

# CUCM과 통합된 Expressway를 통해 비즈니스 대 비즈니스 오디오 및 비디오 통화 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[1단계. CUCM과 Expressway-C 간의 SIP 트렁크](#)

[a. 새 SIP 트렁크 보안 프로필을 추가합니다.](#)

[b. CUCM에서 SIP 트렁크를 구성합니다.](#)

[c. Expressway-C에서 인접 영역 구성](#)

[d. 인증서 확인](#)

[2단계. Expressway-C와 Expressway-E 간의 접근 영역 구성](#)

[a. Expressway-C의 B2B 트래픽에 대한 접근 영역 컨피그레이션](#)

[b. Expressway-E의 B2B 트래픽에 대한 접근 영역 컨피그레이션](#)

[3단계. Expressway-E에서 DNS 영역 구성](#)

[4단계. 다이얼 플랜 구성](#)

[a. Expressway-C 및 E의 변환 및/또는 검색 규칙](#)

[b. CUCM의 SIP 경로 패턴](#)

[c. SIP 통화 라우팅의 경우 공용 DNS 서버에 SRV 레코드를 만들어야 합니다.](#)

[d. CUCM에서 Cluster Fully Qualified Domain Name을 구성합니다.](#)

[e. Expressway-C에서 변환을 생성하여 CUCM에서 초대에 수신된 URI에서 포트를 제거합니다.](#)

[5단계. Expressway에 리치 미디어 라이선스 업로드](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 Cisco CUCM(Unified Call Manager)과 통합된 Expressway를 통해 오디오 및 비디오 통화를 위한 B2B(Business to Business) 구축을 통합/구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Expressway-C(Exp-C)
- Expressway-E(Exp-E)
- Cisco CUCM(Unified Call Manager)
- CUC(Cisco Unity Connection)
- Telepresence Video Communication Server-C(VCS-C)
- Jabber 전화
- Cisco CTS(Telepresence System)
- EX 전화
- SIP(Session Initiation Protocol)
- HTTP(Hypertext Transfer Protocol)
- XMPP(eXtensible Messaging and Presence Protocol)
- Cisco Unified IM and Presence(IM&P)
- 인증서

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Expressway C 및 E X8.1.1 이상
- CUCM(Unified Communications Manager) 10.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 배경 정보

이 단계에서는 CUCM과 통합된 Expressway를 통해 오디오 및 비디오 통화를 위한 B2B 구축을 통합/구성하여 다른 회사(도메인)로부터 전화를 걸고 받을 수 있는 방법에 대해 자세히 설명합니다.

MRA(Mobile Remote Access) 기능을 사용하는 Expressway는 네트워크 다이어그램에 표시된 대로 엔터프라이즈 네트워크 외부에 있는 Jabber 및 TC 엔드포인트를 원활하게 등록할 수 있도록 합니다.

또한 동일한 아키텍처는 서로 다른 기업, 즉 Business to Business 통합을 위한 원활한 통합/통화를 제공하며, 이를 통해 오디오, 비디오 및 IM&P(B2B)를 지원합니다.

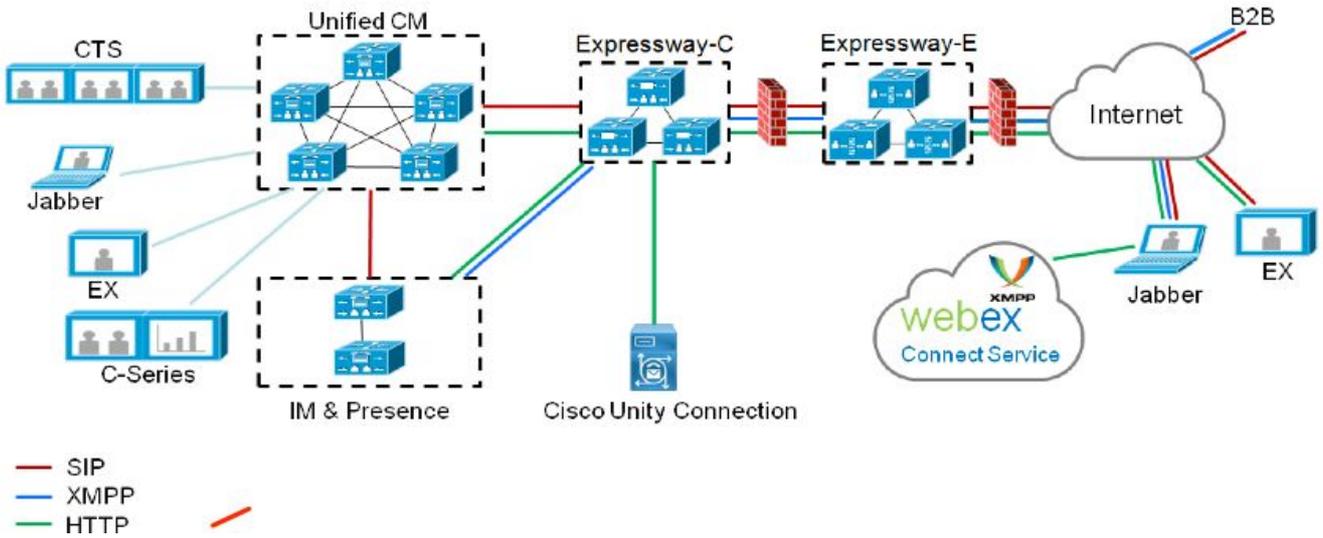
이 문서에서는 IM&P 부품에 대해 다루지 않으며 H.323 통합에 대해서도 다루지 않습니다.

계속하기 전에 도메인에 대해 관련 DNS 서비스(SRV)를 만들어야 합니다. 이러한 레코드는 다른 회사에서 Expressway의 위치를 찾는 데 사용됩니다.

## 구성

### 네트워크 다이어그램

이 이미지는 네트워크 다이어그램의 예를 제공합니다.



## 1단계. CUCM과 Expressway-C 간의 SIP 트렁크

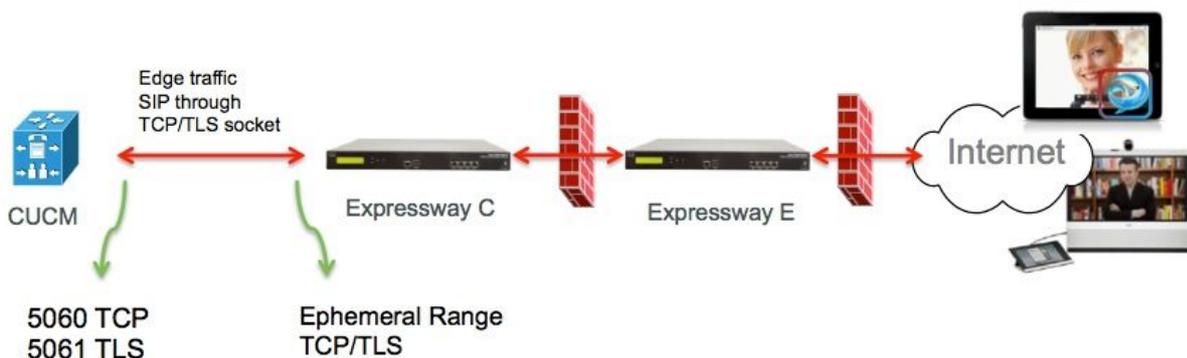
Expressway-C에서 CUCM 검색을 수행하면 인접 영역이 각 노드에 대해 자동으로 구성되고 전송 프로토콜이 검색됩니다.

CUCM 클러스터가 혼합 모드로 구성된 경우 목적지 포트 5060과 목적지 포트 5061의 보안 트래픽을 위한 TLS(Transport Layer Security)용 1개의 영역이 있는 비보안 트래픽에 대해 TCP(Transmission Control Protocol)에 대한 하나의 영역이 있습니다. 이러한 포트는 변경할 수 없습니다.

이 두 영역은 에지 엔드포인트와의 모든 에지 통화에 사용됩니다.

에지 엔드포인트의 인바운드 통화는 이러한 자동 추가 영역의 경로를 사용하므로 CUCM의 TCP 5060 또는 TLS 5061을 대상으로 합니다.

설정된 소켓 에지 엔드포인트를 통해 통화를 등록 및 발신/수신합니다.



B2B 통화의 경우 일반적으로 CUCM이 포트 5060 또는 5061에서 이 게이트웨이에서 인바운드 트래픽을 수신하는 Expressway-C를 가리키는 CUCM에서 SIP 트렁크를 구성합니다.

에지 트래픽은 포트 5060/5061이 있는 동일한 소스 IP에서 오므로 CUCM에서 이 트렁크에 대해 다른 수신 포트를 사용해야 합니다. 그렇지 않으면 에지 트래픽이 CUCM의 SIP 트렁크 디바이스로 라우팅되고 엔드포인트 디바이스(CSF 또는 EX)로 라우팅되지 않습니다.

Expressway-C의 경우 SIP(Session Initiation Protocol) TCP/TLS에 포트 5060 및 5061을 사용합니다.

CUCM이 포트 6060/6061에서 이 트렁크의 인바운드 트래픽에 대해 수신 대기하는 예는 이미지에 나와 있습니다



이러한 단계는 이 구축에 대해 문서화된 다양한 구성 단계입니다. 보안 및 비보안 구축을 모두 지원합니다.

a. 새 SIP 트렁크 보안 프로필을 추가합니다.

CUCM Administration(CUCM 관리) 페이지에서 > Device(디바이스) > Trunk(트렁크)로 이동합니다

5060/5061과 다른 수신 포트를 구성합니다. 여기서는 TCP에 6060을 사용하고 TLS에는 6061을 사용합니다

**비보안 SIP 트렁크 프로파일**

## - 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

### 보안 SIP 트렁크 프로파일

TLS의 경우 Expressway-c에서 제공하는 인증서의 CN과 일치하는 X.509 주체 이름을 구성해야 합니다. 또한 Expressway-C 또는 CA 인증서(Expressway-C 인증서를 발급한)를 CUCM 인증서 신뢰 저장소에 업로드합니다.

## - 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. CUCM에서 SIP 트렁크를 구성합니다.

이 트렁크를 통해 모든 B2B 통화는 CUCM과 주고받는 통화입니다.

SIP 트렁크 컨피그레이션 매개변수는 VCS 구축의 CUCM에 대해 표준입니다.

1단계에서 생성한 보안 프로파일을 연결해야 합니다.

### c. Expressway-C에서 인접 영역 구성

CUCM을 타겟으로 지정하려면 Expressway-C에서 인접 영역을 구성해야 합니다.

이 영역은 인바운드 B2B 트래픽을 CUCM으로 라우팅하는 데 사용됩니다.

컨피그레이션은 표준으로, 목적지 포트를 구성해야 CUCM의 SIP 트렁크에 할당된 SIP 트렁크 보안 프로필에 구성된 수신 대기 포트에 해당하는지 확인해야 합니다.

이 예에서 사용된 대상 포트는 SIP/TCP의 경우 6060, SIP/TLS의 경우 6061입니다(1단계 참조).

Expressway 관리 페이지에서 구성 > 다이얼 플랜 > 컨피그레이션으로 변환

SIP TCP용 인접 영역:

**Configuration**

Name: CUCMZONE

Type: Neighbor

Hop count: 20

**H.323**

Mode: Off

**SIP**

Mode: On

Port: 6060

Transport: TCP

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

Peer 2 address:

Peer 3 address:

Peer 4 address:

Peer 5 address:

Peer 6 address:

SIP: Reachable: 10.48.79.105:6050

**Advanced**

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

Save | Cancel | Delete

SIP TLS용 네이버 영역 - TLS 확인 모드가 켜짐

TLS 확인 모드가 로 설정된 경우 피어 주소가 CUCM에서 제공하는 인증서의 CN 또는 SAN과 일치하는지 확인해야 합니다. 일반적으로 TLS 확인 모드에서 피어 주소에 대한 CUCM 노드의 FQDN(Fully Qualified Domain Name)을 구성합니다.

Expressway 관리 페이지에서 Configuration(컨피그레이션) > Dial Plan(다이얼 플랜) > Transform y Configuration(컨피그레이션 변환)으로 이동합니다.

**Configuration**

Name  ⓘ

Type Neighbor

Hop count  ⓘ

---

**H.323**

Mode  ⓘ

---

**SIP**

Mode  ⓘ

Port  ⓘ

Transport  ⓘ

TLS verify mode  ⓘ

Accept proxied registrations  ⓘ

Media encryption mode  ⓘ

ICE support  ⓘ

---

**Authentication**

Authentication policy  ⓘ

SIP authentication trust mode  ⓘ

---

**Location**

Peer 1 address  ⓘ SIP: Reachable: 10.48.79.105:6050

Peer 2 address  ⓘ

Peer 3 address  ⓘ

Peer 4 address  ⓘ

Peer 5 address  ⓘ

Peer 6 address  ⓘ

---

**Advanced**

Zone profile  ⓘ

## SIP TLS용 네이버 영역 - TLS 확인 모드가 꺼져 있음

TLS 확인 모드가 피어 주소 외부로 설정된 경우 CUCM 노드의 IP 주소, 호스트 이름 또는 FQDN이 될 수 있습니다.

Expressway 관리 페이지에서 구성 > 다이얼 플랜 > 컨피그레이션으로 변환

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 ⓘ <span style="color: green;">SIP: Reachable 10.48.79.105:6050</span>
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. 인증서 확인

TLS의 경우 다음을 확인합니다.

- Expressway-C 서버 인증서 또는 CA 루트(인증서 서명에 사용됨)가 CUCM 클러스터의 모든 서버에 있는 CUCMTrust 저장소에 업로드됩니다.

- CallManager 인증서 또는 CA 루트(인증서 서명에 사용됨)가 Expressway-C 서버의 신뢰할 수 있는 CA 인증서 목록에 업로드됩니다.

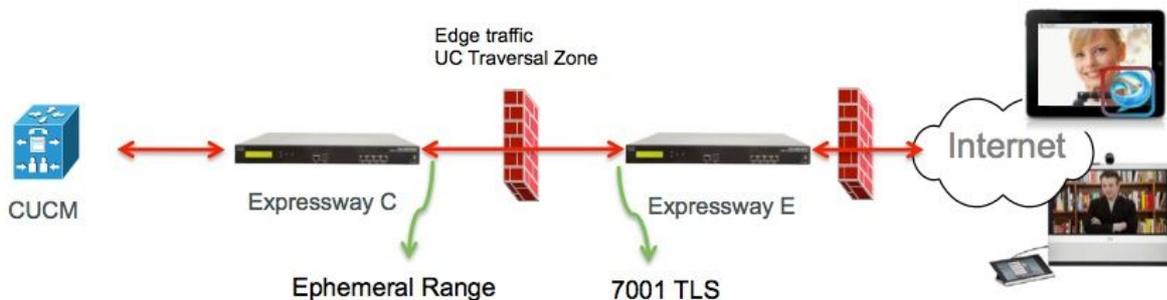
### 2단계. Expressway-C와 Expressway-E 간의 접근 영역 구성

Expressway-C와 Expressway-E 간에 B2B 트래픽을 라우팅하려면 별도의 접근 영역을 구성해야 합니다.

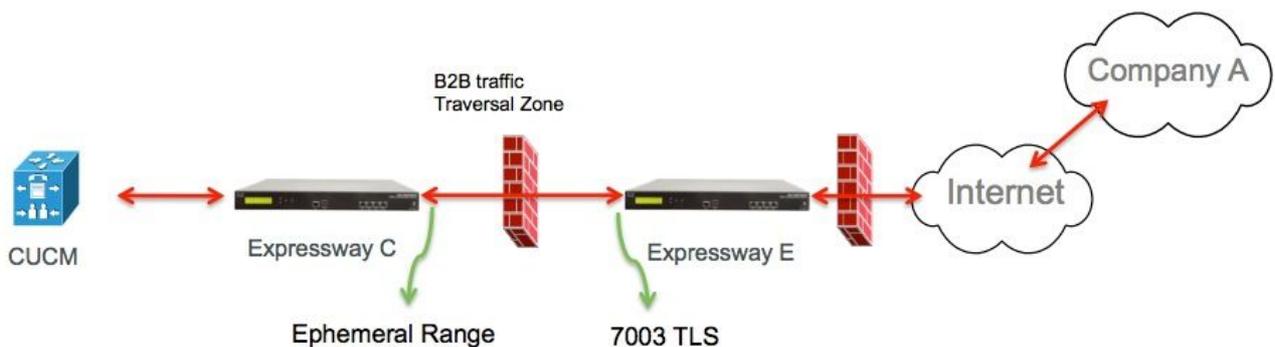
이는 표준 접근 영역 구성이지만 CUCM의 SIP 트렁크와 유사하지만 에지 트래픽에 대해 UC 접근 영역에서 사용하는 포트를 구성해야 합니다.

UC 접근 영역의 표준 포트는 7001입니다. B2B Traversal 영역의 경우 7003을 구성할 수 있습니다.

이미지에 표시된 대로 에지 트래픽을 위한 UC 접근 영역



이미지에 표시된 대로 B2B 트래픽에 대한 접근 영역



#### a. Expressway-C의 B2B 트래픽에 대한 접근 영역 컨피그레이션

Expressway-C는 traversal zone client입니다. 이 예에서는 대상 포트가 7003입니다.

TLS 확인 모드가 On으로 설정된 경우 구성된 피어 주소가 Expressway-E에서 제공한 인증서의 CN 또는 SAN과 일치하는지 확인합니다.

Expressway 관리 페이지에서 Configuration(컨피그레이션) > Dial Plan(다이얼 플랜) > Transforms y Configuration(컨피그레이션 변환)으로 이동합니다.

**Configuration**

Name: b2B-Traversal

Type: Traversal client

Hop count: 15

**Connection credentials**

Username: eft

Password: \*\*\*\*\*

**H.323**

Mode: Off

Protocol: Assent

**SIP**

Mode: On

Port: 7003

Transport: TLS

TLS verify mode: On

Accept proxied registrations: Allow

Media encryption mode: Auto

ICE support: Off

SIP poison mode: Off

**Authentication**

Authentication policy: Do not check credentials

**Client settings**

Retry interval: 120

**Location**

Peer 1 address: eft-xwye.coluc.com

Peer 2 address:

Peer 3 address:

## b. Expressway-E의 B2B 트래픽에 대한 접근 영역 컨피그레이션

Expressway-E는 traversal 영역 서버입니다. 이 예에서는 수신 포트가 7003입니다.

TLS 확인 모드가 On으로 설정된 경우 구성된 **TLS 확인 주체 이름**이 Expressway-C에서 제공한 인증서의 CN 또는 SAN과 일치하는지 확인합니다.

Expressway 관리 페이지에서 Configuration(컨피그레이션) > Dial Plan(다이얼 플랜) > Transform > Configuration(컨피그레이션 변환)으로 이동합니다.

**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  ⓘ

### 3단계. Expressway-E에서 DNS 영역 구성

B2B 트래픽을 라우팅하려면 Expressway-E에서 DNS 영역을 구성합니다.

이 영역으로 향하는 트래픽의 Expressway-E는 SIP URI의 도메인 부분에서 파생된 도메인에 대해 \_sip 또는 \_sips에 대해 DNS SRV 조회를 수행합니다.

SIP 호출을 라우팅하는 데 사용된 DNS 서버에서 반환한 SRV 대상

컨피그레이션은 표준 DNS 영역 컨피그레이션입니다.

Expressway 관리 페이지에서 Configuration(컨피그레이션) > Zones(영역)로 이동합니다.

**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  ⓘ

## 4단계. 다이얼 플랜 구성

### a. Expressway-C 및 E의 변환 및/또는 검색 규칙

Expressway 관리 페이지에서 Configuration(구성) > Dial Plan(다이얼 플랜) > Transform y Configuration(컨피그레이션으로 변환) > Dial Plan(다이얼 플랜) > Transform or Search Rules(변환 또는 검색 규칙)

자세한 내용은 라우팅 컨피그레이션에 대한 장, VCS 구축 설명서(Control with Expressway)를 참조하십시오.

## b. CUCM의 SIP 경로 패턴

자세한 내용은 CUCM [System and Administration\(CUCM 시스템 및 관리\) 가이드](#)(다이얼 플랜 구축 설명서)를 참조하십시오.

## c. SIP 통화 라우팅의 경우 공용 DNS 서버에 SRV 레코드를 만들어야 합니다.

이미지에 표시된 것처럼, 필요한 SRV 레코드 및 이 문서에서 논의되지 않은 H323 B2B 통화가 나열됩니다. 또한 SIP UDP는 기본적으로 Expressway에서 비활성화되어 있습니다

### 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. CUCM에서 Cluster Fully Qualified Domain Name을 구성합니다.

선택으로 구분된 여러 항목을 입력할 수 있습니다.

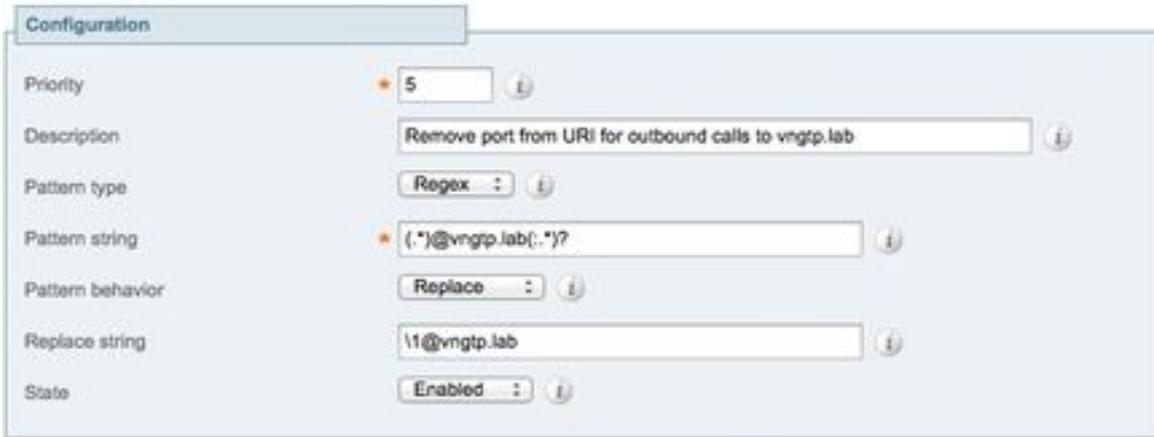


The screenshot shows a configuration window titled "Clusterwide Domain Configuration". It contains two input fields: "Organization Top Level Domain" and "Cluster Fully Qualified Domain Name". The second field contains the text "vcs.domain".

## e. Expressway-C에서 변환을 생성하여 CUCM에서 초대에 수신된 URI에서 포트를 제거합니다.

자세한 내용은 VCS Expressway Sent to Wrong IP Address(VCS Expressway에서 [DNS 영역으로 CUCM에서 잘못된 IP 주소로 전송된 통화](#)) 문서를 참조하십시오.

Expressway 관리 페이지에서 Configuration(컨피그레이션) > Dial Plan(다이얼 플랜) > Transform y Configuration(컨피그레이션 변형) > Dial Plan(다이얼 플랜) > Transform(변형)으로 이동합니다.



SRND에는 다이얼 플랜에 대한 광범위한 장이 포함되어 있습니다.

## 5단계. Expressway에 리치 미디어 라이선스 업로드

리치 미디어 라이선스(Traversal Zone 라이선스라고도 함)는 각 Expressway 서버에 업로드해야 합니다.

이 오류가 누락되었거나 잘못된 컨피그레이션 통화로 인해 발생한 경우 다음 오류 메시지와 함께 릴리스됩니다. "통화 라이선스 제한에 도달함: 동시 통과 통화 라이선스의 라이선스 제한에 도달했습니다."

## 다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

## 문제 해결

추가 B2B 문제 해결 정보는 이 문서 [Expressway를 통한 비즈니스 간 통화 시 가장 일반적인 문제 해결](#)

## 관련 정보

- [Cisco TelePresence VCS\(Video Communication Server\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)