

# FAQ(자주 묻는 질문)로 NAT(Network Address Translation) 문제 해결

## 목차

[소개](#)

[일반 NAT](#)

[Q. NAT란 무엇입니까?](#)

[Q. NAT는 어떻게 작동합니까?](#)

[Q. NAT는 어떻게 구성합니까?](#)

[Q. Cisco IOS®Software와 Cisco ASA\(Adaptive Security Appliance\) NAT 구현 간의 주요 차이점은 무엇입니까?](#)

[Q. 어떤 Cisco 라우팅 하드웨어에서 Cisco IOS NAT를 사용할 수 있습니까? 하드웨어를 주문하려면 어떻게 해야 합니까?](#)

[Q. NAT는 라우팅 전 또는 후에 발생합니까?](#)

[Q. NAT는 공용 무선 LAN 환경에서 구축할 수 있습니까?](#)

[Q. NAT는 내부 네트워크의 서버에 대해 TCP 로드 밸런싱을 수행합니까?](#)

[Q. NAT 변환 수를 속도 제한할 수 있습니까?](#)

[Q. NAT에서 사용하는 IP 서브넷 또는 주소에 대해 라우팅을 학습하거나 전파하려면 어떻게 해야 합니까?](#)

[Q. Cisco IOS NAT에서는 몇 개의 동시 NAT 세션이 지원됩니까?](#)

[Q. Cisco IOS NAT에서는 어떤 종류의 라우팅 성능을 기대할 수 있습니까?](#)

[Q. Cisco IOS NAT를 하위 인터페이스에 적용할 수 있습니까?](#)

[Q. Cisco IOS NAT를 HSRP\(Hot Standby Router Protocol\)와 함께 사용하여 ISP에 대한 이중 링크를 제공할 수 있습니까?](#)

[Q. Cisco IOS NAT는 프레임 릴레이 인터페이스에서 인바운드 변환을 지원합니까? 이더넷 측에서 아웃바운드 변환을 지원합니까?](#)

[Q. 단일 NAT 지원 라우터를 통해 일부 사용자는 동일한 이더넷 인터페이스의 NAT를 사용하고 다른 사용자는 자신의 IP 주소를 계속 사용할 수 있습니까?](#)

[Q. PAT\(overloading\)가 구성된 경우, 내부 글로벌 IP 주소당 생성될 수 있는 최대 변환 수는 얼마입니까?](#)

[Q. PAT는 어떻게 작동합니까?](#)

[Q. NAT IP 풀이란 무엇입니까?](#)

[Q. 구성 가능한 NAT IP 풀\(ip nat pool "name"\)의 최대 수는 몇 개입니까?](#)

[Q. NAT 풀에서 Route-Map과 ACL의 장점은 무엇입니까?](#)

[Q. NAT 컨텍스트 내에서 "중복"되는 IP 주소는 무엇입니까?](#)

[Q. 고정 NAT 변환이란 무엇입니까?](#)

[Q. NAToverloading이라는 용어는 무엇을 의미합니까? 이 PAT입니까?](#)

[Q. 동적 NAT 변환이란 무엇입니까?](#)

[Q. ALG란 무엇입니까?](#)

[Q. 고정 및 동적 NAT 변환을 모두 사용하여 컨피그레이션을 구축할 수 있습니까?](#)

[Q. traceroute가 NAT 라우터를 통해 수행되는 경우 traceroute는 NAT-Global 주소를 표시해야 합니까, 아니면 NAT-Local 주소를 누설해야 합니까?](#)

[Q. PAT는 포트를 어떻게 할당합니까?](#)

[Q. IP 프래그먼트화와 TCP 세그멘테이션은 어떻게 됩니까?](#)

[Q. NAT는 IP 프래그먼트화 및 TCP 세그멘테이션에 대해 비순차적\(out-of-order\)을 지원합니까?](#)

[Q. IP 프래그먼트화 및 TCP 세그멘테이션을 디버깅하는 방법은 무엇입니까?](#)

[Q. 지원되는 NAT MIB가 있습니까?](#)

[Q. TCP 시간 제한이란 무엇이며, NAT TCP 타이머와 어떻게 관련됩니까?](#)

[Q. NAT 변환에 걸리는 시간을 NAT 변환 테이블에서 시간 초과로 변경할 수 있습니까?](#)

[Q. LDAP\(Lightweight Directory Access Protocol\)가 각 LDAP 응답 패킷에 추가 바이트를 연결할 때 LDAP를 중지하려면 어떻게 합니까?](#)

[Q. NAT 상자의 내부 전역/외부 로컬 IP 주소에 대한 경로 권장 사항은 무엇입니까?](#)

[Q. Cisco IOS NAT는 log 키워드와 함께 ACL을 지원합니까?](#)

#### [음성 NAT](#)

[Q. NAT는 CUCM\(Cisco Unified Communications Manager\) V7과 함께 제공되는 SCCP\(Skinny Client Control Protocol\) v17을 지원합니까?](#)

[Q. NAT에서 어떤 CUCM /SCCP/펌웨어 로드 버전을 지원합니까?](#)

[Q. RTP 및 RTCP에 대한 서비스 공급자 PAT 포트 할당 개선은 무엇입니까?](#)

[Q. SIP\(Session Initiation Protocol\)란 무엇이며 NAT를 통해 SIP 패킷을 라우팅할 수 있습니까?](#)

[Q. SBC\(Session Border Controller\)에 대한 Hosted NAT Traversal 지원이란 무엇입니까?](#)

[Q. 라우터 메모리와 CPU가 NAT로 처리할 수 있는 SIP, Skinny 및 H323 통화의 수는 몇 개입니까?](#)

[Q. NAT 라우터는 Skinny 및 H323 패킷의 TCP 세그멘테이션을 지원합니까?](#)

[Q. 음성 구축에서 NAT 오버로드 컨피그레이션을 사용할 때 주의해야 할 사항이 있습니까?](#)

[Q. 음성 구축에서 clear ip nat trans \\*명령 또는 clear ip nat trans forced 명령을 사용할 때 발생하는 알려진 문제가 있습니까?](#)

[Q. NAT는 공동 배치 음성 솔루션을 지원합니까?](#)

[Q. NVI는 Skinny ALG, H323 ALG 및 TCP SIP ALG를 지원합니까?](#)

#### [VRF/MPLS를 사용하는 NAT](#)

[Q. NAT 라우터가 VRF의 동일한 주소 공간과 전역 주소 공간에서 스스로를 지원할 수 있습니까? 현재 다음과 같은 경고가 표시됩니다. "% 유사한 정적 항목\(10.1.1.1 -> 10.2.2.2\)이 이미 있습니다. "이 항목을 구성하려고 하면 다음과 같은 경고가 표시됩니다.](#)

[Q. 레거시 NAT는 VRF-Lite\(VRF에서 다른 VRF로의 경로\)를 지원합니까?](#)

#### [NAT NVI](#)

[Q. NAT NVI란 무엇입니까?](#)

[Q. NAT NVI를 사용하여 전역 인터페이스와 VRF 인터페이스 간에 라우팅해야 합니까?](#)

[Q. NAT-NVI에 대한 TCP 세그멘테이션은 지원됩니까?](#)

[Q. NVI는 Skinny ALG, H323 ALG 및 TCP SIP ALG를 지원합니까?](#)

[Q. SNAT에서 TCP 세그멘테이션을 지원합니까?](#)

#### [스넷](#)

[Q: SNAT\(Stateful NAT\)란 무엇입니까?](#)

[Q. SNAT에서는 TCP 세그멘테이션이 지원됩니까?](#)

[Q. SNAT는 비대칭 라우팅을 지원합니까?](#)

#### [NAT-PT\(v6~v4\)](#)

[Q. NAT-PT란 무엇입니까?](#)

[Q. NAT-PT는 CEF\(Cisco Express Forwarding\) 경로에서 지원됩니까?](#)

[Q. NAT-PT에서는 어떤 ALG가 지원됩니까?](#)

[Q. ASR 1004는 NAT-PT를 지원합니까?](#)

#### [플랫폼에 의존하는 Cisco 7600/6k](#)

[Q. SX Train의 Catalyst 6500에서 SNAT\(Stateful NAT\)를 사용할 수 있습니까?](#)

[Q. VRF 인식 NAT는 6k의 하드웨어에서 지원됩니까?](#)

[Q. 7600 및 Cat6000은 VRF 인식 NAT를 지원합니까?](#)

[플랫폼에 의존하는 Cisco 850](#)

[Q. Cisco 850은 릴리스 12.4T에서 Skinny NAT ALG를 지원합니까?](#)

[NAT 구축](#)

[Q. NAT는 어떻게 구현합니까?](#)

[Q. NAT with voice는 어떻게 구현합니까?](#)

[Q. NAT를 MPLS VPN과 어떻게 통합합니까?](#)

[Q. NAT 고정 매핑은 고가용성을 위해 HSRP를 지원합니까?](#)

[Q. NAT NVI는 어떻게 구현합니까?](#)

[Q. NAT로 로드 밸런싱을 구현하려면 어떻게 해야 합니까?](#)

[Q. IPSec과 함께 NAT를 구현하려면 어떻게 해야 합니까?](#)

[Q. NAT-PT는 어떻게 구현합니까?](#)

[Q. 멀티캐스트 NAT는 어떻게 구현합니까?](#)

[Q. SNAT\(stateful NAT\)는 어떻게 구현합니까?](#)

[NAT 모범 사례](#)

[Q. NAT 모범 사례가 있습니까?](#)

[관련 정보](#)

## 소개

이 문서에서는 NAT(Network Address Translation) 라우터 프로세스의 작동 방식을 설명하고 몇 가지 일반적인 질문에 대한 답변을 제공합니다.

## 일반 NAT

### Q. NAT란 무엇입니까?

A. NAT(Network Address Translation)는 IP 주소 보존을 위해 설계되었습니다. 등록되지 않은 IP 주소를 사용하는 사설 IP 네트워크가 인터넷에 연결될 수 있도록 합니다. NAT는 일반적으로 두 네트워크를 함께 연결하는 경우 라우터에서 작동하며, 패킷이 다른 네트워크로 전달되기 전에 내부 네트워크의 비공개(전역적으로 고유하지 않음) 주소를 올바른 주소로 변환합니다.

이 기능의 일부로서 전체 네트워크에 대해 하나의 주소만 외부로 알리도록 NAT를 구성할 수 있습니다. 이는 전체 내부 네트워크를 해당 주소 뒤에 효과적으로 숨겨 추가 보안을 제공합니다. NAT는 보안과 주소 보존의 이중 기능을 제공하며 일반적으로 원격 액세스 환경에서 구현됩니다.

### Q. NAT는 어떻게 작동합니까?

A. 기본적으로 NAT는 라우터와 같은 단일 장치가 인터넷(또는 공용 네트워크)과 로컬 네트워크(또는 사설 네트워크) 사이에서 에이전트 역할을 할 수 있도록 합니다. 즉, 단일 고유 IP 주소만 있으면 전체 컴퓨터 그룹을 네트워크 외부에 나타낼 수 있습니다.

### Q. NAT는 어떻게 구성합니까?

A. 기존 NAT를 구성하려면 라우터에 있는 하나 이상의 인터페이스(NAT 외부) 및 라우터에 있는 다른 인터페이스(NAT 내부)와 패킷 헤더의 IP 주소에 대한 변환 규칙 집합(그리고 필요한 경우 페이로드)을 만들어야 하며 이러한 규칙을 구성해야 합니다. NVI(Nat Virtual Interface)를 구성하려면 위에

서 설명한 것과 동일한 규칙 집합과 함께 NAT 활성화로 구성된 하나 이상의 인터페이스가 필요합니다.

자세한 내용은 [Cisco IOS IP 주소 지정 서비스 컨피그레이션 가이드](#) 또는 NAT [가상 인터페이스 구성에 대한 섹션](#)을 참조하십시오.

### Q. NAT의 Cisco IOS<sup>®</sup> Software와 Cisco ASA(Adaptive Security Appliance) 구현의 주요 차이점은 무엇입니까?

A. Cisco IOS 소프트웨어 기반 NAT는 Cisco ASA의 NAT 기능과 근본적으로 다르지 않습니다. 주요 차이점은 구현 및 설계 요구 사항에서 지원되는 다른 트래픽 유형을 포함합니다. Cisco ASA [디바이스](#)의 NAT 컨피그레이션에 대한 자세한 내용은 NAT 컨피그레이션 예를 참조하십시오(지원되는 트래픽 유형 포함).

### Q. 어떤 Cisco 라우팅 하드웨어에서 Cisco IOS NAT를 사용할 수 있습니까? 하드웨어를 주문하려면 어떻게 해야 합니까?

A. Cisco Feature Navigator 툴을 사용하여 고객은 기능(NAT)을 식별하고 이 Cisco IOS Software 기능을 사용할 수 있는 릴리스 및 하드웨어 버전을 찾을 수 있습니다. 이 [툴](#)을 사용하려면 Cisco 기능 탐색기를 참조하십시오.

### Q. NAT는 라우팅 전 또는 후에 발생합니까?

A. 트랜잭션이 NAT에 의해 처리되는 순서는 패킷이 내부 네트워크에서 외부 네트워크로 이동하는지, 외부 네트워크에서 내부 네트워크로 이동하는지에 따라 결정됩니다. 내부-외부 변환은 라우팅 후에 발생하고 외부-내부 변환은 라우팅 전에 발생합니다. 자세한 [내용은 NAT](#) 작동 순서를 참조하십시오.

### Q. NAT는 공용 무선 LAN 환경에서 구축할 수 있습니까?

A.예. NAT - 고정 IP 지원 기능은 고정 IP 주소를 사용하는 사용자를 지원하며, 이러한 사용자가 공용 무선 LAN 환경에서 IP 세션을 설정할 수 있도록 합니다.

### Q. NAT는 내부 네트워크의 서버에 대해 TCP 로드 밸런싱을 수행합니까?

A.예. NAT를 사용하면 실제 호스트 간의 로드 밸런스를 조정하는 가상 호스트를 내부 네트워크에 설정할 수 있습니다.

### Q. NAT 변환 수를 속도 제한할 수 있습니까?

A.예. 속도 제한 NAT 변환 기능은 라우터에서 동시 NAT 작업의 최대 수를 제한하는 기능을 제공합니다. 이를 통해 사용자는 NAT 주소 사용 방법을 보다 효과적으로 제어할 수 있으며, 속도 제한 NAT 변환 기능을 사용하여 바이러스, 웜 및 서비스 거부 공격의 영향을 제한할 수 있습니다.

### Q. NAT에서 사용하는 IP 서브넷 또는 주소에 대해 라우팅을 학습하거나 전파하려면 어떻게 해야 합니까?

A.NAT에 의해 생성되는 IP 주소에 대한 라우팅은 다음과 같은 경우에 학습됩니다.

- 내부 전역 주소 풀은 next-hop 라우터의 서브넷에서 파생됩니다.
- 고정 경로 엔트리는 next-hop 라우터에서 구성되고 라우팅 네트워크 내에서 재배포됩니다.

내부 전역 주소가 로컬 인터페이스와 일치하는 경우 NAT는 IP 별칭 및 ARP 항목을 설치합니다. 이 경우 라우터는 이러한 주소에 대해 `canproxy-arp`를 수행합니다. 이 동작을 원하지 않으면 `theno-aliaskeyword`를 사용합니다.

NAT 풀이 구성된 경우 자동 경로 주입에 `add-route` 옵션을 사용할 수 있습니다.

## Q. Cisco IOS NAT에서는 몇 개의 동시 NAT 세션이 지원됩니까?

A. NAT 세션 제한은 라우터에서 사용 가능한 DRAM의 양에 따라 제한됩니다. 각 NAT 변환은 DRAM에서 약 312바이트를 소비합니다. 그 결과, 10,000개의 변환(일반적으로 단일 라우터에서 처리되는 것보다 많음)이 약 3MB를 소비합니다. 따라서 일반적인 라우팅 하드웨어는 수천 개의 NAT 변환을 지원할 수 있을 만큼 충분한 메모리를 보유하고 있습니다. 그러나 플랫폼 사양을 검증하는 것도 좋습니다.

## Q. Cisco IOS NAT에서는 어떤 종류의 라우팅 성능을 기대할 수 있습니까?

A. Cisco IOS NAT는 CEF(Cisco Express Forwarding) 스위칭, 고속 스위칭 및 프로세스 스위칭을 지원합니다. 12.4T 릴리스 이상에서는 고속 스위칭 경로가 더 이상 지원되지 않습니다. Cat6k 플랫폼의 경우 스위칭 순서는 Netflow(HW 스위칭 경로), CEF, 프로세스 경로입니다.

성능은 다음과 같은 몇 가지 요소에 따라 달라집니다.

- 애플리케이션 유형 및 트래픽 유형
- IP 주소의 포함 여부
- 여러 메시지 교환 및 검사
- 소스 포트 필요
- 번역 수
- 해당 시간에 실행되는 기타 애플리케이션
- 하드웨어 및 프로세서의 유형

## Q. Cisco IOS NAT를 하위 인터페이스에 적용할 수 있습니까?

A.예. 소스 및/또는 목적지 NAT 변환은 IP 주소가 있는 모든 인터페이스 또는 하위 인터페이스에 적용할 수 있습니다(다이얼러 인터페이스 포함). NAT는 무선 가상 인터페이스로 구성할 수 없습니다. NVRAM에 쓸 때 무선 가상 인터페이스가 존재하지 않습니다. 따라서 재부팅 후 라우터는 무선 가상 인터페이스의 NAT 컨피그레이션을 잃게 됩니다.

## Q. Cisco IOS NAT를 HSRP(Hot Standby Router Protocol)와 함께 사용하여 ISP에 대한 이중 링크를 제공할 수 있습니까?

A.예. NAT는 HSRP 이중화를 제공합니다. 그러나 SNAT(Stateful NAT)와는 다릅니다. NAT with HSRP는 상태 비저장 시스템입니다. 현재 세션은 장애가 발생해도 유지되지 않습니다. 고정 NAT 컨피그레이션 중에(패킷이 STATIC 규칙 컨피그레이션과 일치하지 않는 경우) 패킷은 변환 없이 전송됩니다.

## Q. Cisco IOS NAT는 프레임 릴레이 인터페이스에서 인바운드 변환을 지원합니까? 이더넷 측에서 아웃바운드 변환을 지원합니까?

A.예. NAT의 경우 캡슐화는 중요하지 않습니다. NAT는 인터페이스에 IP 주소가 있고 인터페이스가 NAT inside 또는 NAT outside인 경우에 수행할 수 있습니다. NAT가 작동하려면 내부와 외부가 있어야 합니다. NVI를 사용하는 경우 NAT 활성화 인터페이스가 하나 이상 있어야 합니다. 자세한 내용은 이전 질문인 [How do I configure NAT?](#)를 참조하십시오.

## Q. 단일 NAT 지원 라우터를 통해 일부 사용자는 동일한 이더넷 인터페이스의 NAT를 사용하고 다른 사용자는 자신의 IP 주소를 계속 사용할 수 있습니까?

A.예. 이는 NAT가 필요한 호스트 또는 네트워크 집합을 설명하는 액세스 목록을 사용하여 수행할 수 있습니다. 동일한 호스트에 있는 모든 세션은 변환되거나 라우터를 통과하여 변환되지 않을 수 있습니다.

액세스 목록, 확장 액세스 목록 및 경로 맵을 사용하여 IP 디바이스가 변환되는 규칙을 정의할 수 있습니다. 네트워크 주소와 적절한 서브넷 마스크를 항상 지정해야 합니다. 키워드 anyany는 네트워크 주소 또는 서브넷 마스크 대신 사용할 수 없습니다. Static NAT 컨피그레이션에서는 패킷이 STATIC 규칙 컨피그레이션과 일치하지 않을 경우 어떤 변환 없이 패킷을 전송할 수 있습니다.

## Q. PAT(overloading)가 구성된 경우, 내부 글로벌 IP 주소당 생성될 수 있는 최대 변환 수는 얼마입니까?

A.PAT(과부하)는 전역 IP 주소당 사용 가능한 포트를 0-511, 512-1023 및 1024-65535의 세 범위로 나눕니다. PAT는 각 UDP 또는 TCP 세션에 대해 고유한 소스 포트를 할당합니다. 원래 요청의 동일한 포트 값을 할당하려고 시도하지만 원래 소스 포트가 이미 사용된 경우 특정 포트 범위의 처음부터 스캔을 시작하여 사용 가능한 첫 번째 포트를 찾아 대화에 할당합니다.

## Q. PAT는 어떻게 작동합니까?

A.PAT는 하나의 전역 IP 주소 또는 여러 주소와 함께 작동합니다.

### IP 주소 테이블이 하나인 PAT

#### 조건 설명

- 1 NAT/PAT는 트래픽을 검사하고 이를 변환 규칙에 매칭합니다.
- 2 규칙이 PAT 컨피그레이션과 일치합니다.
- 3 PAT가 트래픽 유형에 대해 알고 있고 해당 트래픽 유형에 사용할 수 있는 "특정 포트 또는 포트 집합"인 경우 PAT는 이들을 따로 설정하며 고유한 식별자로 할당하지 않습니다.
- 4 특별한 포트 요구 사항이 없는 세션이 연결을 시도할 경우 PAT는 IP 소스 주소를 변환하고 원래 소스의 가용성을 확인합니다(예: 433). **참고를 참조하십시오.**
- 5 요청된 소스 포트를 사용할 수 있는 경우 PAT는 소스 포트를 할당하고 세션이 계속됩니다.
- 6 요청된 소스 포트를 사용할 수 없는 경우 PAT는 관련 그룹의 처음부터 검색을 시작합니다(TCP 또는 애플리케이션의 경우 1에서 시작하고 ICMP의 경우 0에서 시작).
- 7 사용 가능한 포트가 있는 경우 포트가 할당되고 세션이 계속됩니다.
- 8 사용 가능한 포트가 없는 경우 패킷이 삭제됩니다.

**참고:** TCP(Transmission Control Protocol) 및 UDP(User Datagram Protocol)의 경우 범위는 1-511, 512-1023, 1024-65535입니다. ICMP(Internet Control Message Protocol)의 경우 첫 번째 그룹은 0에서 시작합니다.

### 여러 IP 주소의 PAT

#### 조건 설명

- 1-7 처음 7개의 조건은 단일 IP 주소의 경우와 동일합니다.
- 8 첫 번째 IP 주소의 관련 그룹에 사용 가능한 포트가 없는 경우 NAT는 풀의 다음 IP 주소로 이동하고 원래 소스 포트를 할당하려고 시도합니다.
- 9 요청된 소스 포트를 사용할 수 있는 경우 NAT는 소스 포트를 할당하고 세션은 계속됩니다.
- 10 요청된 소스 포트를 사용할 수 없는 경우 NAT는 관련 그룹의 처음부터 검색을 시작합니다(TCP 또는 애플리케이션의 경우 1에서 시작하고 ICMP의 경우 0에서 시작).
- 11 사용 가능한 포트가 있는 경우 포트가 할당되고 세션이 계속됩니다.
- 12 사용 가능한 포트가 없는 경우, 풀에서 다른 IP 주소를 사용할 수 없는 한 패킷이 삭제됩니다.

## Q. NAT IP 풀이란 무엇입니까?

A. NAT IP 풀은 필요에 따라 NAT 변환에 할당되는 IP 주소의 범위입니다. 풀을 정의하려면 configuration 명령을 사용합니다.

```
ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type {rotary}]
```

### 예 1

다음 예는 192.168.1.0 또는 192.168.2.0 네트워크에서 주소가 지정된 내부 호스트를 전역 고유 10.69.233.208/28 네트워크로 변환합니다.

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

### 예 2

다음 예에서는 가상 주소를 정의하는 것이 목적이며, 이 가상 주소에 대한 연결은 실제 호스트 집합 간에 분산됩니다. 풀은 실제 호스트의 주소를 정의합니다. 액세스 목록은 가상 주소를 정의합니다. 변환이 아직 없는 경우, 목적지가 액세스 목록과 일치하는 직렬 인터페이스 0(외부 인터페이스)의 TCP 패킷이 풀의 주소로 변환됩니다.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

## Q. 구성 가능한 NAT IP 풀(ip nat pool "name")의 최대 수는 몇 개입니까?

A. 실용적인 사용 시 구성 가능한 IP 풀의 최대 수는 특정 라우터에서 사용 가능한 DRAM의 양에 따라 제한됩니다. (풀 크기는 255로 구성하는 것이 좋습니다.) 각 풀은 16비트 이하여야 합니다. 12.4(11)T 이상에서 Cisco IOS는 CCE(Common Classification Engine)를 도입했습니다. 이로 인해 NAT는 최대 255개의 풀만 포함하도록 제한됩니다.

## Q. NAT 풀에서 Route-Map과 ACL의 장점은 무엇입니까?

A.A 경로 맵은 원치 않는 외부 사용자를 보호하여 내부 사용자/서버에 연결합니다. 또한 규칙에 따라 단일 내부 IP 주소를 다른 내부 전역 주소에 매핑하는 기능도 있습니다. 자세한 [내용은 경로 맵을 사용하는 다중 풀에](#) 대한 NAT 지원을 참조하십시오.

## Q. NAT 컨텍스트 내에서 "중복"되는 IP 주소는 무엇입니까?

A.IP 주소 중복은 두 위치를 상호 연결하려는 두 위치가 동일한 IP 주소 체계를 사용하는 상황을 나타냅니다. 이것은 드문 일이 아닙니다; 이것은 종종 회사들이 합병하거나 인수할 때 발생합니다. 특별한 지원이 없으면 두 위치를 연결하여 세션을 설정할 수 없습니다. 중복된 IP 주소는 다른 회사에 할당된 공용 주소, 다른 회사에 할당된 사설 주소일 수 있으며, RFC 1918에 정의된 사설 주소 범위에서 가져올 수 있습니다.

프라이빗 IP 주소는 라우팅할 수 없으며 외부 세계로의 연결을 허용하려면 NAT 변환이 필요합니다. 이 솔루션에는 외부에서 내부로 전달되는 DNS(Domain Name System) 이름 쿼리 응답, 외부 주소에 대한 변환 설정 가로채기가 포함되며, DNS 응답은 내부 호스트로 전달되기 전에 수정되어야 합니다. NAT 장치 양쪽에서 두 네트워크 간에 연결하려는 사용자를 확인하려면 DNS 서버가 관여해야 합니다.

NAT는 Using NAT [in Overlapping Networks](#)에 나와 있는 것처럼 DNSAandPTRrecords의 내용에 대해 주소 변환을 검사하고 수행할 수 있습니다.

## Q. 고정 NAT 변환이란 무엇입니까?

A. 고정 NAT 변환에는 로컬 주소와 글로벌 주소 간에 일대일 매핑이 있습니다. 사용자는 포트 레벨로 고정 주소 변환을 구성하고 나머지 IP 주소를 다른 변환에 사용할 수도 있습니다. 이는 일반적으로 PAT(Port Address Translation)를 수행하는 경우에 발생합니다.

다음 예는 고정 NAT에 대해 외부-내부 변환을 허용하도록 route-map을 구성하는 방법을 보여줍니다.

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

## Q. NAToverloading이라는 용어는 무엇을 의미합니까? 이 PAT입니까?

A.예. NAT 오버로딩은 PAT이며, 여기에는 하나 이상의 주소 범위의 풀 사용 또는 포트와 결합된 인터페이스 IP 주소 사용이 포함됩니다. 오버로드하면 전체 확장 변환이 생성됩니다. 이는 IP 주소 및

소스/목적지 포트 정보를 포함하는 변환 테이블 항목이며, 이를 일반적으로 PAT 또는 오버로드라고 합니다.

PAT(또는 오버로드)는 내부(내부 로컬) 개인 주소를 하나 이상의 외부(내부 전역, 일반적으로 등록된) IP 주소로 변환하는 데 사용되는 Cisco IOS NAT의 기능입니다. 각 변환의 고유한 소스 포트 번호를 사용하여 대화를 구분합니다.

## Q. 동적 NAT 변환이란 무엇입니까?

A. 동적 NAT 변환에서 사용자는 로컬 주소와 글로벌 주소 간에 동적 매핑을 설정할 수 있습니다. 동적 매핑은 변환할 로컬 주소와 전역 주소를 할당할 주소 또는 인터페이스 IP 주소 풀을 정의하고 두 주소를 연결할 때 수행됩니다.

## Q. ALG란 무엇입니까?

A. ALG는 ALG(애플리케이션 레이어 게이트웨이)입니다. NAT는 애플리케이션 데이터 스트림에서 소스 및/또는 목적지 IP 주소를 전달하지 않는 TCP/UDP(Transmission Control Protocol/User Datagram Protocol) 트래픽에 대해 변환 서비스를 수행합니다.

이러한 프로토콜에는 FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, 텔넷, 아카이브, 핑거, NTP, NFS, rlogin, rsh, rcp가 포함됩니다. 페이로드 내에 IP 주소 정보를 포함하는 특정 프로토콜에서는 ALG(Application Level Gateway)를 지원해야 합니다.

자세한 내용은 [NAT와 함께 애플리케이션 레벨](#) 게이트웨이 사용을 참조하십시오.

## Q. 고정 및 동적 NAT 변환을 모두 사용하여 컨피그레이션을 구축할 수 있습니까?

A. 예. 그러나 NAT 고정 컨피그레이션이나 NAT 동적 컨피그레이션용 풀에서는 동일한 IP 주소를 사용할 수 없습니다. 모든 공용 IP 주소는 고유해야 합니다. 고정 변환에 사용되는 전역 주소는 동일한 전역 주소를 포함하는 동적 풀에서 자동으로 제외되지 않습니다. 고정 엔트리에 의해 할당된 주소를 제외하려면 동적 풀을 생성해야 합니다. 자세한 내용은 [고정 및 동적 NAT 동시 구성을 참조하십시오](#).

## Q. traceroute가 NAT 라우터를 통해 수행되는 경우 traceroute는 NAT-Global 주소를 표시해야 합니까, 아니면 NAT-Local 주소를 누설해야 합니까?

외부의 A. Traceroute는 항상 전역 주소를 반환해야 합니다.

## Q. PAT는 포트를 어떻게 할당합니까?

A. NAT에는 추가 포트 기능, 즉 full-range 및 port-map이 도입됩니다.

- Full-range를 사용하면 기본 포트 범위와 상관없이 NAT에서 모든 포트를 사용할 수 있습니다.
- Port-map을 사용하면 NAT에서 특정 애플리케이션에 대한 사용자 정의 포트 범위를 예약할 수 있습니다.

자세한 내용은 [PAT에 대한 사용자 정의 소스 포트](#) 범위를 참조하십시오.

12.4(20)T2에서 NAT는 L3/L4 및 대칭 포트에 대한 포트 임의 설정을 도입합니다.

- 포트 임의 설정은 NAT가 소스 포트 요청에 대한 전역 포트를 임의로 선택할 수 있도록 합니다.

- 대칭 포트는 NAT가 **포인트 독립적으로 지원할 수 있도록 합니다.**

## Q. IP 프래그먼트화와 TCP 세그멘테이션은 어떻게릅니까?

A.IP 프래그먼트화는 레이어 3(IP)에서 발생하고 TCP 세그멘테이션은 레이어 4(TCP)에서 발생합니다. IP 프래그먼트화는 인터페이스의 MTU(Maximum Transmission Unit)보다 큰 패킷이 이 인터페이스 밖으로 전송될 때 발생합니다. 이러한 패킷은 인터페이스 외부로 전송될 때 프래그먼트화되거나 폐기되어야 합니다. 이 Don't Fragment (DF) 패킷의 IP 헤더에 비트가 설정되지 않아 패킷을 프래그먼트화할 수 있습니다. 패킷의 IP 헤더에 DF 비트가 설정되어 있으면 패킷이 삭제되고 다음 홉 MTU 값이 전송자에게 반환된다는 ICMP 오류 메시지가 표시됩니다. IP 패킷의 모든 프래그먼트는 IP 헤더에서 동일한 ID를 전달하며, 이를 통해 최종 수신자는 프래그먼트를 원래 IP 패킷으로 리어셈블할 수 있습니다. 자세한 내용은 [내용은 GRE 및 IPsec으로 IP 프래그먼트화, MTU, MSS 및 PMTUD 문제 해결을 참조하십시오.](#)

TCP 세그멘테이션은 엔드 스테이션의 애플리케이션이 데이터를 전송할 때 발생합니다. 애플리케이션 데이터는 TCP에서 가장 크기가 큰 청크로 간주하여 전송합니다. TCP에서 IP로 전달되는 이 데이터 단위를 세그먼트라고 합니다. TCP 세그먼트는 IP 데이터그램으로 전송됩니다. 그러면 이러한 IP 데이터그램이 네트워크를 통과할 때 IP 프래그먼트가 될 수 있으며, 통과될 수 있는 MTU 링크보다 더 낮은 MTU 링크가 나타납니다.

TCP는 먼저 이 데이터를 TCP 세그먼트(TCP MSS 값 기반)로 분할하고 TCP 헤더를 추가한 다음 이 TCP 세그먼트를 IP에 전달할 수 있습니다. 그런 다음 IP는 IP 헤더를 추가하여 패킷을 원격 엔드 호스트로 전송할 수 있습니다. TCP 세그먼트가 있는 IP 패킷이 TCP 호스트 간 경로의 발신 인터페이스에서 IP MTU보다 클 경우 IP는 IP/TCP 패킷을 조각화하여 맞출 수 있습니다. 이러한 IP 패킷 프래그먼트는 IP 레이어에 의해 원격 호스트에서 리어셈블될 수 있으며, 원래 전송되었던 전체 TCP 세그먼트를 TCP 레이어에 전달할 수 있습니다. TCP 레이어는 IP가 전송 중에 패킷을 조각화했다는 것을 알지 못합니다.

NAT는 IP 프래그먼트를 지원하지 않지만, TCP 세그먼트는 지원하지 않습니다.

## Q. NAT는 IP 프래그먼트화 및 TCP 세그멘테이션에 대해 비순차적(out-of-order)을 지원하지합니까?

A.NAT는 ofip 가상 리어셈블이므로 비순차적 IP 프래그먼트만 지원합니다.

## Q. IP 프래그먼트화 및 TCP 세그멘테이션을 디버깅하는 방법은 무엇입니까?

A.NAT는 IP 프래그먼트화 및 TCP 세그멘테이션에 동일한 디버그 CLI를 사용합니다.`debug ip nat frag.`

## Q. 지원되는 NAT MIB가 있습니까?

A.아니요. 지원되는 NAT MIB가 없거나 CISCO-IETF-NAT-MIB가 지원되지 않습니다.

## Q. TCP 시간 제한이란 무엇이며, NAT TCP 타이머와 어떤 관련이 있습니까?

A.3방향 핸드셰이크가 완료되지 않았고 NAT에서 TCP 패킷을 볼 경우 NAT는 60초 타이머를 시작할 수 있습니다. 3방향 핸드셰이크가 완료되면 NAT는 기본적으로 NAT 엔트리에 대해 24시간 타이머를 사용합니다. 엔드 호스트가 RESET을 전송하는 경우 NAT는 기본 타이머를 24시간에서 60초로 변경합니다. FIN의 경우 NAT는 FIN과 FIN-ACK을 수신하면 기본 타이머를 24시간에서 60초로

변경합니다.

**Q. NAT 변환에 걸리는 시간을 NAT 변환 테이블에서 시간 초과로 변경할 수 있습니까?**

A.예. 모든 항목 또는 다른 유형의 NAT 변환(예: udp-timeout, dns-timeout, tcp-timeout, first-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout 및 arp-ping-timeout)에 대한 NAT 시간 초과 값을 변경할 수 있습니다.

**Q. LDAP(Lightweight Directory Access Protocol)가 각 LDAP 응답 패킷에 추가 바이트를 연결할 때 LDAP를 중지하려면 어떻게 합니까?**

A.LDAP는 Search-Res-Entry 유형의 메시지를 처리하는 동안 추가 바이트(LDAP 검색 결과)를 추가하도록 설정됩니다. LDAP는 각 LDAP 응답 패킷에 10바이트의 검색 결과를 첨부합니다. 이 10바이트의 추가 데이터로 인해 패킷이 발생하고 네트워크의 MTU(Maximum Transmission Unit)를 초과하는 경우 패킷이 삭제됩니다. 이 경우, 패킷을 보내고 받기 위해 `CLIno ip nat service append-ldap-search-res` 명령을 사용하여 이 LDAP 동작을 끄는 것이 좋습니다.

**Q. NAT 상자의 내부 전역/외부 로컬 IP 주소에 대한 경로 권장 사항은 무엇입니까?**

A.A 경로는 NAT-NVI와 같은 기능의 내부 전역 IP 주소에 대해 NAT 구성 상자에 지정해야 합니다. 마찬가지로 외부 로컬 IP 주소에 대한 NAT 상자에도 경로를 지정해야 합니다. 이 경우 외부 고정 규칙이 있는 수신-발신 방향의 패킷에는 이러한 종류의 경로가 필요합니다. 이러한 시나리오에서는 IG/OL에 대한 경로를 제공하지만 다음 홉 IP 주소도 구성해야 합니다. 다음 홉 컨피그레이션을 찾을 수 없는 경우 컨피그레이션 오류로 간주되어 정의되지 않은 동작이 발생합니다.

NVI-NAT는 출력 기능 경로에만 있습니다. NAT-NVI를 사용하여 서브넷을 직접 연결했거나 박스에 구성된 외부 NAT 변환 규칙이 있는 경우 이러한 시나리오에서는 더미 Next Hop IP 주소와 Next Hop에 대한 관련 ARP를 제공해야 합니다. 이는 기본 인프라가 변환을 위해 패킷을 NAT에 전달하는 데 필요합니다.

**Q. Cisco IOS NAT는 log 키워드와 함께 ACL을 지원합니까?**

A. 동적 NAT 변환을 위해 Cisco IOS NAT를 구성할 때 ACL은 변환 가능한 패킷을 식별하는 데 사용됩니다. 현재 NAT 아키텍처는 log 키워드를 사용하는 ACL을 지원하지 않습니다.

## 음성 NAT

**Q. NAT는 CUCM(Cisco Unified Communications Manager) V7과 함께 제공되는 SCCP(Skinny Client Control Protocol) v17을 지원합니까?**

A.CUCM 7 및 CUCM 7의 모든 기본 전화기 로드는 SCCPv17을 지원합니다. 사용되는 SCCP 버전은 전화기가 등록될 때 CUCM과 전화기 간의 가장 일반적인 버전에 따라 결정됩니다.

NAT는 아직 SCCP v17을 지원하지 않습니다. SCCP v17에 대한 NAT 지원이 구현되기 전까지는 SCCP v16이 협상되도록 펌웨어를 버전 8-3-5 이하로 다운그레이드해야 합니다. CUCM6는 SCCP v16을 사용하는 한 어떤 전화기 로드에서도 NAT 문제가 발생할 수 없습니다. Cisco IOS는 현재 SCCP 버전 17을 지원하지 않습니다.

## Q. NAT에서 어떤 CUCM /SCCP/펌웨어 로드 버전을 지원합니까?

A. NAT는 CUCM 버전 6.x 및 이전 릴리스를 지원합니다. 이러한 CUCM 버전은 SCCP v15(또는 이전)를 지원하는 기본 8.3.x(또는 이전) 폰 펌웨어 로드와 함께 릴리스됩니다.

NAT는 CUCM 버전 7.x 이상 릴리스를 지원하지 않습니다. 이 CUCM 버전은 SCCP v17 이상을 지원하는 기본 8.4.x 전화기 펌웨어 로드와 함께 릴리스됩니다.

CUCM 7.x 이상을 사용하는 경우 NAT에서 지원하려면 전화기에서 SCCP v15 이전 버전의 펌웨어 로드를 사용하도록 CUCM TFTP 서버에 이전 펌웨어 로드를 설치해야 합니다.

## Q. RTP 및 RTCP에 대한 서비스 공급자 PAT 포트 할당 개선은 무엇입니까?

A. RTP 및 RTCP를 위한 서비스 공급자 PAT 포트 할당 개선은 SIP, H.323 및 Skinny 음성 통화에 대해 보장됩니다. RTP 스트림에 사용되는 포트 번호는 짝수 포트 번호이며 RTCP 스트림은 다음 홀수 포트 번호입니다. 포트 번호는 지정된 범위 내에서 RFC-1889를 준수하는 번호로 변환됩니다. 범위 내에 있는 포트 번호의 통화는 이 범위 내의 다른 포트 번호로 PAT 변환을 초래할 수 있습니다. 마찬가지로, 이 범위를 벗어난 포트 번호에 대한 PAT 변환은 지정된 범위 내의 번호로 변환할 수 없습니다.

## Q. SIP(Session Initiation Protocol)란 무엇이며 NAT를 통해 SIP 패킷을 라우팅할 수 있습니까?

A. SIP(Session Initiation Protocol)는 둘 이상의 엔드포인트 간에 통화를 설정, 유지 관리 및 종료하는 데 사용할 수 있는 ASCII 기반 애플리케이션 레이어 제어 프로토콜입니다. SIP는 IP를 통한 멀티미디어 컨퍼런싱을 위해 IETF(Internet Engineering Task Force)에서 개발한 대체 프로토콜입니다. Cisco SIP를 구현하면 지원되는 Cisco 플랫폼에서 IP 네트워크를 통해 음성 및 멀티미디어 통화를 설정할 수 있습니다. SIP 패킷은 NAT할 수 있습니다.

## Q. SBC(Session Border Controller)에 대한 Hosted NAT Traversal 지원이란 무엇입니까?

A. Cisco IOS Hosted NAT Traversal for SBC 기능을 사용하면 Cisco IOS NAT SIP ALG(Application-Level Gateway) 라우터가 Cisco Multiservice IP-to-IP 게이트웨이에서 SBC 역할을 할 수 있습니다. 이를 통해 VoIP(Voice over IP) 서비스를 원활하게 제공할 수 있습니다.

자세한 내용은 [세션 보더 컨트롤러에 대한 Cisco IOS 호스팅 NAT 접근 구성](#)을 참조하십시오.

## Q. 라우터 메모리와 CPU가 NAT로 처리할 수 있는 SIP, Skinny 및 H323 통화의 수는 몇 개입니까?

A. NAT 라우터에서 처리하는 통화 수는 상자에서 사용할 수 있는 메모리 양과 CPU의 처리 능력에 따라 달라집니다.

## Q. NAT 라우터는 Skinny 및 H323 패킷의 TCP 세그멘테이션을 지원합니까?

A. Cisco IOS-NAT는 H323의 TCP 세그멘테이션 및 SKINNY의 TCP 세그멘테이션 지원을 지원합니다.

**Q. 음성 구축에서 NAT 오버로드 컨피그레이션을 사용할 때 주의해야 할 사항이 있습니까?**

A.예. NAT 오버로드 컨피그레이션 및 음성 구축이 있는 경우 NAT를 통과하고 이 내부 장치에 연결하기 위해 out->in에 대한 연결을 생성하려면 등록 메시지가 필요합니다. 내부 디바이스는 주기적으로 이 등록을 전송하고 NAT는 시그널링 메시지에서처럼 정보에서 이 핀-홀/연관을 업데이트합니다

**Q. 음성 구축에서 clear ip nat trans \*명령 또는 clear ip nat trans forced 명령을 사용할 때 발생하는 알려진 문제가 있습니까?**

A. clear ip nat trans \*명령 또는 clear ip nat trans forced 명령을 실행하고 동적 NAT가 있는 음성 구축에서는 핀 홀/연결을 지우고 내부 디바이스에서 다음 등록 주기를 기다려야 이 설정이 다시 설정됩니다. 음성 구축에서는 이러한 clear 명령을 사용하지 않는 것이 좋습니다.

**Q. NAT는 공동 배치 음성 솔루션을 지원합니까?**

A.아니요. 같은 위치의 솔루션은 현재 지원되지 않습니다. NAT를 사용한 다음 구축(같은 상자)은 CME/DSP-Farm/SCCP/H323과 같은 공동 배치 솔루션으로 간주됩니다.

**Q. NVI는 Skinny ALG, H323 ALG 및 TCP SIP ALG를 지원합니까?**

A.아니요. 대부분의 구축에서 사용되는 UDP SIP ALG는 영향을 받지 않습니다.

## VRF/MPLS를 사용하는 NAT

**Q. NAT 라우터가 VRF의 동일한 주소 공간과 전역 주소 공간에서 스스로를 지원할 수 있습니까? 현재 다음과 같은 경고가 표시됩니다. "% 유사한 정적 항목(10.1.1.1 -> 10.2.2.2)이 이미 있습니다." 이 항목을 구성하려고 할 때 다음과 같이 표시됩니다**

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

A. 레거시 NAT는 서로 다른 VRF를 통한 중복 주소 컨피그레이션을 지원합니다. 규칙에서 match-in-vrfoption을 사용하여 겹침을 구성하고 특정 VRF를 통한 트래픽에 대해 동일한 VRF에서 uip nat 내부/외부로 설정해야 합니다. 중복 지원에는 전역 라우팅 테이블이 포함되지 않습니다.

서로 다른 VRF에 대해 겹치는 VRF 고정 NAT 엔트리에 대해 match-in-vrff 키워드를 추가해야 합니다. 그러나 전역 NAT 주소와 vrf NAT 주소는 중복될 수 없습니다.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

**Q. 레거시 NAT는 VRF-Lite(VRF에서 다른 VRF로의 경로)를 지원합니까?**

A.아니요. 서로 다른 VRF 간에 NAT를 수행하려면 NVI를 사용해야 합니다. 레거시 NAT를 사용하여 VRF에서 전역 또는 동일한 VRF 내의 NAT로의 NAT를 수행할 수 있습니다.

# NAT NVI

## Q. NAT NVI란 무엇입니까?

A.NVI는 NAT Virtual Interface를 나타냅니다. 이를 통해 NAT는 서로 다른 두 VRF 간에 변환할 수 있습니다. 이 솔루션은 Stick의 Network Address Translation 대신 사용해야 합니다.

## Q. NAT NVI를 사용하여 전역 인터페이스와 VRF 인터페이스 간에 라우팅해야 합니까?

A.Cisco에서는 VRF용 레거시 NAT를 전역 NAT(ip nat inside/out) 및 동일한 VRF의 인터페이스 간에 사용하는 것을 권장합니다. NVI는 서로 다른 VRF 간의 NAT에 사용됩니다.

## Q. NAT-NVI에 대한 TCP 세그멘테이션은 지원됩니까?

A. NAT-NVI에 대한 TCP 세그멘테이션은 지원되지 않습니다.

## Q. NVI는 Skinny ALG, H323 ALG 및 TCP SIP ALG를 지원합니까?

A.아니요. 대부분의 구축에서 사용되는 UDP SIP ALG는 영향을 받지 않습니다.

## Q. SNAT에서 TCP 세그멘테이션을 지원합니까?

A.SNAT는 어떤 TCP ALG(예: SIP, SKINNY, H323 또는 DNS)도 지원하지 않습니다. 따라서 TCP 세그멘테이션은 지원되지 않습니다. 그러나 UDP SIP 및 DNS는 지원됩니다.

## 스낫

## Q: SNAT(Stateful NAT)란 무엇입니까?

A.SNAT를 사용하면 둘 이상의 네트워크 주소 변환기가 변환 그룹으로 작동할 수 있습니다. 변환 그룹의 한 멤버가 IP 주소 정보의 변환이 필요한 트래픽을 처리합니다. 또한 활성 플로우가 발생하면 백업 변환기에 알립니다. 그러면 백업 번역기는 활성 번역기의 정보를 사용하여 중복된 번역 테이블 엔트리를 준비할 수 있다. 따라서 심각한 장애로 인해 활성 변환기가 방해를 받는 경우 트래픽이 백업으로 신속하게 전환될 수 있습니다. 동일한 네트워크 주소 변환이 사용되고 해당 변환의 상태가 이전에 정의되었으므로 트래픽 흐름이 계속됩니다.

## Q. SNAT에서는 TCP 세그멘테이션이 지원됩니까?

A.SNAT는 어떤 TCP ALG(예: SIP, SKINNY, H323 또는 DNS)도 지원하지 않습니다. 따라서 TCP 세그멘테이션은 지원되지 않습니다. 그러나 UDP SIP 및 DNS는 지원됩니다.

## Q. SNAT는 비대칭 라우팅을 지원합니까?

A. 비대칭 라우팅은 NAT를 활성화할 때 NAT를 지원합니다 as-queuing . 기본적으로 as-queueing은 활성화되어 있습니다. 그러나 12.4(24)T 이후부터는 as-queuing 은(는) 더 이상 지원되지 않습니다. 비대칭 라우팅이 올바르게 작동하려면 패킷이 제대로 라우팅되고 적절한 지연이 추가되었는지 확인

해야 합니다.

## NAT-PT(v6~v4)

### Q. NAT-PT란 무엇입니까?

A. NAT-PT는 NAT에 대한 v4-v6 변환입니다. NAT-PT(Protocol Translation)는 RFC 2765 및 RFC 2766에 정의된 대로 IPv6-IPv4 변환 메커니즘이며, IPv6 전용 디바이스가 IPv4 전용 디바이스와 통신할 수 있도록 하며 그 반대의 경우도 가능합니다.

### Q. NAT-PT는 CEF(Cisco Express Forwarding) 경로에서 지원됩니까?

A. NAT-PT는 CEF 경로에서 지원되지 않습니다.

### Q. NAT-PT에서는 어떤 ALG가 지원됩니까?

A. NAT-PT는 TFTP/FTP 및 DNS를 지원합니다. NAT-PT에서는 음성 및 SNAT가 지원되지 않습니다.

### Q. ASR 1004는 NAT-PT를 지원합니까?

A. ASR(Aggregation Services Router)은 NAT64를 사용합니다.

## 플랫폼에 의존하는 Cisco 7600/6k

### Q. SX Train의 Catalyst 6500에서 SNAT(Stateful NAT)를 사용할 수 있습니까?

SX 열차의 Catalyst 6500에서는 A.SNAT를 사용할 수 없습니다.

### Q. VRF 인식 NAT는 6k의 하드웨어에서 지원됩니까?

A. VRF 인식 NAT는 이 플랫폼의 하드웨어에서 지원되지 않습니다.

### Q. 7600 및 Cat6000은 VRF 인식 NAT를 지원합니까?

A. 65xx/76xx 플랫폼에서는 VRF 인식 NAT가 지원되지 않으며 CLI가 차단됩니다.

참고: 가상 컨텍스트 투명 모드에서 실행되는 FWSM을 활용하는 경우 설계를 구현할 수 있습니다.

## 플랫폼에 의존하는 Cisco 850

### Q. Cisco 850은 릴리스 12.4T에서 Skinny NAT ALG를 지원합니까?

A. 아니요. 850 Series의 12.4T에서는 Skinny NAT ALG를 지원하지 않습니다.

# NAT 구축

## Q. NAT는 어떻게 구현합니까?

A. NAT는 등록되지 않은 IP 주소를 사용하는 사설 IP 인터넷워크를 인터넷에 연결할 수 있도록 합니다. NAT는 패킷이 다른 네트워크로 전달되기 전에 내부 네트워크의 프라이빗(RFC1918) 주소를 합법적인 라우팅 가능 주소로 변환합니다.

## Q. NAT with voice는 어떻게 구현합니까?

A. NAT의 음성 지원 기능을 사용하면 NAT(Network Address Translation)로 구성된 라우터를 통과한 SIP 포함 메시지를 패킷으로 다시 변환할 수 있습니다. ALG(Application Layer Gateway)는 음성 패킷을 변환하는 데 NAT와 함께 사용됩니다.

## Q. NAT를 MPLS VPN과 어떻게 통합합니까?

A. NAT와 MPLS VPN의 통합 기능을 사용하면 여러 MPLS VPN을 단일 디바이스에서 구성하여 함께 작동할 수 있습니다. NAT는 MPLS VPN이 모두 동일한 IP 주소 지정 체계를 사용하더라도 어떤 MPLS VPN에서 IP 트래픽을 수신하는지 구분할 수 있습니다. 이러한 개선을 통해 여러 MPLS VPN 고객이 서비스를 공유하는 동시에 각 MPLS VPN이 완전히 다른 MPLS VPN과 분리됩니다.

## Q. NAT 고정 매핑은 고가용성을 위해 HSRP를 지원합니까?

A. NAT(Network Address Translation) 고정 매핑으로 구성되고 라우터가 소유한 주소에 대해 ARP(Address Resolution Protocol) 쿼리가 트리거되면 NAT는 ARP가 가리키는 인터페이스의 BIA MAC 주소에 응답합니다. 2개의 라우터가 HSRP 활성화 및 대기 상태로 작동합니다. NAT 내부 인터페이스는 그룹에 속하도록 활성화 및 구성해야 합니다.

## Q. NAT NVI는 어떻게 구현해야 합니까?

A. NAT NVI(가상 인터페이스) 기능은 인터페이스를 NAT 내부 또는 NAT 외부로 구성해야 하는 요구 사항을 제거합니다.

## Q. NAT로 로드 밸런싱을 구현하려면 어떻게 해야 합니까?

A. NAT를 사용하여 수행할 수 있는 로드 밸런싱에는 두 가지 종류가 있습니다. 즉, 인바운드 서버를 서버 집합에 로드 밸런싱하여 서버에 로드를 분산시킬 수 있으며, 둘 이상의 ISP를 통해 사용자 트래픽을 인터넷으로 로드 밸런싱할 수 있습니다.

아웃바운드 로드 밸런싱에 대한 자세한 내용은 [Cisco IOS NAT Load-Balancing for Two ISP Connections](#)를 참조하십시오.

## Q. IPSec과 함께 NAT를 구현하려면 어떻게 해야 합니까?

A. Cisco는 IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT 및 IPSec NAT 투명성.

IPSec ESP through NAT 기능은 오버로드 또는 PAT(Port Address Translation) 모드로 구성된 Cisco IOS NAT 디바이스를 통해 여러 개의 동시 IPSec ESP 터널 또는 연결을 지원하는 기능을 제공합니다. IPSec NAT 투명성 기능에서는 NAT와 IPSec 간의 알려진 여러 비호환성 문제를 해결할

때 IPSec 트래픽이 네트워크의 NAT 또는 PAT 지점을 통과할 수 있도록 지원합니다.

## Q. NAT-PT는 어떻게 구현합니까?

A. NAT-PT(Network Address Translation—Protocol Translation)는 RFC 2765 및 RFC 2766에 정의된 대로 IPv6-IPv4 변환 메커니즘으로, IPv6 전용 디바이스가 IPv4 전용 디바이스와 통신할 수 있도록 하며 그 반대의 경우도 가능합니다.

## Q. 멀티캐스트 NAT는 어떻게 구현합니까?

A. 멀티캐스트 스트림에 대한 소스 IP를 NAT할 수 있습니다. 멀티캐스트를 위한 동적 NAT가 완료되면 경로 맵을 사용할 수 없으며, 액세스 목록만 지원됩니다.

자세한 내용은 멀티캐스트 NAT가 [Cisco 라우터에서 작동하는 방식을 참조하십시오](#). 대상 멀티캐스트 그룹은 NAT와 Multicast Service Reflection 솔루션을 사용합니다.

## Q. SNAT(stateful NAT)는 어떻게 구현합니까?

A. SNAT는 동적으로 매핑된 NAT 세션에 대해 연속 서비스를 활성화합니다. 정적으로 정의된 세션은 SNAT 없이도 이중화의 이점을 누릴 수 있습니다. SNAT가 없을 경우, 동적 NAT 매핑을 사용하는 세션은 심각한 장애가 발생할 경우 중단되며 다시 설정해야 합니다. 최소 SNAT 컨피그레이션만 지원됩니다. 향후 구축은 Cisco 어카운트 팀과 논의한 후에만 수행되어야 현재 제한과 관련된 설계를 검증할 수 있습니다.

다음 시나리오에서는 SNAT를 사용하는 것이 좋습니다.

- HSRP에 비해 일부 기능이 없으므로 기본/백업은 권장되는 모드가 아닙니다.
- 장애 조치 시나리오 및 2-라우터 설정 즉, 한 라우터가 충돌할 경우 다른 라우터가 원활하게 작업을 인계받습니다. SNAT 아키텍처는 인터페이스 폴랩을 처리하도록 설계되지 않았습니다.
- 비비대칭 라우팅 시나리오가 지원됩니다. 비대칭 라우팅은 응답 패킷의 레이턴시가 SNAT 메시지 교환을 위한 2개의 SNAT 라우터 간의 레이턴시보다 높은 경우에만 처리할 수 있습니다.

현재 SNAT 아키텍처는 견고성을 처리하도록 설계되지 않았으므로 다음 테스트는 성공하지 못할 것으로 예상됩니다.

- 트래픽이 있는 동안 NAT 항목이 지워지는 경우.
- 트래픽이 있는 동안 인터페이스 매개변수(예: IP 주소 변경, shut/no-shut 등)가 변경된 경우
- SNAT specific clear or show commands는 제대로 실행되지 않을 것으로 예상되며 권장되지 않습니다. 일부 SNAT 관련 clear and show command는 다음과 같습니다.

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer >
sh ip snat distributed verbose
sh ip snat peer < IP address of peer >
```

- 사용자가 항목을 지우려면 clear ip nat trans forced or clear ip nat trans \* 명령을 사용할 수 있습니다. 사용자가 항목을 보려면 show ip nat translation, show ip nat translations verbose, show

`ip nat stats` 명령을 사용할 수 있습니다. 서비스 내부가 구성된 경우 SNAT 관련 정보도 표시할 수 있습니다.

- 백업 라우터에서 NAT 변환이 지워지는 것은 권장되지 않습니다. 항상 기본 SNAT 라우터의 NAT 엔트리를 지웁니다.
- SNAT는 HA가 아니므로 두 라우터의 컨피그레이션이 동일해야 합니다. 두 라우터 모두 동일한 이미지를 실행해야 합니다. 또한 두 SNAT 라우터에 사용되는 기본 플랫폼이 동일한지 확인합니다.

## NAT 모범 사례

### Q. NAT 모범 사례가 있습니까?

A.예. 다음은 NAT 모범 사례입니다.

1. 동적 NAT와 고정 NAT를 모두 사용할 경우, 동적 NAT에 대한 규칙을 설정하는 ACL은 겹치지 않도록 고정 로컬 호스트를 제외해야 합니다.
2. permit ip가 있는 NAT에 ACL을 사용하는 경우 예측할 수 없는 결과를 얻을 수 있습니다. 12.4(20)T 이후에 NAT는 로컬에서 생성된 HSRP 및 라우팅 프로토콜 패킷이 외부 인터페이스 외부로 전송되는 경우 및 NAT 규칙과 일치하는 로컬에서 암호화된 패킷을 변환할 수 있습니다.
3. NAT에 대해 중복되는 네트워크가 있는 경우 `match-in-vrf` 키워드를 사용합니다. 서로 다른 VRF에 대해 겹치는 VRF 고정 NAT 엔트리에 대해 `match-in-vrf` 키워드를 추가해야 하지만 전역 및 vrf NAT 주소를 겹칠 수는 없습니다.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

4. `match-in-vrfq` 키워드를 사용하지 않는 한 주소 범위가 같은 NAT 풀을 다른 VRF에서 사용할 수 없습니다. 예를 들면 다음과 같습니다.

```
ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
ip nat pool poolB 172.31.1.1 172.31.1.10 prefix-length 24
ip nat inside source list 1 poolA vrf A match-in-vrf
ip nat inside source list 2 poolB vrf B match-in-vrf
```

**참고:** CLI 컨피그레이션이 유효하더라도 `match-in-vrf` 키워드가 없으면 컨피그레이션이 지원되지 않습니다.

5. NAT 인터페이스 오버로드를 사용하여 ISP 로드 밸런싱을 구축할 때 모범 사례는 route-map을 인터페이스 match over ACL 매칭과 함께 사용하는 것입니다.
6. 풀 매핑을 사용할 때 동일한 NAT 풀 주소를 공유하기 위해 서로 다른 두 매핑(ACL 또는 route-map)을 사용해서는 안 됩니다.
7. 장애 조치 시나리오에서 서로 다른 두 라우터에 동일한 NAT 규칙을 구축할 경우 HSRP 이중화를 사용해야 합니다.
8. 고정 NAT 및 동적 풀에서 동일한 내부 전역 주소를 정의하지 마십시오. 이러한 행동은 바람직하지 않은 결과를 초래할 수 있다.

## 관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.