Configuration Example: Mobile and Remote Access through Expressway/VCS in a multi−domain deployment

Document ID: 117811

Contributed by Kristof Van Coillie and Philip Smeuninx, Cisco TAC Engineers.

Aug 07, 2014

Contents

Introduction

This document describes how to configure the Cisco TelePresence Video Communication Server (VCS) for Mobile Remote Access (MRA) when multiple domains are used.

The MRA set up when there is only one domain is relatively straightforward, and you can follow the steps that are documented in the deployment guide. When the deployment involves multiple domains, it becomes more complex. This document is not a configuration guide, but it describes the important aspects when multiple domains are involved. The main configuration is documented in the Cisco TelePresence Video Communication Server (VCS) Deployment Guide.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

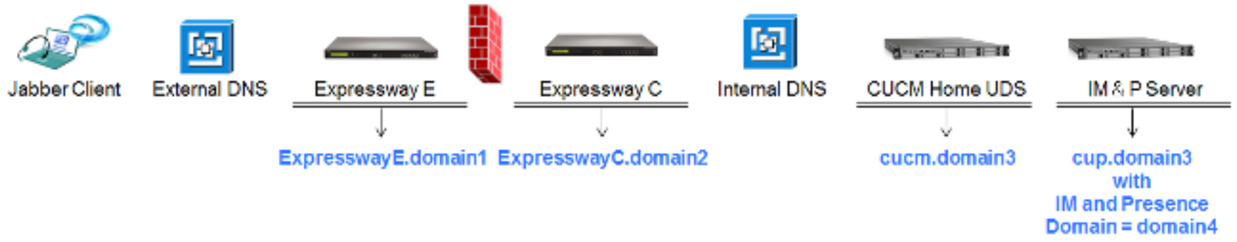
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Use the information that is described in this section in order to configure the VCS.

Network Diagram

The only required difference when you use multiple domains instead of only one is that the domain from the servers in the Cisco Unified Communications Manager (CUCM) cluster and the Cisco Unified Presence (CUP) server must be the same, and the rest can be different:

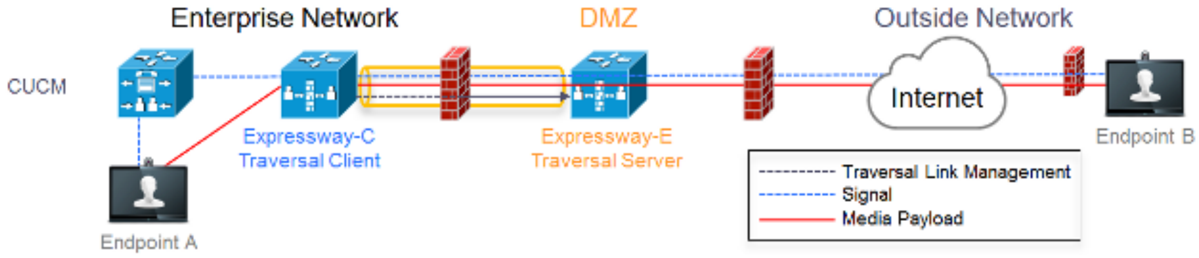


Here is a short overview of the different domains:

- ***domain1*** − This is the Edge domain that is used by the client in order to discover the location of the Edge server and through which it discovers the User Data Service (UDS).
- ***domain2 and domain3*** − This is used for server discovery.
- ***domain4*** − This is the Instant Messaging and Presence (IM&P) domain that is used by Extensible Calibration Protocol (XCP) and Extensible Messaging and Presence Protocol (XMPP) traffic.

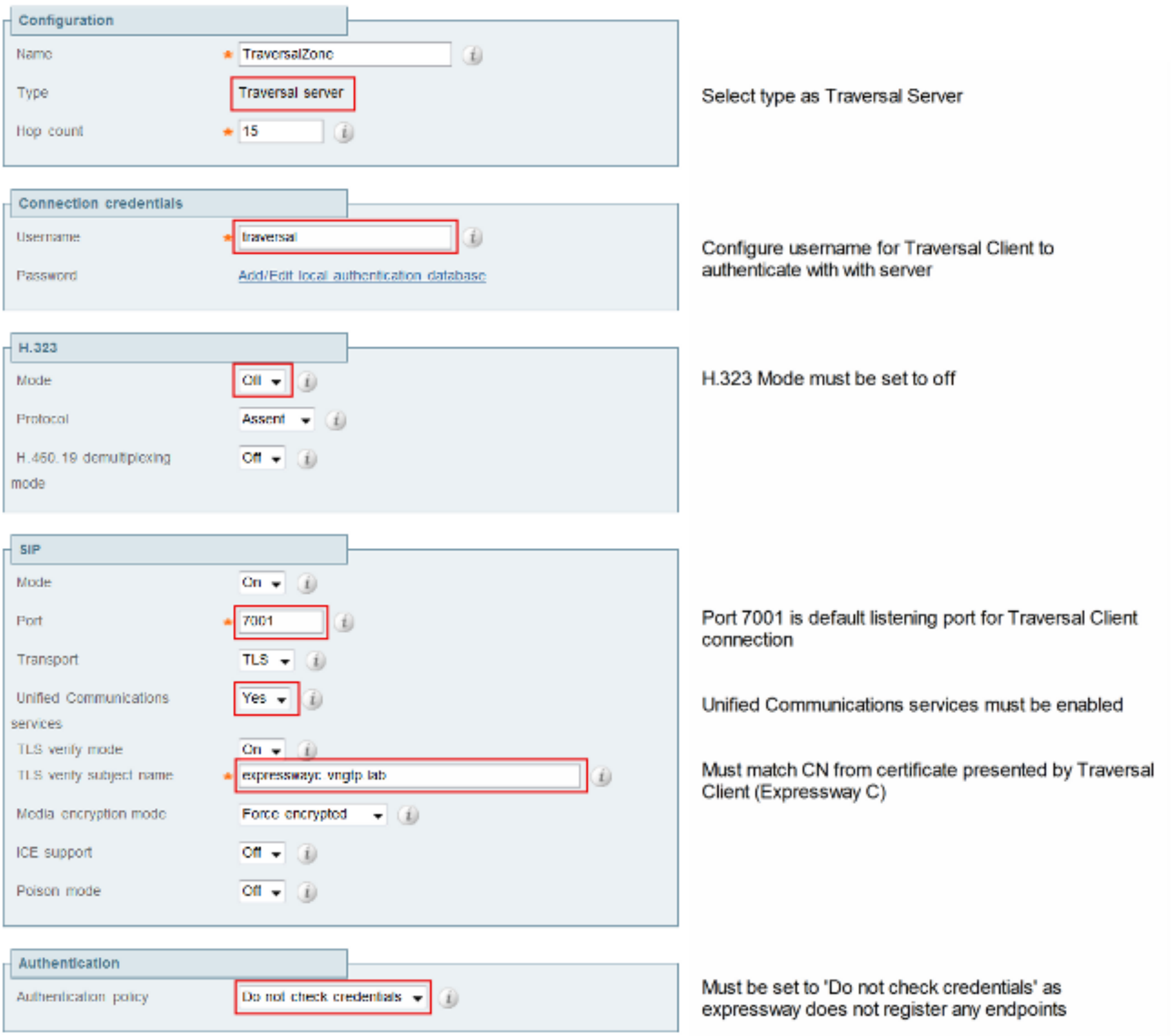
Traversal Zone

The Traversal Zone consists of the Traversal Server (***expresswayE***), located in the De−Militarized Zone (DMZ), and the Traversal Client (***expresswayC***), located inside the network:



Traversal Server

The Traversal Server is located in the zone configuration on the Expressway E:



Configuration

Name	* TraversalZone
Type	Traversal server
Hop count	* 15

Select type as Traversal Server

Connection credentials

Username	* traversal
Password	Add/Edit local authentication database

Configure username for Traversal Client to authenticate with with server

H.323

Mode	Off
Protocol	Assent
H.460.19 demultiplexing mode	Off

H.323 Mode must be set to off

SIP

Mode	On
Port	* 7001
Transport	TLS
Unified Communications services	Yes
TLS verify mode	On
TLS verify subject name	* expresswayc.vngtp.lab
Media encryption mode	Force encrypted
ICE support	Off
Poison mode	Off

Port 7001 is default listening port for Traversal Client connection

Unified Communications services must be enabled

Must match CN from certificate presented by Traversal Client (Expressway C)

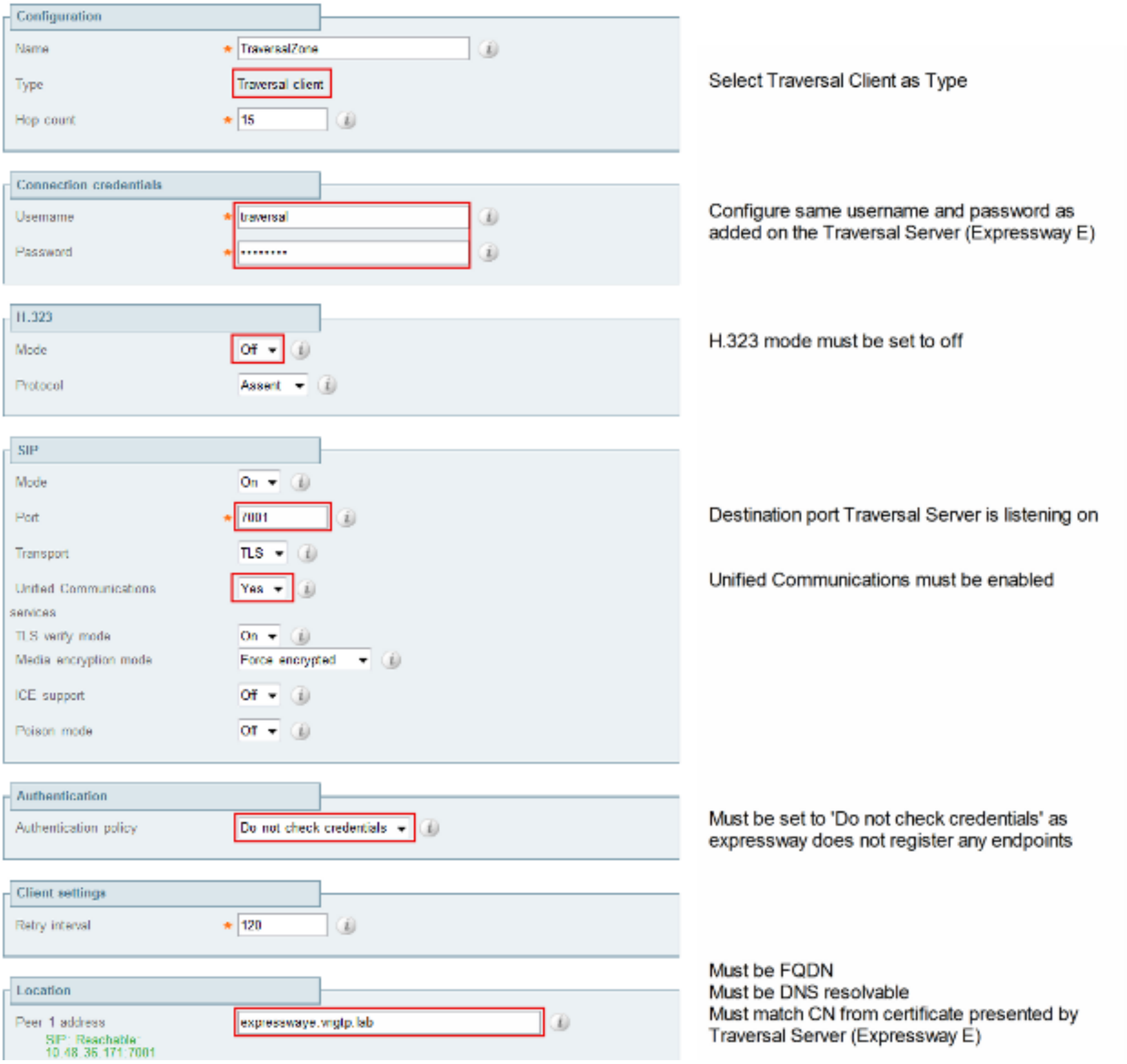
Authentication

Authentication policy	Do not check credentials

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

Traversal Client

The Traversal Client is located in the zone configuration on the Expressway C:



Configuration

Name * TraversalZone

Type Traversal client

Hop count * 15

Select Traversal Client as Type

Connection credentials

Username * traversal

Password * ••••••••

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

H.323

Mode Off

Protocol Assent

H.323 mode must be set to off

SIP

Mode On

Port * 7001

Destination port Traversal Server is listening on

Transport TLS

Unified Communications services Yes

Unified Communications must be enabled

TLS verify mode On

Media encryption mode Force encrypted

ICE support Off

Poison mode Off

Authentication

Authentication policy Do not check credentials

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

Client settings

Retry interval * 120

Location

Peer 1 address expresswaye.vngtp.lab

SIP: Reachable: 10.48.36.171:7001

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

Voice Services Domain

The user always logs in with ***userid@domain4***, as there should be no difference in user experience when inside or outside. This means that if ***domain1*** is different from ***domain4***, you must configure the voice services domain in the Jabber client. This is because the domain portion of the login is used in order to discover the Collaboration Edge services using Service (SRV) record lookups.

The client performs a Domain Name System (DNS) SRV record query for ***_collab−edge._tls.<domain>***. This implies that when the domain from the login user ID is different than the domain from the Expressway E, you must use the voice service domain configuration. Jabber uses this configuration in order to discover the Collaboration Edge and the UDS.

There are three options that you can use in order to complete this task:

1. Add this as a parameter when you install Jabber via the Media Services Interface (MSI):

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

2. Navigate to ***%APPDATA%*** > ***Cisco*** > ***Unified Communications*** > ***Jabber*** > ***CSF*** > ***Config***, and create this ***jabber−config−user.xml*** file in the directory:

```
<?xml version="1.0" encoding="utf-8"?>
<config version ="1.0">
```

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

Note: This method is experimental only and not officially supported by Cisco.

3. Edit the ***jabber−config.xml*** file. This requires that the client logs in internally first. The Jabber Config File Generator can be used for this:

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

Note: It is required to use the voice services domain because you must ensure that you perform the lookup for the Collaboration Edge SRV records for the outside domain (***domain1***).

DNS Records

This section describes the configuration settings for the external and internal DNS records.

External

Type	***Entry***	***Resolves To***
SRV record	_collab−edge._tls.domain1	ExpresswayE.domain1
A record	ExpresswayE.domain1	IP address ExpresswayE

It is important to note that:

- The SRV records return a Fully Qualified Domain Name (FQDN) and not an IP address.
- The FQDN that is returned by the SRV records must match the actual FQDN of the Expressway−E, or the SRV record target is a CNAME and the alias points to a server within the same domain as the Expressway−E (pending Cisco bug ID CSCuo82526).

This is required because the Expressway−E sets a cookie on the client with its own domain (***domain1***), and if this does not match with the domain that is returned by the FQDN, the client does not accept this. Cisco bug ID CSCuo83458 is opened as an enhancement for this scenario.

Internal

Type	***Entry***	***Resolves To***
SRV record	_cisco−uds._tcp.domain1	cucm.domain3
A record	cucm.domain3	IP address CUCM

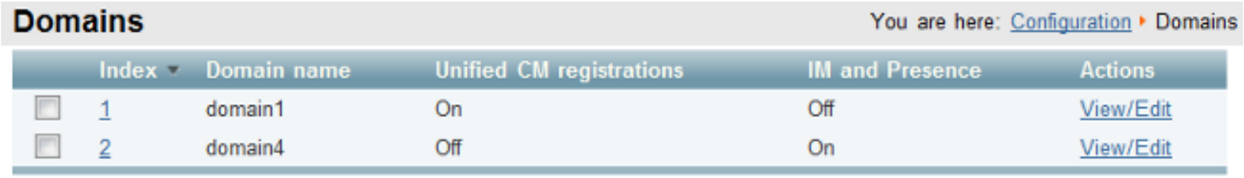
Because the voice services domain is set to ***domain1***, Jabber embeds ***domain1*** in the transformed URL for the Collaboration Edge configuration discovery (***get edge_config***). Once received, the Expressway−C performs an SRV UDS record query for ***domain1*** and returns the records in the ***200 OK*** message.

Type	***Entry***	***Resolves To***
SRV	_cisco−uds._tcp.domain4	cucm.domain3
A record	cucm.domain3	IP address CUCM

When the client is on−net, the SRV UDS record discovery is required for ***domain4***.

SIP Domains on Expressway−C

You must add these Session Initiation Protocol (SIP) domains on the Expressway−C and enable them for MRA:

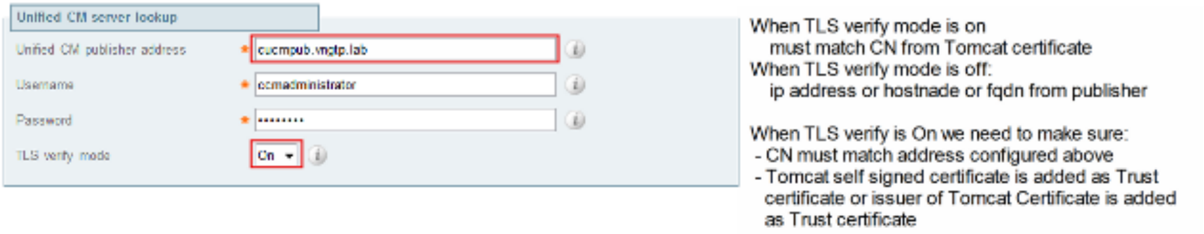


Domains

You are here: Configuration ▸ Domains

	Index ▾	Domain name	Unified CM registrations	IM and Presence	Actions
□	1	domain1	On	Off	View/Edit
□	2	domain4	Off	On	View/Edit

Hostname/IP Address CUCM Servers



Unified CM server lookup

Unified CM publisher address *	cucmpub.vngtp.lab
Username *	ccmadministrator
Password *	••••••••
TLS verify mode	On

When TLS verify mode is on
must match CN from Tomcat certificate
When TLS verify mode is off:
ip address or hostnade or fqdn from publisher

When TLS verify is On we need to make sure:
- CN must match address configured above
- Tomcat self signed certificate is added as Trust certificate or issuer of Tomcat Certificate is added as Trust certificate

When you configure the CUCM servers, there are two scenarios:

- If your Expressway−C (***domain2***) is configured with the same domain as your CUCM server (***domain3***), you can configure your CUCM servers (***System*** > ***Servers***) with:
  - ♦ The IP address
  - ♦ The hostname
  - ♦ The FQDN
- If the Expressway−C (***domain2***) is configured with a different domain than the CUCM server (***domain3***), then you must configure the CUCM servers with:
  - ♦ The IP address
  - ♦ The FQDN

This is required because when the Expressway−C discovers the CUCM servers and the hostname is returned, it performs a DNS lookup for ***hostname.domain2***, which does not work if ***domain2*** and ***domain3*** are different.

Certificates

Aside from the general certificate requirements, a few things must be added to the Subject Alternate Names (SAN) of the certificates:

- Expressway−C
  - ♦ The chat node aliases that are configured on the IM&P Servers must be added. This is only required for the Unified Communications XMPP federation deployments that intend to use both Transport Layer Security (TLS) and group chat. This is added automatically to the Certificate Signing Request (CSR), provided it has discovered the IM&P servers already.
  - ♦ The names, in FQDN format, of all of the phone security profiles in the CUCM that are

configured for encrypted TLS and are used for devices that require remote access must be added.

Note: The FQDN format is only required when your Certificate Authority (CA) does not allow hostname syntax in the SAN.

- Expressway−E
    - ♦ All of the domains that are configured for Unified Communications (***domain1*** and ***domain4***) must be added.

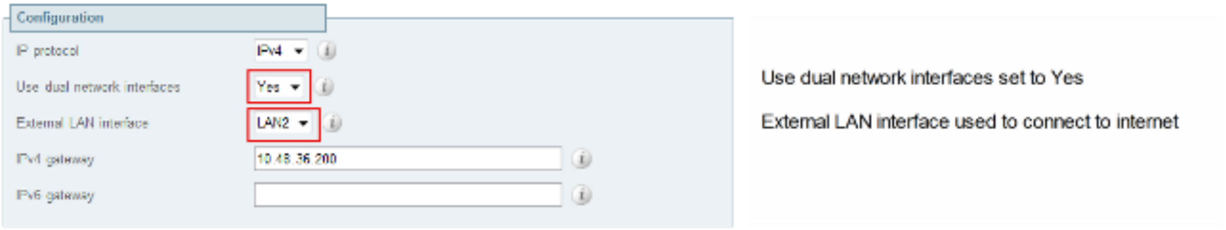
      Note: For Jabber clients, the FQDN of the Expressway−E is sufficient, as they can match the domain from the FQDN. This is not yet supported by Traffic Class (TC) endpoints; hence the recommendation to add them. The ***domain4*** is needed if you do not want to receive a popup on the client−side for Jabber.
    - ♦ The chat node aliases that are configured on the IM&P Servers must be added. This is only required for Unified Communications XMPP federation deployments that intend to use both TLS and group chat. These can be copied from the CSR that is generated on the Expressway−C.

Dual NIC

This section describes the configuration settings when dual Network Interface Cards (NICs) are used.

Two Interfaces

When you configure the Expressway−E in order to use dual network interfaces, it is important to ensure that both interfaces are configured and used.



Configuration

IP protocol: IPv4

Use dual network interfaces: Yes

External LAN interface: LAN2

IPv4 gateway: 10.48.36.200

IPv6 gateway:

Use dual network interfaces set to Yes

External LAN interface used to connect to internet

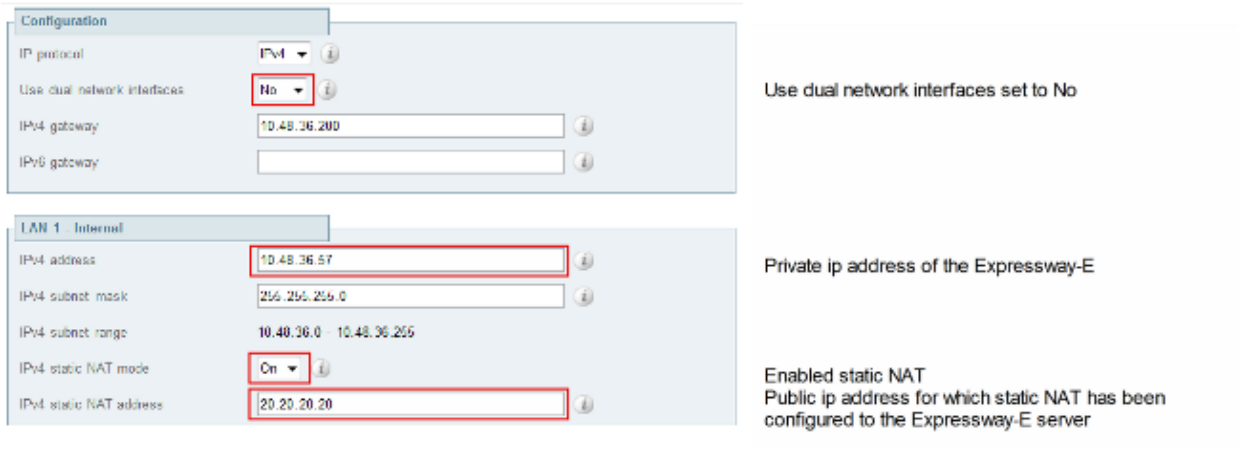
When the ***Use dual network interfaces*** is configured with a value of ***Yes***, the Expressway−E only listens on the internal interface for XMPP communication with the Expressway−C. Thus, you must ensure that this interface is configured and works correctly.

One Interface − Public IP Address

When only one interface is used, and you configure the Expressway−E with a public IP address, no special considerations must be taken.

One Interface − Private IP Address

When only one interface is used, and you configure the Expressway−E with a private IP address, you must configure the static Network Address Translation (NAT) address as well:



Configuration

IP protocol	IPv4
Use dual network interfaces	No
IPv4 gateway	10.48.36.200
IPv6 gateway	

LAN 1 - Internal

IPv4 address	10.48.36.57
IPv4 subnet mask	255.255.255.0
IPv4 subnet range	10.48.36.0 - 10.48.36.255
IPv4 static NAT mode	On
IPv4 static NAT address	20.20.20.20

Use dual network interfaces set to No

Private ip address of the Expressway-E

Enabled static NAT
Public ip address for which static NAT has been configured to the Expressway-E server

In this situation, it is important to ensure that:

- The Expressway−C is allowed by the firewall to send traffic to the public IP address. This is known as *NAT reflection*.
- The Traversal Client zone on the Expressway−C is configured with a peer address that matches the static NAT address on the Expressway−E, which is ***20.20.20.20*** in this case.

Tip: More information about advanced network deployments is available in ***Appendix 4*** of the Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Traversal Zone

When the peer address is configured as an IP address or the peer address does not match the Common Name (CN), you see this in the logs:

```
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"
```

When the password is incorrect, you see this in the Expressway−E logs:

```
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?
```

Dual NIC

When Dual−NIC is enabled but the second interface is not used or connected, the Expressway−C cannot connect to the Expressway−E for XMPP communication on Port 7400, and the Expressway−C logs show this:

```
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

When the FQDN that is returned by the SRV record lookup for Collaboration Edge does not match the FQDN that is configured on the Expressway−E, the Jabber logs show this error:

```
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
```

In the diagnostic logs for the Expressway−E, you can see for which domain the cookie is set in the HTTPS message:

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

SIP Domains

When the required SIP domains are not added on the Expressway−C, the Expressway−E does not accept messages for this domain and in the diagnostic logs you see a ***403 Forbidden*** message that is sent to the client:

```
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"
```