# Configurar acesso móvel e remoto pelo Expressway/VCS em uma implantação com vários domínios

## Contents



## Introduction

Este documento descreve como configurar o Cisco TelePresence Video Communication Server (VCS) para acesso remoto móvel (MRA, Mobile Remote Access) quando são utilizados vários domínios.

A configuração do MRA quando há apenas um domínio é relativamente simples e você pode seguir as etapas documentadas no guia de implantação. Quando a implantação envolve vários domínios, ela se torna mais complexa. Este documento não é um guia de configuração, mas descreve os aspectos importantes quando vários domínios estão envolvidos. A configuração principal é documentada no Guia de implantação do Cisco TelePresence Video Communication Server (VCS).

# Prerequisites

## Requirements

Não existem requisitos específicos para este documento.

## Componentes Utilizados

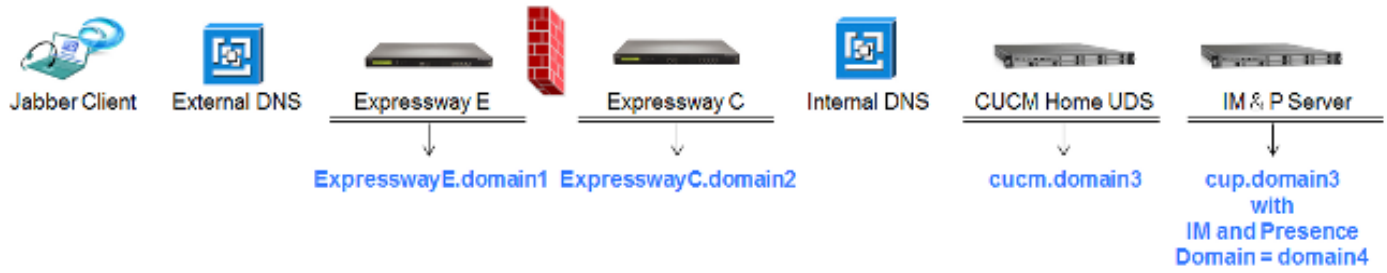
Este documento não se restringe a versões de software e hardware específicas.

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

# Configurar

Use as informações descritas nesta seção para configurar o VCS.

## Diagrama de Rede

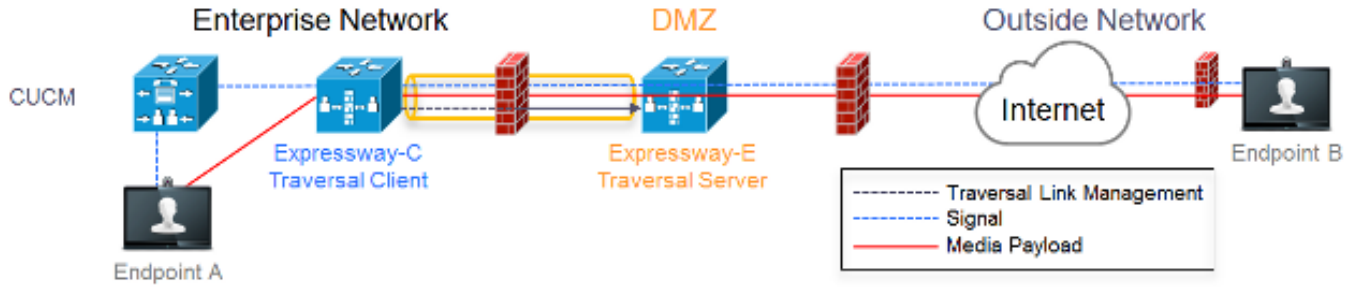



Este é um breve resumo dos diferentes domínios:

- **domain1 - este é o domínio de borda usado pelo cliente para descobrir a localização do servidor de borda e pelo qual ele descobre o serviço de dados do usuário (UDS).**
- **domain2 e domain3 - usados na descoberta de servidores.**
- **domain4 - este é o domínio de mensagens instantâneas e de presença (IM&P) usado pelo tráfego da plataforma extensível de comunicações (XCP) e do protocolo extensível de Mensagem e Presença (XMPP).**

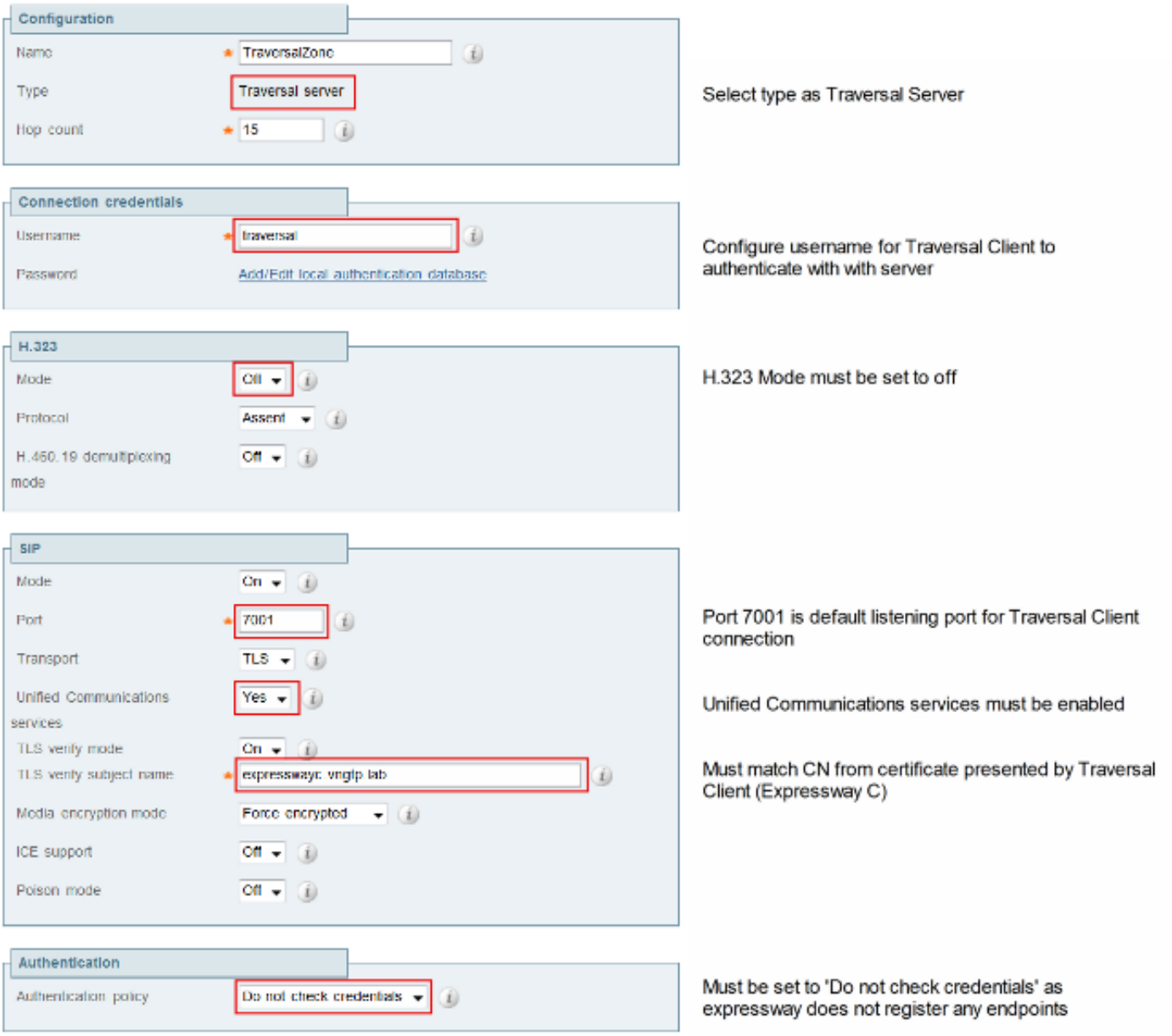
## Zona transversal

A zona transversal consiste no servidor transversal (**Expressway E**), localizado na zona desmilitarizada (DMZ) e no cliente transversal (**Expressway C**), localizado dentro da rede:



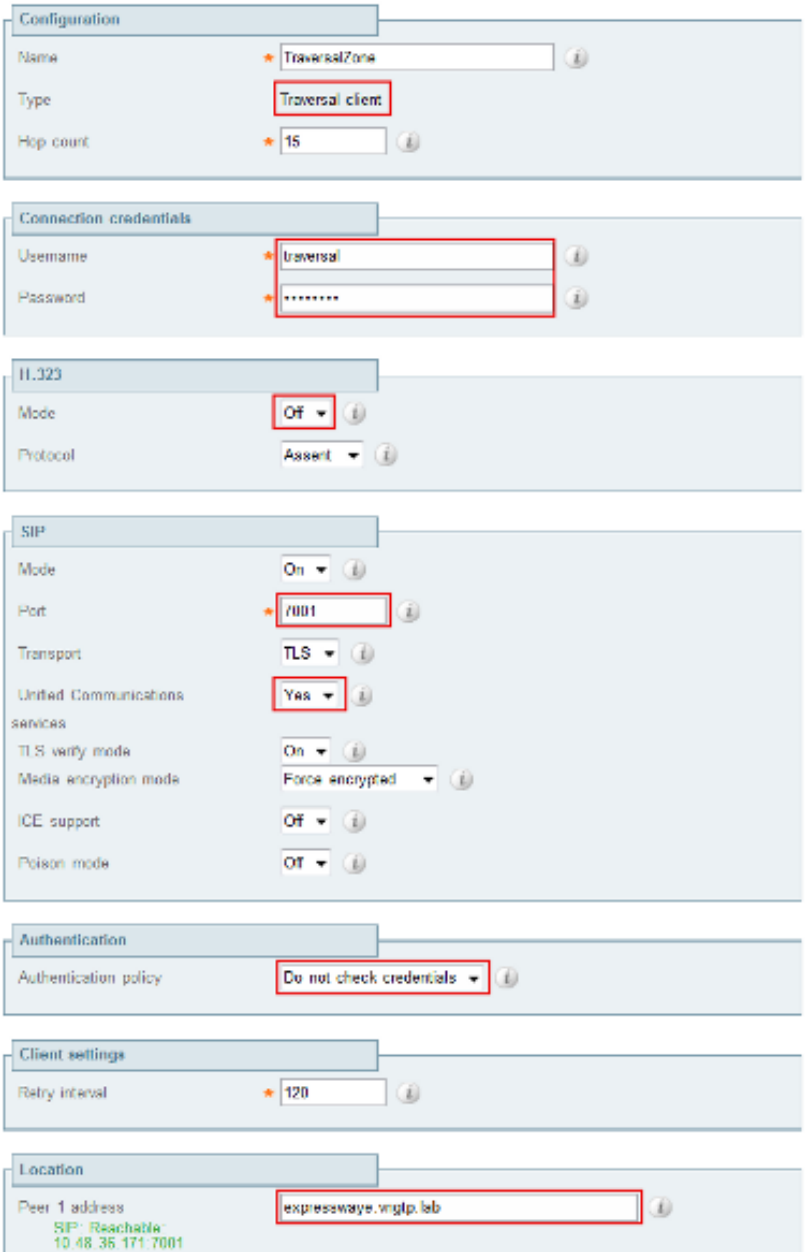

## Servidor de transversal

O servidor transversal está localizado na configuração de zona da Expressway E:




## Cliente transversal

O cliente transversal está localizado na configuração de zona da Expressway C:




Select Traversal Client as Type

Configure same username and password as added on the Traversal Server (Expressway E)

H.323 mode must be set to off

Destination port Traversal Server is listening on

Unified Communications must be enabled

Must be set to 'Do not check credentials' as expressway does not register any endpoints

Must be FQDN
Must be DNS resolvable
Must match CN from certificate presented by Traversal Server (Expressway E)

## Domínio de serviços de voz

O usuário sempre faz logon com **userid@domain4**, já que não deve haver nenhuma diferença na experiência do usuário quando dentro ou fora do ambiente do usuário. Isso significa que se **domain1 é diferente de domain4**, você deve configurar o domínio de serviços de voz no cliente Jabber. Isso ocorre porque a parte do domínio do logon é usada para descobrir os serviços de borda de colaboração pelo uso de pesquisas no registro de serviço (SRV).

O cliente executa uma consulta de registro SRV no sistema de nomes de domínio (DNS) por **_collab-edge._tls.<domain>**. Isso significa que, quando o domínio da ID de logon do usuário é diferente do domínio da Expressway E, você deve usar a configuração do domínio de serviço de voz. O Jabber usa essa configuração para descobrir a borda de colaboração e o UDS.

Existem várias opções que você pode usar para realizar essa tarefa:

1. Adicione-o como um parâmetro quando você instalar o Jabber com a Media Services Interface (MSI):

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

2. Navegue até **%APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config** e crie este **arquivo jabber-config-user.xml no diretório:**

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

**Note**: Esse método é experimental e não tem suporte oficial da Cisco.

3. Edite o **arquivo jabber-config.xml.** Isso exige que o cliente faça o logon internamente primeiro. O Jabber Config File Generator pode ser usado para:

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

4. Além disso, clientes Jabber móveis podem ser configurados para o domínio de serviços de voz de início, então não precisam fazer logon internamente primeiro. Isto é explicado no guia de instalação e implantação no capítulo Descoberta de serviço. Você deve criar uma URL de configuração que o usuário precisa clicar:

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

**Note**: É necessário usar o domínio de serviços de voz porque você deve assegurar que executou a pesquisa nos registos SRV de borda de colaboração para o domínio externo (**domain1**).

## Registros de DNS

Esta seção descreve as definições de configuração dos registros de DNS internos e externos.

### Externos

| Tipo | Entrada | Resolve em |
|---|---|---|
| Registro SRV | _collab-edge._tls.domain1 | ExpresswayE.domain1 |
| Um registro | ExpresswayE.domain1 | O endereço IP da Expressway E |

Éimportante notar que:

- Os registros SRV retornam um nome de domínio totalmente qualificado (FQDN) e não um endereço IP.
- O FQDN retornado pelos registros SRV deve corresponder ao FQDN real da Expressway-E ou o destino do registro SRV é um CNAME e os pontos de alias para um servidor dentro do mesmo domínio da Expressway-E (ID de Cisco bug pendente CSCuo82526).

Isso é necessário porque a Expressway-E define um cookie no cliente com domínio próprio (**domain1**) e se isto não corresponde ao domínio retornado pelo FQDN, o cliente não aceita isso. A ID do Cisco bug CSCuo83458 está em aberto como um aprimoramento para esse cenário.

### Interno

| Tipo | Entrada | Resolve em |
|---|---|---|
| Registro SRV | _cisco-uds._tcp.domain1 | cucm.domain3 |
| Um registro | cucm.domain3 | Endereço IP CUCM |

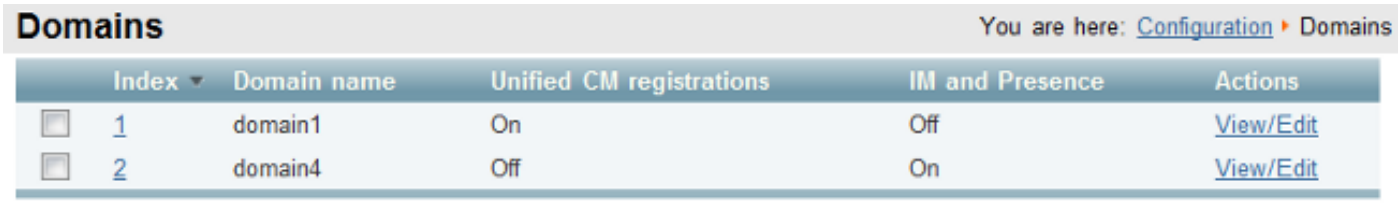
Devido ao domínio de serviços de voz estar definido como **domain1**, o Jabber incorpora **domain1 na URL transformada da descoberta de configuração de borda de colaboração (get edge_config)**. Uma vez recebida, a Expressway-C executa uma consulta de registro no UDS do SRV por **domain1 e retorna os registros na mensagem 200 OK.**

| Tipo | Entrada | Resolve em |
|---|---|---|
| SRV | _cisco-uds._tcp.domain4 | cucm.domain3 |
| Um registro | cucm.domain3 | Endereço IP CUCM |

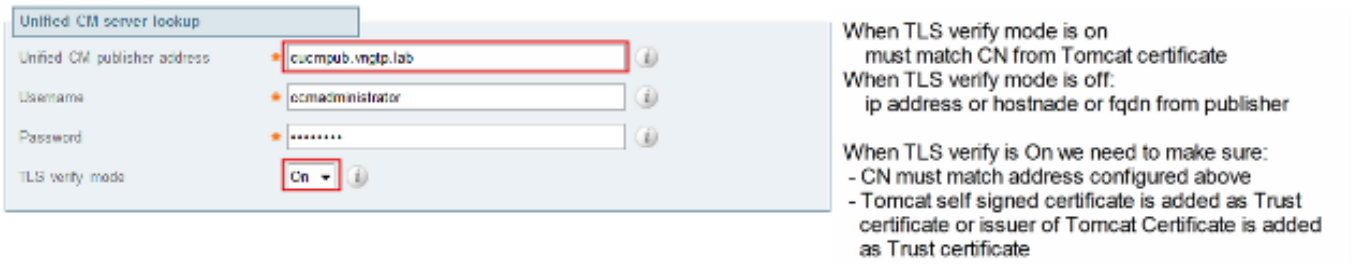
Quando o cliente está na rede, a descoberta de registro no UDS do SRV é necessária para o **domain4**.

## Domínios SIP na Expressway-C

Você deve adicionar esses domínios do Session Initiation Protocol (SIP) à Expressway-C e ativá-los para ARM:




## Nome de host/Endereço IP dos servidores CUCM




Ao configurar os servidores Cisco Unified Communications Manager (CUCM), existem dois cenários:

- Se a Expressway-C (**domain2**) estiver configurada no mesmo domínio que o servidor CUCM (**domain3**), você pode configurar os servidores CUCM (**Sistema > Servidores**) com:

  O endereço IPO nome de hostO FQDN
- Se a Expressway-C (**domain2**) estiver configurada em um domínio diferente do servidor CUCM (**domain3**), então você deve configurar os servidores CUCM com:

  O endereço IPO FQDN

Isso é necessário porque quando a Expressway-C descobre os servidores CUCM e o nome de host é retornado, ela executa uma pesquisa de DNS por **hostname.domain2**, que não funciona se **domain2 e domain3 são diferentes.**

## Certificados

Além dos requisitos de certificado geral, algumas coisas devem ser adicionadas aos nomes alternativos de assunto (SAN, Subject Alternate Names) dos certificados:

- Expressway-C

  Os aliases de nó de bate-papo configurados nos servidores IM&P devem ser adicionados. Isso só é necessário para implantações em federação do Unified Communications XMPP que pretendam usar a segurança de camada de transporte (TLS) e o bate-papo em grupo. Isso é adicionado automaticamente à solicitação de assinatura de certificado (CSR, Certificate Signing Request), desde que ele já tenha descoberto os servidores IM&P.

  Os nomes, no formato FQDN, de todos os perfis de segurança por telefone no CUCM configurados com TLS criptografado e usados em dispositivos que exigem acesso remoto devem ser adicionados.
  **Note**: O formato FQDN é apenas necessário quando sua autoridade de certificação (CA) não permite a sintaxe de nome de host no SAN.
- Expressway-E

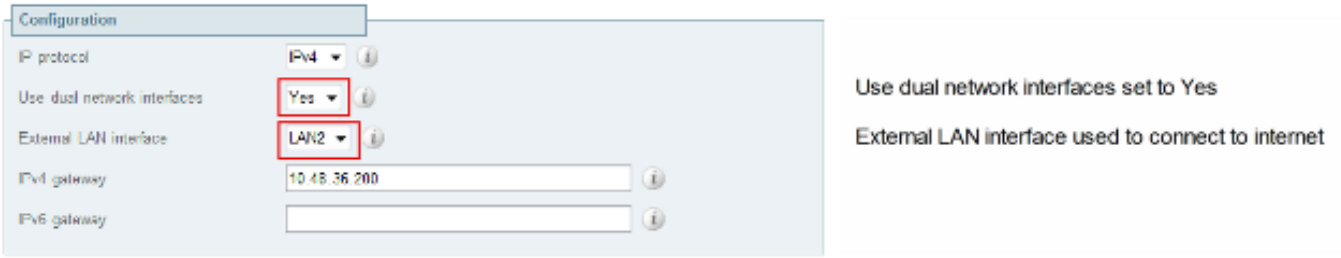
  O domínio usado para descoberta de serviços (**domain1**) deve ser adicionado. Domínios em federação XMPP.Os aliases de nó de bate-papo configurados nos servidores IM&P devem ser adicionados. Isso só é necessário para implantações em federação do Unified Communications XMPP que pretendam usar TLS e bate-papo em grupo. Eles podem ser copiados da CSR gerada na Expressway-C.

## NIC dupla

Esta seção descreve as definições de configuração quando placas de interface de rede (NICs) duplas são usadas.

### Duas Interfaces

Ao configurar a Expressway-E para usar interfaces de rede duplas, é importante assegurar que as duas interfaces estejam configuradas e sejam usadas.



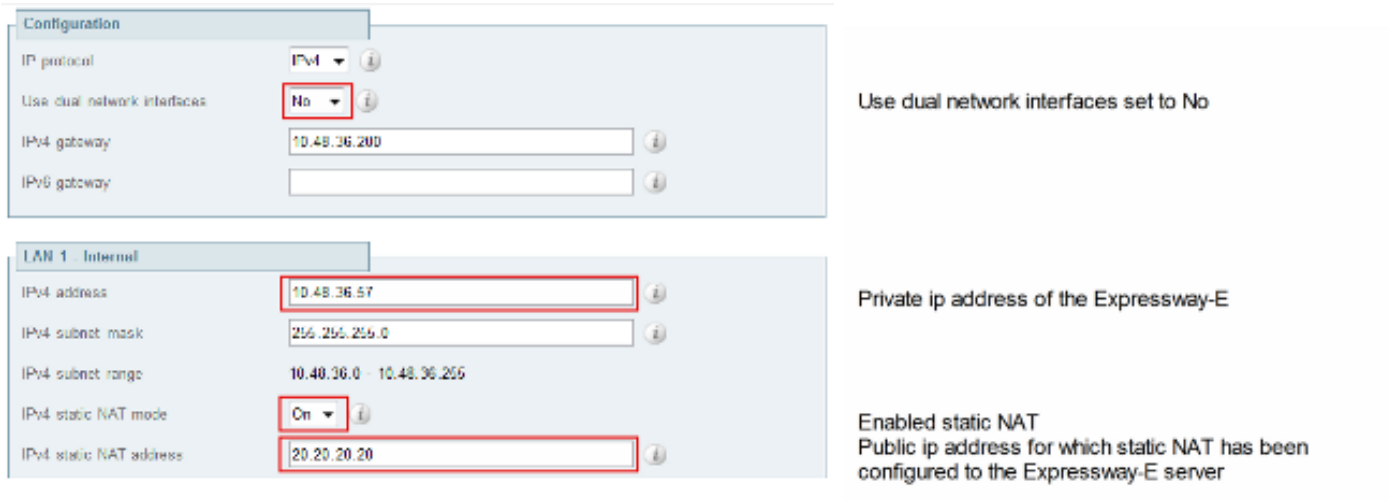

Quando a **opção Usar interfaces de rede duplas** é configurada com um valor de **Sim**, o Expressway-E só escuta na interface interna para comunicação XMPP com o Expressway-C. Portanto, você deve garantir que essa interface esteja configurada e funcione corretamente.

### Uma Interface - endereço IP público

Quando apenas uma interface é usada e você configura a Expressway-E com um endereço IP público, nenhuma consideração especial é necessária.

### Uma Interface - endereço IP privado

Quando apenas uma interface é usada e você configura a Expressway-E com um endereço IP privado, você também deve configurar o endereço estático da Network Address Translation (NAT):




Nesta situação, é importante assegurar que:

- A Expressway-C tem permissão do firewall para enviar tráfego ao endereço IP público. Isso é conhecido como *reflexão de NAT*
- A zona do cliente transversal na Expressway-C é configurada com um endereço de mesmo nível que corresponde ao endereço NAT estático na Expressway-E, que é **20.20.20.20 neste caso.**

**Tip**: Mais informações sobre implantações de redes avançadas estão disponíveis no **Apêndice 4 do** Guia de implantação da configuração básica (controle do Expressway) do Cisco TelePresence Video Communication Server.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Alguns cenários específicos são cobertos nesta seção, mas você também pode usar o Analisador de soluções de colaboração que oferece uma visão detalhada de todas as comunicações para tentativas de logon ARM e informações para a solução de problemas com base em seus registros de diagnóstico.

## Zona transversal

Quando o endereço de mesmo nível é configurado como um endereço IP ou não corresponde ao nome comum (CN), isso aparece nos registros:

```
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"
```

Quando a senha está incorreta, você vê isso nos registros da Expressway-E:

```
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"
```

## NIC dupla

Quando a NIC dupla está ativada, mas a segunda interface não é usada nem está conectada, a Expressway-C não pode se conectar com a Expressway-E para a comunicação XMPP na porta 7400 e os registros da Expressway-C mostram isso:

```
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

Quando o FQDN retornado pela pesquisa de registro SRV para borda de colaboração não corresponde ao FQDN configurado na Expressway-E, os registros do Jabber mostram esse erro:

```
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
```

Nos registros de diagnóstico da Expressway-E, você pode ver para qual domínio o cookie está

definido na mensagem HTTPS:

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

## Domínios SIP

Quando os domínios SIP necessários não são adicionados à Expressway-C, a Expressway-E não aceita mensagens desse domínio e nos registros de diagnóstico você vê uma mensagem **403 Forbidden** enviada para o cliente:

```
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"
```