다중 도메인 구축에서 Expressway/VCS를 통해 모바일 및 원격 액세스 구성

목차

소개

이 문서에서는 여러 도메인을 사용할 때 MRA(Mobile Remote Access)용 Cisco TelePresence VCS(Video Communication Server)를 구성하는 방법에 대해 설명합니다.

도메인이 하나만 있을 때 설정된 MRA는 비교적 간단하며 구축 가이드에 설명된 단계를 수행할 수 있습니다.구축에 여러 도메인이 포함되는 경우 구축이 더욱 복잡해집니다.이 문서는 컨피그레이션 가이드가 아니지만 여러 도메인이 관련된 중요한 사항에 대해 설명합니다.기본 컨피그레이션은 Cisco TelePresence VCS(Video Communication Server) 구축 가이드에 설명되어 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

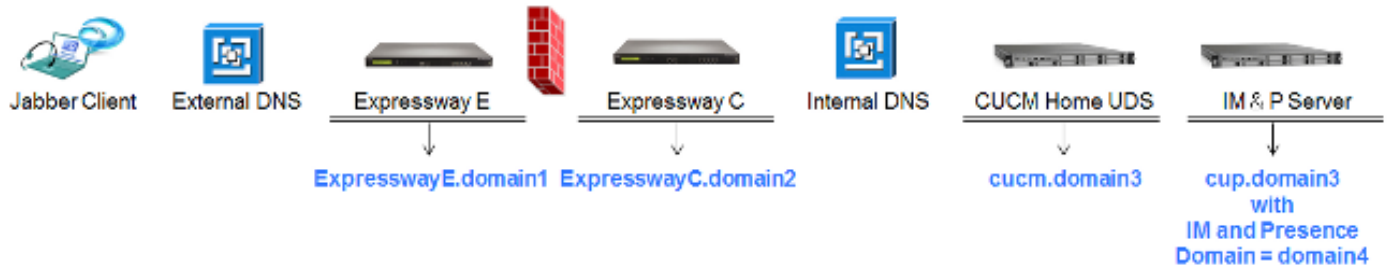
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

VCS를 구성하려면 이 섹션에 설명된 정보를 사용하십시오.

네트워크 다이어그램

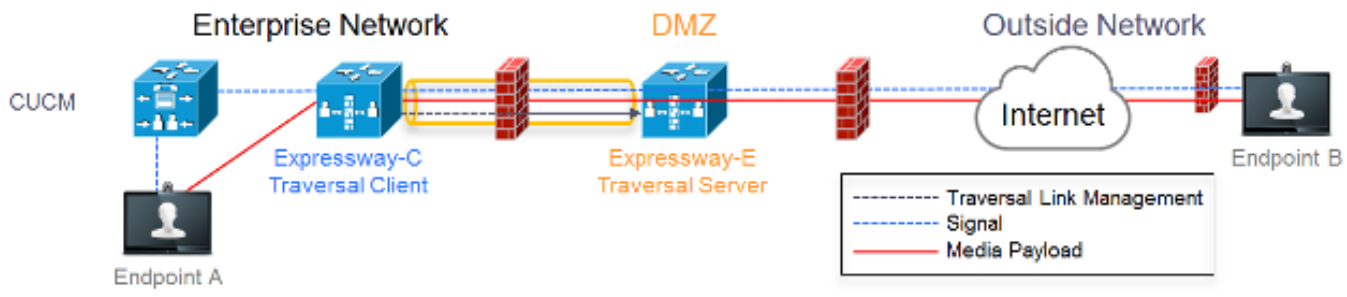


다음은 서로 다른 도메인에 대한 간략한 개요입니다.

- **domain1** - 에지 서버의 위치를 검색하고 UDS(사용자 데이터 서비스)를 검색하는 데 클라이언트에서 사용하는 에지 도메인입니다.
- **domain2 및 domain3** - 서버 검색에 사용됩니다.
- **domain4** - XCP(Extensible Communications Platform) 및 XMPP(Extensible Messaging and Presence Protocol) 트래픽에서 사용되는 IM&P(Instant Messaging and Presence) 도메인입니다.

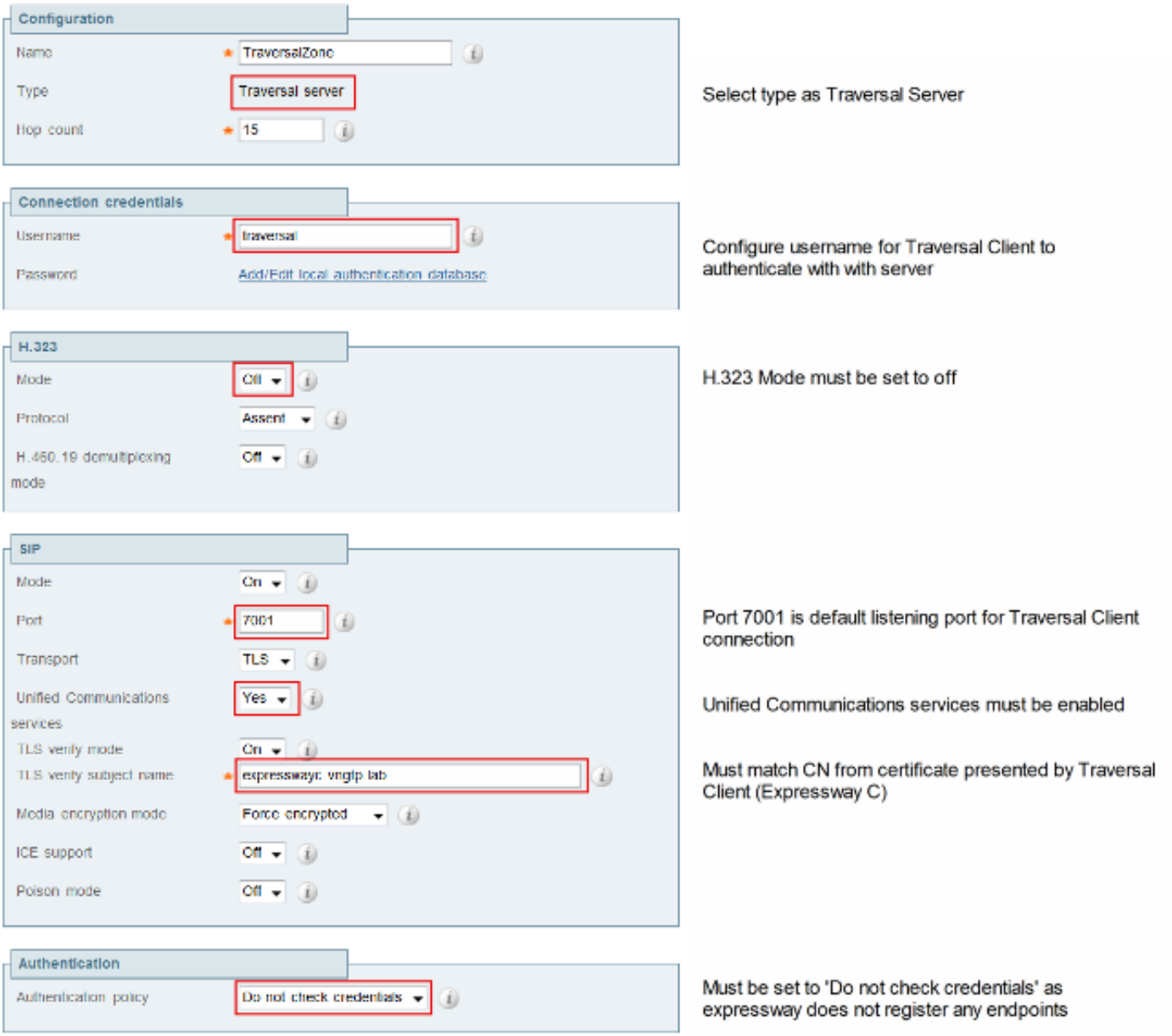
접근 영역

Traversal Zone은 DMZ(**De**-Demarized Zone)에 있는 Traversal Server(ExpresswayE)와 네트워크 내부에 있는 Traversal Client(**expresswayC**)로 구성됩니다.



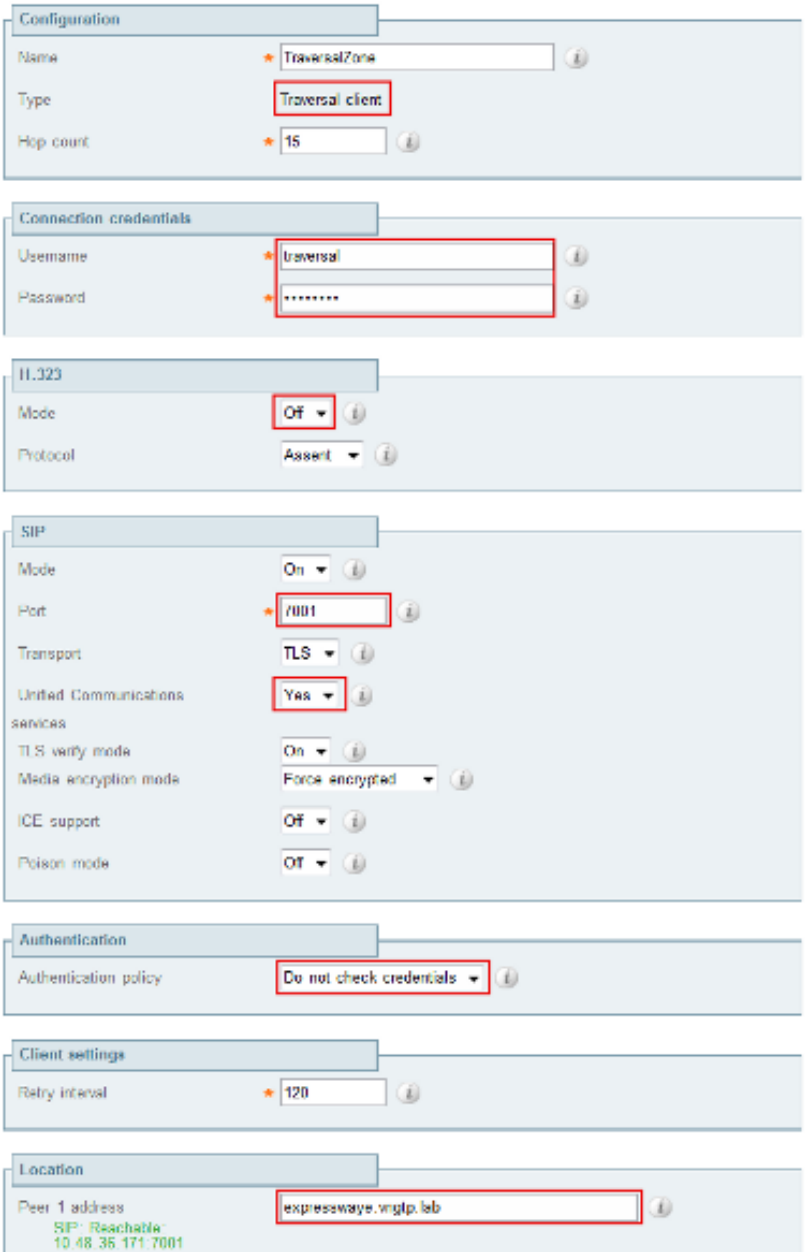
접근 서버

Traversal Server는 Expressway E의 영역 컨피그레이션에 있습니다.



접근 클라이언트

Traversal Client는 Expressway C의 영역 컨피그레이션에 있습니다.



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)

음성 서비스 도메인

내부 또는 외부에서 사용자 환경에 차이가 없으므로 사용자는 항상 **userid@domain4**으로 로그인합니다.즉, **domain1**이 **domain4**와 다른 경우 Jabber 클라이언트에서 음성 서비스 도메인을 구성해야 합니다.서비스(SRV) 레코드 조회를 사용하여 Collaboration Edge 서비스를 검색하기 위해 로그인의 도메인 부분이 사용되기 때문입니다.

클라이언트는 **_collab-edge._tls.<domain>**에 대해 DNS(Domain Name System) SRV 레코드 쿼리를 **수행합니다**.즉, 로그인 사용자 ID의 도메인이 Expressway E의 도메인과 다른 경우 음성 서비스 도메인 구성을 사용해야 합니다.Jabber는 이 컨피그레이션을 사용하여 Collaboration Edge 및 UDS를 검색합니다.

이 작업을 완료하기 위해 사용할 수 있는 여러 옵션이 있습니다.

1. MSI(Media Services Interface)를 통해 Jabber를 설치할 때 이 매개 변수를 매개 변수로 추가합니다.

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

2. %APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config로 이동하고 다음 디렉토리에 jabber-config-user.xml 파일을 만듭니다.

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

참고:이 방법은 실험적인 방법이며 Cisco에서 공식적으로 지원하지 않습니다.

3. jabber-config.xml 파일을 편집합니다.이렇게 하려면 클라이언트가 먼저 내부적으로 로그인해야 합니다.Jabber Config File Generator를 사용할 수 있습니다.

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

4. 또한 모바일 Jabber 클라이언트는 먼저 내부적으로 로그인할 필요가 없도록 Voice Services Domain을 사용하여 구성할 수 있습니다.이는 서비스 검색 장의 구축 및 설치 가이드에서 설명합니다.사용자가 클릭해야 하는 컨피그레이션 URL을 생성해야 합니다.

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

참고:외부 도메인(**domain1**)에 대해 Collaboration Edge SRV 레코드 조회를 수행해야 하므로 음성 서비스 도메인을 사용해야 합니다.

DNS 레코드

이 섹션에서는 외부 및 내부 DNS 레코드의 컨피그레이션 설정에 대해 설명합니다.

외부

유형	항목	해결 대상
SRV 레코드	_collab-edge._tls.domain1	ExpresswayE.domain1
레코드	ExpresswayE.domain1	IP 주소 ExpresswayE

다음 사항에 유의해야 합니다.

- SRV 레코드는 IP 주소가 아닌 FQDN(Fully Qualified Domain Name)을 반환합니다.
- SRV 레코드에서 반환되는 FQDN은 Expressway-E의 실제 FQDN과 일치해야 합니다. 또는 SRV 레코드 대상은 CNAME이고 별칭은 Expressway-E와 동일한 도메인 내의 서버를 가리킵니다(보류 중인 Cisco 버그 ID CSCuo82526).

Expressway-E가 자체 도메인(**domain1**)을 사용하여 클라이언트에 쿠키를 설정하므로 이가 필요하며, FQDN에서 반환하는 도메인과 일치하지 않으면 클라이언트가 이를 허용하지 않습니다.Cisco 버그 ID CSCuo83458는 이 시나리오에 대한 향상된 기능으로 열립니다.

내부

유형	항목	해결 대상
SRV 레코드	_cisco-uds._tcp.domain1	cucm.domain3
레코드	cucm.domain3	IP 주소 CUCM

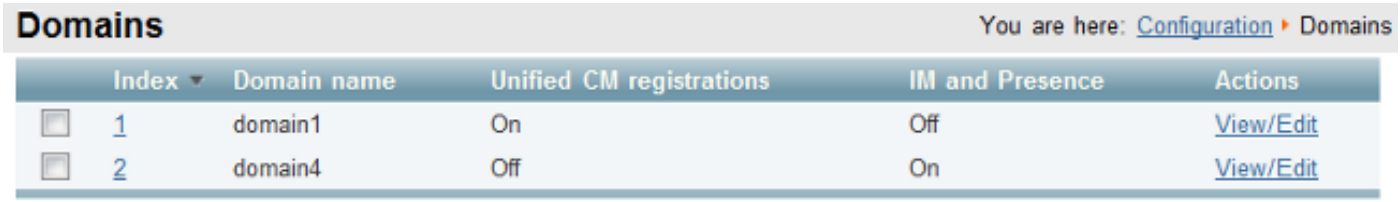
음성 서비스 도메인이 **domain1**으로 설정되어 있으므로 Jabber는 Collaboration Edge 구성 검색(**get edge_config**)을 위한 변환된 URL에 domain**1**을 포함합니다. 수신되면 Expressway-C는 **domain1**에 대해 SRV UDS 레코드 쿼리를 수행하고 **200 OK** 메시지의 레코드를 반환합니다.

유형	**항목**	**해결 대상**
SRV	_cisco-uds._tcp.domain4	cucm.domain3
레코드	cucm.domain3	IP 주소 CUCM

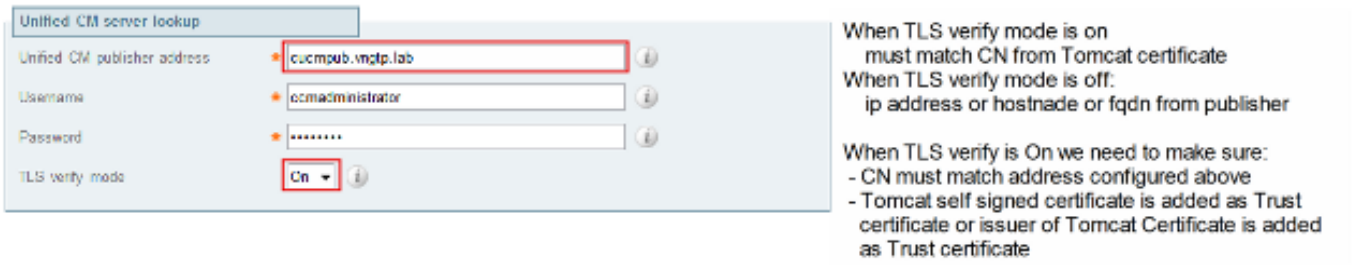
클라이언트가 온넷인 경우 **domain4**에 SRV UDS 레코드 검색이 필요합니다.

Expressway-C의 SIP 도메인

Expressway-C에 이러한 SIP(Session Initiation Protocol) 도메인을 추가하고 MRA에 대해 활성화해야 합니다.



호스트 이름/IP 주소 CUCM 서버



Cisco CUCM(Unified Communications Manager) 서버를 구성할 때 다음 두 가지 시나리오가 있습니다.

- Expressway-C(**domain2**)가 CUCM 서버(**domain3**)와 동일한 도메인으로 구성된 경우 다음을 사용하여 CUCM 서버(**시스템 > 서버**)를 구성할 수 있습니다.

  IP 주소호스트 이름FQDN
- Expressway-C(**domain2**)가 CUCM 서버(**domain3**)와 다른 도메인으로 구성된 경우 다음을 사용하여 CUCM 서버를 구성해야 합니다.

  IP 주소FQDN

Expressway-C가 CUCM 서버를 검색하고 호스트 이름이 반환되면 **domain2**와 **domain3**이 다른 경우 작동하지 않는 hostname.**domain2**에 대해 DNS 조회를 수행하므로 이가 필요합니다.

인증서

일반적인 인증서 요구 사항 외에 인증서의 SAN(Subject Alternate Names)에 몇 가지 사항을 추가해야 합니다.

- Expressway-C

  IM&P 서버에 구성된 채팅 노드 별칭을 추가해야 합니다.이는 TLS(Transport Layer Security) 및 그룹 채팅을 모두 사용하려는 Unified Communications XMPP 페더레이션 구축에만 필요합니다.IM&P 서버가 이미 검색된 경우 CSR(Certificate Signing Request)에 자동으로 추가됩니다.

  암호화된 TLS에 대해 구성되고 원격 액세스가 필요한 디바이스에 사용되는 CUCM의 모든 전화기 보안 프로파일(FQDN 형식)의 이름을 추가해야 합니다.
  참고:FQDN 형식은 CA(Certificate Authority)가 SAN에서 호스트 이름 구문을 허용하지 않는 경우에만 필요합니다.
- Expressway-E

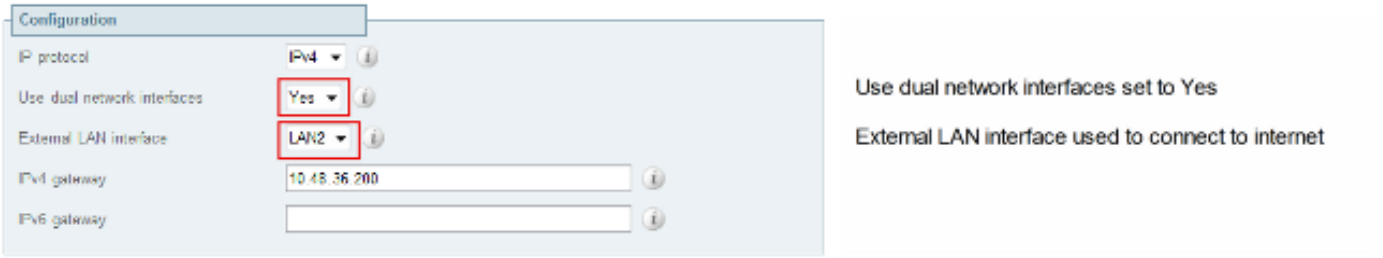
  서비스 검색에 사용되는 도메인(**domain1**)을 추가해야 합니다. XMPP 페더레이션 도메인IM&P 서버에 구성된 채팅 노드 별칭을 추가해야 합니다.TLS와 그룹 채팅을 모두 사용하려는 Unified Communications XMPP 페더레이션 구축에만 필요합니다.Expressway-C에서 생성된 CSR에서 복사할 수 있습니다.

듀얼 NIC

이 섹션에서는 듀얼 NIC(Network Interface Card)를 사용하는 경우의 컨피그레이션 설정에 대해 설명합니다.

2개의 인터페이스

이중 네트워크 인터페이스를 사용하기 위해 Expressway-E를 구성할 때 두 인터페이스가 모두 구성 및 사용되도록 하는 것이 중요합니다.



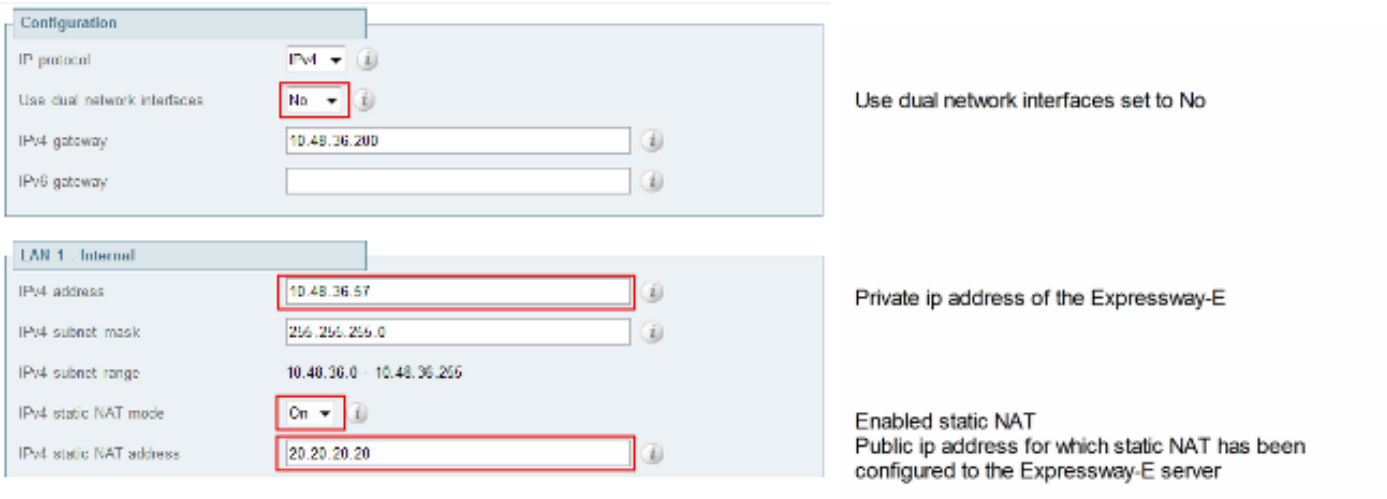
Use dual **network interfaces(듀얼 네트워크 인터페이스 사용)**가 **Yes(예)**로 구성된 경우 Expressway-E는 Expressway-C와의 XMPP 통신을 위해 내부 인터페이스에서만 수신 대기합니다. 따라서 이 인터페이스가 구성되고 올바르게 작동하는지 확인해야 합니다.

단일 인터페이스 - 공용 IP 주소

하나의 인터페이스만 사용하고 공용 IP 주소를 사용하여 Expressway-E를 구성하는 경우 특별한 고려 사항이 필요하지 않습니다.

단일 인터페이스 - 프라이빗 IP 주소

하나의 인터페이스만 사용하고 사설 IP 주소로 Expressway-E를 구성하는 경우 고정 NAT(Network Address Translation) 주소도 구성해야 합니다.



이 경우 다음을 확인하는 것이 중요합니다.

- 방화벽에서 공용 IP 주소로 트래픽을 보낼 수 있도록 Expressway-C를 허용합니다.이를 NAT 리플렉션이라고 *합니다*.
- Expressway-C의 Traversal Client 영역은 Expressway-E의 고정 NAT 주소와 일치하는 피어 주소(이 경우 **20.20.20.20**)로 구성됩니다.

  팁:고급 네트워크 구축에 대한 자세한 내용은 Cisco TelePresence Video Communication Server Basic Configuration(Control with Expressway) 구축 설명서의 **부록 4**를 참조하십시오.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

일부 특정 시나리오는 이 섹션에서 다루지만, MRA 로그인 시도를 위한 모든 통신 및 진단 로그를 기반으로 문제 해결 정보를 세부적으로 보여주는 Collaboration Solutions Analyzer를 사용할 수도 있습니다.

접근 영역

피어 주소가 IP 주소로 구성되거나 피어 주소가 CN(Common Name)과 일치하지 않는 경우 로그에 다음 내용이 표시됩니다.

```
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"
```

암호가 올바르지 않으면 Expressway-E 로그에 다음 내용이 표시됩니다.

```
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"
```

듀얼 NIC

Dual-NIC가 활성화되었지만 두 번째 인터페이스가 사용 또는 연결되지 않은 경우 Expressway-C는 포트 7400에서 XMPP 통신을 위해 Expressway-E에 연결할 수 없으며 Expressway-C 로그에는 다음이 표시됩니다.

```
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

Collaboration Edge에 대한 SRV 레코드 조회에서 반환된 FQDN이 Expressway-E에 구성된 FQDN과 일치하지 않으면 Jabber 로그에 다음 오류가 표시됩니다.

```
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
```

Expressway-E의 진단 로그에서 HTTPS 메시지에 쿠키가 설정된 도메인을 확인할 수 있습니다.

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

SIP 도메인

필요한 SIP 도메인이 Expressway-C에 추가되지 않은 경우 Expressway-E는 이 도메인에 대한 메시지를 수락하지 않으며 진단 로그에 클라이언트로 전송되는 **403 Forbidden** 메시지가 표시됩니다.

```
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"
```