双 NIC

本节介绍在使用双网络接口卡 (NIC) 时的配置设置。

双接口

如需将 Expressway-E 配置为使用双网络接口，必须确保正确配置并使用两个接口。



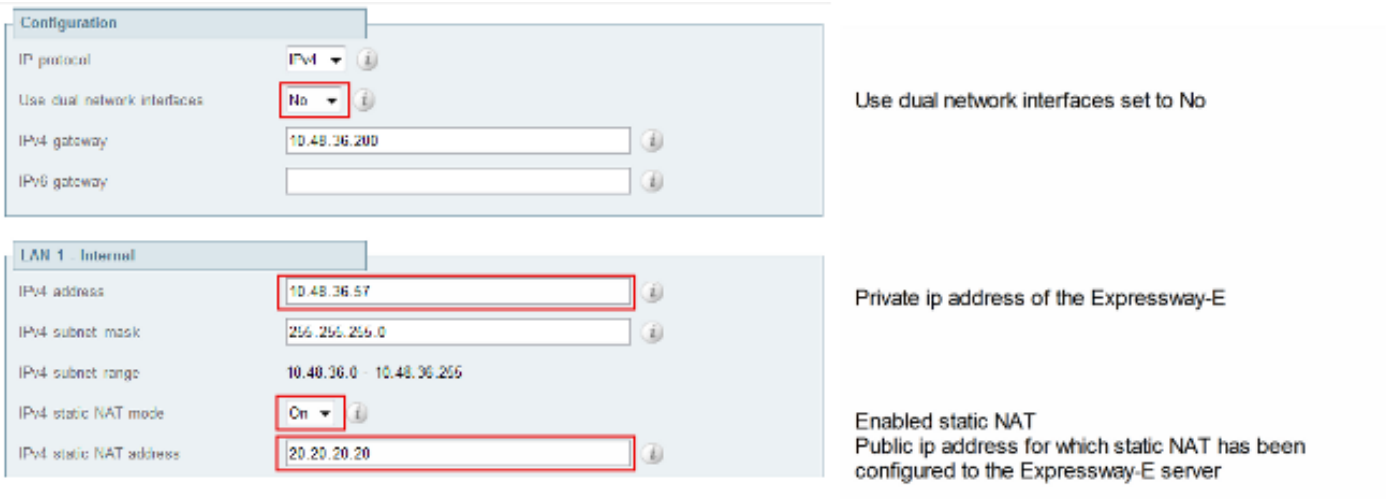
当**使用双网络接口**的值配置为**是**时，Expressway-E仅侦听内部接口上与Expressway-C进行XMPP通信。因此，您必须确保此接口已配置并正常运行。

单接口 - 公共 IP 地址

如果您只使用一个接口，而且为 Expressway-E 配置了公共 IP 地址，则没有需要特别注意的问题。

单接口 - 专用 IP 地址

如果您只使用一个接口，而且为 Expressway-E 配置了专用 IP 地址，则必须额外配置静态网络地址转换 (NAT) 地址：



在这种情况下，应注意以下两点：

- 确保防火墙允许 Expressway-C 向公共 IP 地址发送流量。此行为也称为 *NAT 反射*。
- 确保为 Expressway-C 的穿越客户端区域配置与 Expressway-E 上的静态 NAT 地址相匹配的对等地址（示例中为 **20.20.20.20**）。

  提示：有关高级网络部署的更多信息，请参阅思科网真视频通信服务器基础配置（通过 Expressway 进行控制）部署指南的**附录 4**。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

本节列出了一些特殊情况，但是您也可以使用协作解决方案分析器来查看所有 MRA 登录尝试通信的详细信息，并通过诊断日志获得故障排除信息。

穿越区域

如果对等地址配置为 IP 地址，或者对等地址与通用名称 (CN) 不匹配，您会在日志中看到以下信息：

```
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.80.161"
Src-port="25697" Dst-ip="10.48.36.171" Dst-port="7001" Detail="Peer's TLS
certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.36.171"
```

如果密码不正确，您会在 Expressway-E 日志中看到以下信息：

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found in
directory for identity: traversal"
```

```
Module="developer.nomodule" Level="WARN" CodeLocation="ppcmains/sip/sipproxy/
SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::
checkDigestSAResponse" Thread="0x7f2485cb0700": calculated response does not
match supplied response, calculatedResponse=769c8f488f71eebdf28b61ab1dc9f5e9,
response=319a0bb365decf98c1bb7b3ce350f6ec

Event="Authentication Failed" Service="SIP" Src-ip="10.48.80.161"
Src-port="25723" Detail="Incorrect authentication credential for user"
Protocol="TLS" Method="OPTIONS" Level="1"
```

双 NIC

如果在启用双 NIC 的情况下未使用或未连接第二个接口，Expressway-C 将无法通过端口 7400 连接到 Expressway-E 进行 XMPP 通信。在这种情况下，Expressway-C 日志中会显示以下信息：

```
xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,843" ThreadID=
"139747212576512" Module="Jabber" Level="INFO " CodeLocation="mio.c:1109"
Detail="Connecting on fd 28 to host '10.48.36.171', port 7400"xwayc

XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID="139747212576512"
Module="Jabber" Level="ERROR" CodeLocation="mio.c:1121" Detail="Unable to
connect to host '10.48.36.171', port 7400:(111) Connection refused"

xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID=
"139747406935808" Module="Jabber" Level="ERROR" CodeLocation=
"base_connection.cpp:104" Detail="Failed to connect to component
jabberd-port-1.expresswayc-vngtp-lab"
```

DNS

如果对协作边缘执行的 SRV 记录查找所返回的 FQDN 与 Expressway-E 中配置的 FQDN 不一致，Jabber 日志中将显示如下错误信息：

```
WARNING [9134000] - [csf.edge][executeEdgeConfigRequest] XAuth Cookie expiration
time is invalid or not available. Attempting to Failover.

DEBUG [9134000] - [csf.edge][executeEdgeConfigRequest]Failed to retrieve
EdgeConfig with error:INTERNAL_ERROR
```

在 Expressway-E 的诊断日志中，您可以在 HTTPS 消息部分查看用于设置 Cookie 的域：

```
Set-Cookie: X-Auth=1e1111e1-dddb-49e9-ad0d-ab34526e2b00; Expires=Fri,
09 May 2014 20:21:31 GMT; Domain=.vngtp.lab; Path=/; Secure
```

SIP 域

如果没有将所需的 SIP 域添加到 Expressway-C，Expressway-E 将不会接受该域的消息，您将在诊断日志中看到客户端发送的 **403 禁止访问消息**：

```
ExpresswayE traffic_server[15550]:
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response"
Txn-id="2" Dst-ip="10.48.79.80" Dst-port="50314"
HTTPMSG:
|HTTP/1.1 403 Forbidden
Date: Wed, 21 May 2014 14:31:18 GMT
Connection: close
```

```
Server: CE_E
Content-Length: 0

ExpresswayE traffic_server[15550]: Event="Sending HTTP error response"
Status="403" Reason="Forbidden" Dst-ip="10.48.79.80" Dst-port="50314"
```