

# NAT를 사용하여 ONS 15454의 실제 IP 주소를 숨겨 CTC 세션 설정

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[토폴로지](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[Cisco ONS 15454 구성](#)

[개인 컴퓨터 구성](#)

[라우터 컨피그레이션](#)

[다음을 확인합니다.](#)

[확인 절차](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 CTC(Cisco Transport Controller)와 ONS 15454 간의 세션을 설정하기 위한 NAT(Network Address Translation)의 샘플 컨피그레이션을 제공합니다. 이 컨피그레이션에서는 ONS 15454가 사설 네트워크에 있고 CTC 클라이언트가 공용 네트워크에 상주하는 경우 NAT 및 액세스 목록을 사용합니다.

보안을 위해 NAT 및 액세스 목록을 적용합니다. NAT는 ONS 15454의 실제 IP 주소를 숨깁니다. 액세스 목록은 ONS 15454에서 들어오고 나가는 IP 트래픽을 제어하는 방화벽 역할을 합니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco ONS 15454에 대한 기본적인 지식을 보유하십시오.
- 어떤 Cisco 라우터가 NAT를 지원하는지 확인하십시오.

## [사용되는 구성 요소](#)

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.1(11) 이상
- Cisco ONS 15454 버전 5.X 이상

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.

## [표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오](#).

## [배경 정보](#)

이 섹션에서는 필수 배경 정보를 제공합니다.

## [토폴로지](#)

테스트 토폴로지는 다음과 같이 구성됩니다.

- 서버 역할을 하는 Cisco ONS 15454 1개
- CTC 클라이언트 역할을 하는 PC 1대
- NAT 지원을 제공하는 Cisco 2600 Series 라우터 1개

**참고:** Cisco ONS 15454는 내부 네트워크에 있으며 PC는 외부 네트워크에 있습니다.

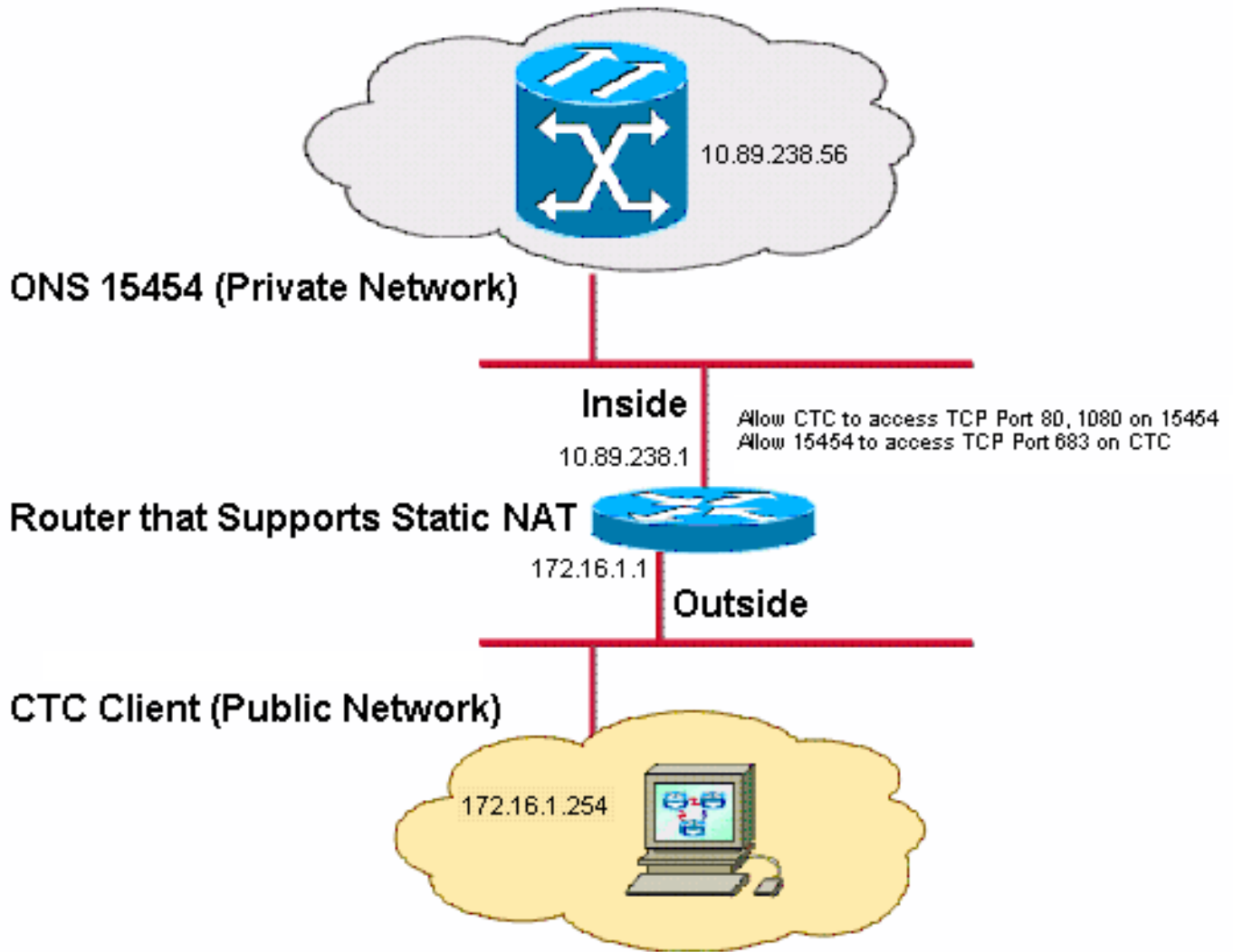
## [구성](#)

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용합니다.

## [네트워크 다이어그램](#)

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 172.16.0.0은 공용 네트워크에서 라우팅할 수 있다고 가정합니다.

## 구성

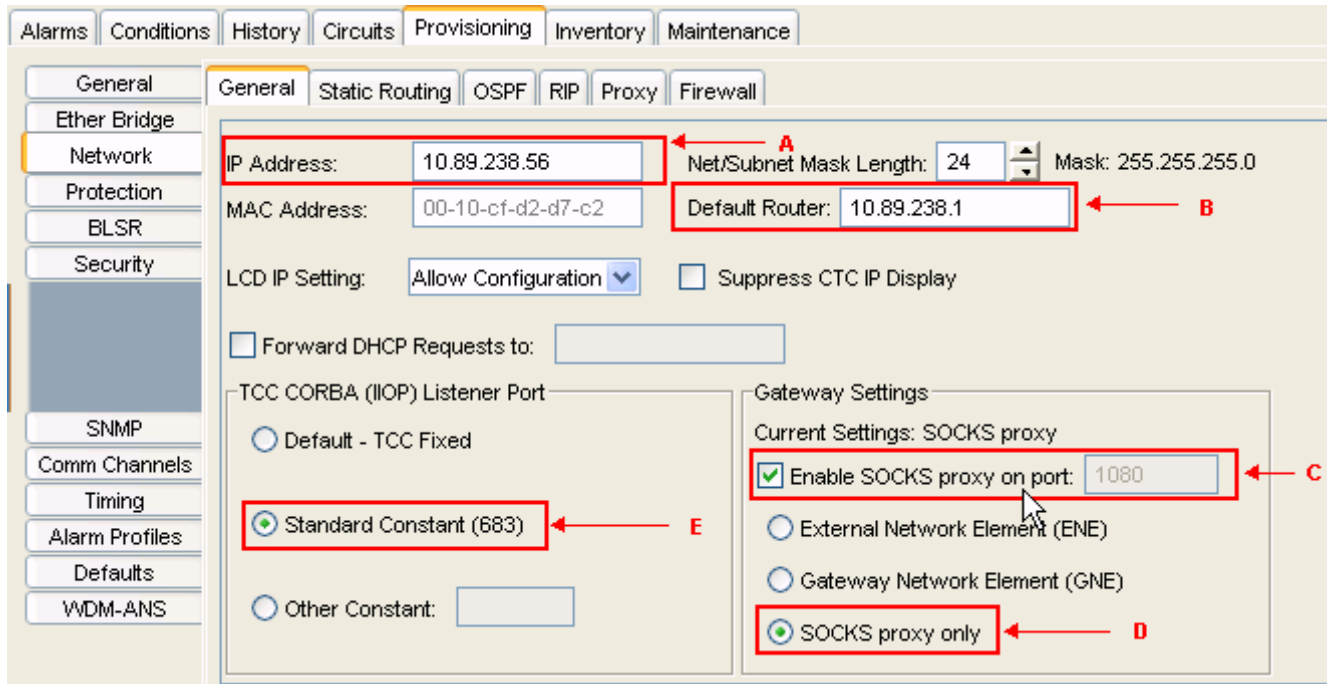
이 문서에서는 다음 구성을 사용합니다.

- ONS 15454
- PC
- 라우터

## Cisco ONS 15454 구성

다음 단계를 완료하십시오.

1. 노드 보기에서 Provisioning(프로비저닝) > **General(일반)** > **Network(네트워크)**를 클릭합니다. ONS 15454의 IP 주소가 IP Address 필드에 10.89.238.56으로 표시되는지 확인합니다([그림 2](#)의 화살표 A 참조). Default Router 필드에 10.89.238.1 값이 포함되어 있는지 확인합니다([그림 2](#)의 화살표 B 참조).**그림 2 - ONS 15454 구성**

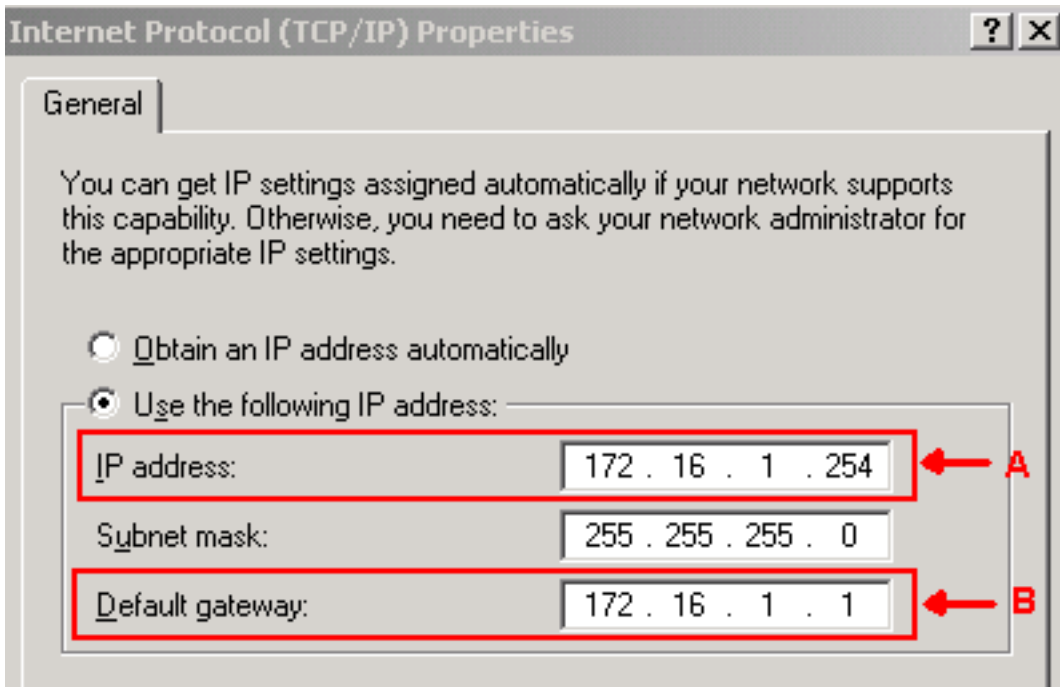


2. Gateway Settings(게이트웨이 설정) 섹션에서 **Enable SOCKS proxy on port(포트에서 SOCKS 프록시 사용)** 확인란을 선택하고(그림 2의 화살표 C 참조) SOCKS 프록시 전용 옵션을 선택합니다(그림 2의 화살표 D 참조).
3. TCC CORBA (IIO) Listener Port 섹션에서 필요한 리스너 포트 옵션을 선택합니다.다음 세 가지 옵션이 있습니다.**Default - TCC Fixed(기본값 - TCC 고정)** - ONS 15454가 CTC 컴퓨터와 같은 방화벽 쪽에 있거나 방화벽이 없는 경우(기본값) 이 옵션을 선택합니다. 이 옵션은 ONS 15454 리스너 포트를 포트 57790으로 설정합니다. 포트 57790이 열려 있는 경우 방화벽을 통한 액세스에 기본 - TCC 고정 옵션을 사용할 수 있습니다.**Standard Constant(표준 상수)** - ONS 15454 리스너 포트로 CORBA 기본 포트 번호인 Port 683을 사용하려면 이 옵션을 선택합니다.이 예에서는 표준 상수(683)를 사용합니다(그림 2의 화살표 E 참조).기타 상수 - 포트 683을 사용하지 않는 경우 이 옵션을 선택합니다. 방화벽 관리자가 지정하는 IIO 포트를 입력합니다.

## 개인 컴퓨터 구성

인터넷 프로토콜(TCP/IP) 속성 대화 상자에서 IP 주소 필드가 PC의 IP 주소로 172.16.1.254을 나타내는지 확인합니다(그림 3의 화살표 A 참조). 또한 172.16.1.1이 기본 게이트웨이인지 확인합니다(그림 3의 화살표 B 참조).

### 그림 3 - PC 구성



## 라우터 컨피그레이션

다음 단계를 완료하십시오.

1. Cisco ONS 15454가 상주하는 내부 인터페이스를 구성합니다.

```
!
interface Ethernet1/0
 ip address 10.89.238.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
!
```

2. 액세스 목록 101을 구성합니다.

```
access-list 101 permit tcp any eq www any
!
! Allow CTC to access TCP Port 80 on ONS 15454
!
access-list 101 permit tcp any eq 1080 any
!
! Allow CTC to access TCP Port 1080 on ONS 15454
!
access-list 101 permit tcp any any eq 683
!
! Allow ONS 15454 to access TCP Port 683 on the PC
!
```

3. PC가 있는 외부 인터페이스를 구성합니다.

```
interface Ethernet1/1
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
!
```

4. 고정 NAT를 구성합니다. 컨피그레이션은 10.89.238.56(내부 로컬)의 IP 주소를 172.16.1.200(외부 전역)의 IP 주소로 변환합니다. 변환 테이블을 보려면 라우터에서 **show ip nat translation** 명령을 실행합니다([그림 4](#) 참조).

```
!
ip nat inside source static 10.89.238.56 172.16.1.200
!
```

### 그림 4 - IP NAT 변환

```

2600-4#show ip nat translation
Pro Inside global  Inside local  Outside local  Outside global
--- 172.16.1.200   10.89.238.56   ---          ---

```

## 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 show 명령은 [출력 인터프리터 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

- show access-list - 액세스 목록을 통과하는 패킷의 수를 표시합니다.

## 확인 절차

구성을 확인하려면 다음 단계를 완료하십시오.

1. Microsoft Internet Explorer를 실행합니다.
2. 브라우저 창의 Address 필드에 http://172.16.1.200을 입력하고 Enter 키를 누릅니다  
.172.16.1.200은 내부 전역 주소입니다.공용 네트워크에서 CTC 사용자는 내부 로컬 주소가 10.89.238.56인 ONS 15454의 내부 전역 주소인 172.16.1.200만 액세스할 수 있습니다.CTC 로그인 창이 나타납니다.
3. 로그인할 사용자 이름과 암호를 입력합니다.CTC 클라이언트가 ONS 15454에 성공적으로 연결됩니다.
4. debug ip nat detailed 명령을 실행하여 IP NAT 상세 추적을 활성화합니다.추적 파일에서 주소 변환을 볼 수 있습니다.예를 들어, 주소 변환은 10.89.238.56에서 172.16.1.200([그림 5](#)의 화살표 A 참조)로, 172.16.1.200에서 10.89.238.56으로([그림 5](#)의 화살표 B 참조).**그림 5 - 디버그 IP NAT 세부 정보**

```

NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55499]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55499]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55500]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55500]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55501]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32895]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32895]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32897]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32897] B

```

5. 액세스 목록을 통과하는 패킷 수를 보려면 라우터에서 show access-list 명령을 실행합니다.**그림 6 - show access-list 명령**

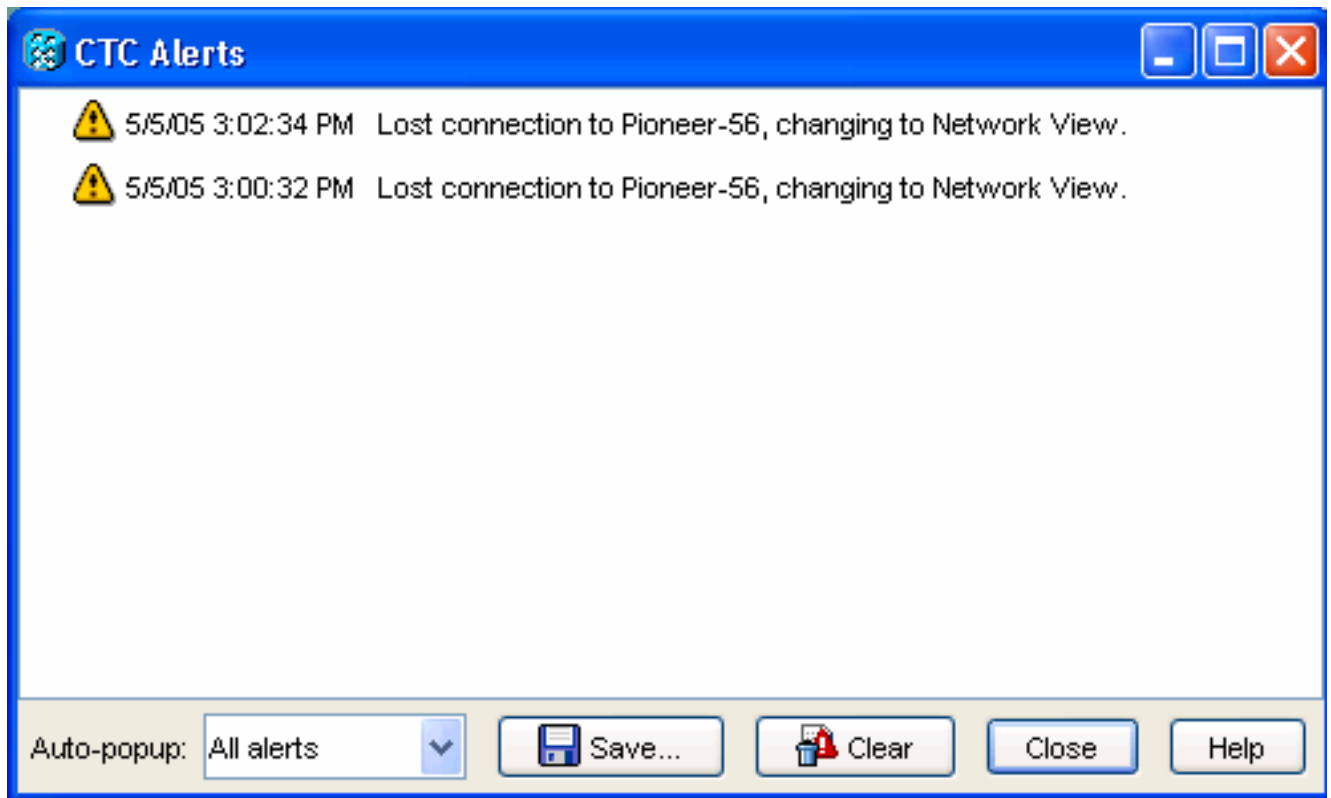
```

2600-4#show access-list
Extended IP access list 101
  permit tcp any eq www any (56 matches)
  permit tcp any eq 1080 any (330 matches)
  permit tcp any any eq 683 (6 matches)

```

액세스

목록이 TCC CORBA(IIOp) Listener Port를 차단하면 ONS 15454를 사용하는 CTC 세션이 정기적으로 시간 초과되고 다음과 같이 2분마다 경고 메시지가 표시됩니다.**그림 7 - CTC 경고 :TCC CORBA(IIOp) 포트가 차단됨**



이를 해결하려면 CTC IIOP 리스너 포트를 열 수 있습니다. Cisco 버그 ID [CSCeh96275](#)([등록된 고객만 해당](#))는 이 문제를 해결합니다. 향후 방화벽에서 TCP 포트 80 및 1080용 도관을 만들면 ONS 15454의 실제 IP 주소를 숨기는 데 충분한 지원을 제공할 수 있습니다.

## [문제 해결](#)

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

## [관련 정보](#)

- [기술 지원 및 문서 - Cisco Systems](#)