

# NAT가 ICMP 프래그먼트를 처리하는 방법

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[사례 1](#)

[사례 2](#)

[사례 3](#)

[요약](#)

[관련 정보](#)

## 소개

이 문서에서는 NAT 오버로드를 구성할 때 NAT(Network Address Translation)가 ICMP(Internet Control Message Protocol) 프래그먼트를 처리하는 방법에 대해 설명합니다. NAT 오버로딩에 대한 자세한 내용은 NAT [FAQ를 참조하십시오](#).

ICMP 프래그먼트의 처리는 NAT 변환 테이블의 상태 및 NAT 라우터가 ICMP 프래그먼트를 수신하는 순서에 따라 달라집니다. 세 가지 다른 사례를 살펴보겠습니다. 여기서는 각각 길이가 3600바이트(3개의 IP 프래그먼트)인 두 개의 ping을 172.16.0.1에서 172.17.1.2으로 보냅니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

## 사례 1

이 시나리오에서는 NAT가 변환 테이블에 완전히 확장된 변환 엔트리를 생성하는 것을 볼 수 있습니다.

니다. 이 작업이 완료되고 NAT 풀에 다른 사용 가능한 주소가 없으면 NAT는 패킷의 첫 번째 프래그먼트(fragment 0) 이전에 수신된 프래그먼트를 삭제합니다.

시작할 때 풀의 한 주소만 오버로드를 수행합니다. NAT 변환 테이블이 비어 있습니다. NAT 컨피그레이션은 다음과 같이 표시됩니다.

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

패킷이 NAT 라우터에 도달하기 시작하면 어떤 일이 발생하는지 살펴보겠습니다.

1. 패킷 1 프래그먼트 0이 도착하고 NAT는 완전한 확장 변환 엔트리를 생성합니다. 그런 다음 NAT는 패킷 1 프래그먼트 0을 변환하고 전달합니다. 이제 변환 테이블이 다음과 같이 나타납니다.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24320	172.16.0.1:24320	172.17.1.2:24320	172.17.1.2:24320

위의 변환 테이블에서 24320을 확인합니다. IP 데이터그램의 ICMP 헤더에 포함된 ICMP IDENT 값입니다. IP 데이터그램의 0조각만 이 ICMP 헤더를 포함합니다. 여러 프래그먼트가 동일한 패킷의 일부인지 확인하려면 NAT가 원래 IP 데이터그램의 모든 프래그먼트의 IP 헤더에 있는 IP ID 값을 추적해야 합니다. 여러 프래그먼트가 확장 변환을 생성한 프래그먼트 0과 동일한 IP ID 값을 갖는 경우 NAT는 동일한 확장 변환 엔트리를 사용하여 이러한 프래그먼트를 변환합니다. IP 식별 필드에 대한 자세한 내용은 RFC [791](#) 을 참조하십시오. ICMP 식별 필드에 대한 자세한 내용은 RFC 792 를 참조하십시오.
2. 패킷 1 프래그먼트 2 및 패킷 1 프래그먼트 1이 도착합니다. 이러한 프래그먼트는 프래그먼트 0(변환을 생성함)을 포함하는 동일한 패킷의 일부이므로 NAT는 위의 변환 엔트리를 사용하여 이러한 프래그먼트를 변환하고 전달합니다. 대상 디바이스는 패킷 1에 대한 모든 프래그먼트를 수신하고 응답을 보냅니다.
3. 패킷 2 프래그먼트 1이 도착합니다. 이 패킷은 새 패킷이므로 IP ID 값이 NAT에서 기록한 패킷과 일치하지 않습니다. 따라서 NAT는 기존 변환을 사용할 수 없습니다. 또한 완전히 확장된 변환 항목이 이미 있고 또 다른 변환을 만들 ICMP ID가 없으므로 새 변환을 만들 수 없습니다. NAT는 패킷 2 프래그먼트 1을 삭제합니다.
4. 패킷 2 프래그먼트 0이 도착합니다. ICMP ID가 일치하므로 NAT는 위의 변환을 사용할 수 있습니다. (단일 ping 집합 내의 모든 ping은 동일한 ICMP ID 번호를 사용합니다.) 이 시점에서 NAT는 이 패킷의 IP ID를 기록합니다. NAT는 패킷 2 프래그먼트 0을 변환하고 전달합니다.
5. 패킷 2 프래그먼트 2가 도착합니다. 이제 NAT는 IP ID 값이 이전 단계에서 기록된 하나의 NAT와 일치하므로 위의 변환을 사용할 수 있습니다. NAT는 패킷 2 프래그먼트 2를 변환하고 전달합니다. 목적지 디바이스는 프래그먼트 0과 2(프래그먼트 1이 누락됨)만 수신하므로 응답을 보내지 않습니다.

## 사례 2

이 시나리오에서는 첫 번째 프래그먼트(fragment 0)가 아닌 프래그먼트가 먼저 도착하면 NAT가 간단한 변환을 생성하는 것으로 확인됩니다. 단, NAT 풀의 주소가 완전히 확장된 변환에서 아직 사용되지 않는 한.

시작할 때 NAT 풀에는 하나의 주소만 있고 NAT 변환 테이블은 비어 있으며 컨피그레이션은 다음과 같이 표시됩니다.

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

1. 패킷 1 프래그먼트 1이 도착합니다.이 프래그먼트에 ICMP ID 정보가 없으므로 NAT가 변환 테이블에서 전체 확장 변환을 생성할 수 없습니다.그러나 완전한 확장 변환이 없는 경우에는 NAT에서 간단한 변환을 시작합니다.그런 다음 NAT는 패킷 1 프래그먼트 1을 변환하고 전달합니다. 변환 항목은 다음과 같이 나타납니다.

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---

2. 패킷 1 프래그먼트 0이 도착합니다.이 프래그먼트에 ICMP ID 정보가 포함되므로 NAT는 완전히 확장된 변환 엔트리를 입력합니다.

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.3	172.16.0.1	---	---
icmp	10.10.10.3:24321	172.16.0.1:24321	172.17.1.2:24321	172.17.1.2:24321

그런 다음 NAT는 IP ID 정보를 기록하고 패킷 1 프래그먼트 0을 변환하고 전달합니다.

3. 패킷 1 프래그먼트 2가 도착합니다.이 프래그먼트는 NAT가 2단계에서 기록한 것과 동일한 IP ID 정보를 가지므로 NAT는 완전히 확장된 변환을 사용하여 패킷 1 프래그먼트 2를 변환하고 전달합니다.대상 장치는 모든 프래그먼트와 응답을 수신합니다.이 시점에서 NAT 변환 테이블이 지워지거나 시간이 초과될 때까지 모든 ping이 성공합니다.

### 사례 3

이 시나리오에서는 첫 번째 프래그먼트(fragment 0)가 아닌 프래그먼트가 먼저 도착하면 NAT가 간단한 변환을 생성하는 것으로 확인됩니다. 단, NAT 풀의 주소가 완전히 확장된 변환에서 아직 사용되지 않는 한.NAT 테이블의 확장 변환에서 이미 주소를 사용하는 경우 각 프래그먼트 소스 주소를 다른 주소로 변환하는 NAT의 위험이 발생합니다.

시작할 때 NAT 풀에 있는 둘 이상의 주소가 오버로드를 수행하고 변환 테이블에 이미 확장 변환이 적용되었으며 컨피그레이션은 다음과 같습니다.

```
ip nat pool POOL1 10.10.10.3 10.10.10.5 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

변환 테이블은 다음과 같이 표시됩니다.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

1. 패킷 1 프래그먼트 1이 도착합니다.이 프래그먼트에 ICMP ID 정보가 없으므로 NAT는 전체 확장 변환 테이블 항목을 생성할 수 없으며, 이 IP 주소에 대한 기존 확장 항목이 있으므로 주소 10.10.10.3에 대한 단순 변환 항목을 생성할 수 없습니다.NAT는 다음 무료 IP 주소 (10.10.10.4)을 선택하고 간단한 변환을 생성합니다.그런 다음 NAT는 패킷 1 프래그먼트 1을 변환하고 전달합니다. 이제 변환 테이블이 다음과 같이 나타납니다.

Pro	Inside global	Inside local	Outside local	Outside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322

2. 패킷 1 프래그먼트 0이 도착합니다.이 프래그먼트에 ICMP ID 정보가 포함되므로 NAT는 주소 10.10.10.3에 대해 완전히 확장된 변환 엔트리를 입력하고 이 패킷에 대한 IP ID 정보를 기록합니다.그런 다음 NAT는 패킷 1 프래그먼트 0을 변환하고 전달합니다. 이제 변환 테이블이다

음과 같이 나타납니다.

Proto	Inside global	Inside local	Outside local	Outside global
---	10.10.10.4	172.16.0.1	---	---
icmp	10.10.10.3:24322	172.16.0.1:24322	172.17.1.2:24322	172.17.1.2:24322
icmp	10.10.10.3:24323	172.16.0.1:24323	172.17.1.2:24323	172.17.1.2:24323

- 패킷 1 프래그먼트 2가 도착합니다. IP ID 정보는 2단계에서 기록된 하나의 NAT와 일치하므로 NAT는 2단계에서 생성한 전체 확장 변환을 사용하여 패킷 1 프래그먼트 2를 변환하고 전달합니다. 이 시점에서 대상 디바이스는 패킷 1의 모든 프래그먼트를 수신하지만 프래그먼트 0과 2의 소스 주소가 10.10.10.3으로 변환되고 프래그먼트 1이 10.10.10.4으로 변환되었습니다. 따라서 대상 디바이스는 패킷을 리어셈블할 수 없으며 응답을 보내지 않습니다.
- 패킷 2 프래그먼트 0이 도착합니다. NAT는 위의 전체 확장 변환을 사용하거나 fragment ICMP ident 필드의 값에 따라 새로운 완전 확장 변환을 생성합니다. 두 경우 모두 NAT는 IP ID 정보를 기록합니다. 그런 다음 NAT는 패킷 2 프래그먼트 0을 변환하고 전달합니다.
- 패킷 2 프래그먼트 2가 도착합니다. IP ID 정보는 4단계에서 기록한 NAT와 일치하므로 NAT는 4단계에서 생성한 두 번째 완전 확장 변환을 사용합니다. NAT는 패킷 2 프래그먼트 2를 변환하고 전달합니다.
- 패킷 2 프래그먼트 1이 도착합니다. IP ID 정보는 4단계에서 기록한 NAT와 일치하므로 NAT는 4단계에서 생성한 두 번째 완전 확장 변환을 사용합니다. NAT는 패킷 2 프래그먼트 1을 변환하고 전달합니다. 대상 디바이스는 동일한 소스(10.10.10.3)에서 패킷 2의 세 개의 프래그먼트를 모두 수신하므로 패킷과 회신을 리어셈블합니다.

## 요약

NAT가 ICMP 프래그먼트를 삭제하거나 전달할지 여부는 NAT 라우터가 프래그먼트를 수신하는 순서 및 그 당시의 변환 테이블 상태에 따라 달라집니다. 특정 조건에서 NAT는 프래그먼트를 다르게 변환하므로 대상 디바이스에서 패킷을 리어셈블할 수 없습니다.

## 관련 정보

- [NAT 지원 페이지](#)
- [IP 라우팅 지원 페이지](#)
- [Technical Support - Cisco Systems](#)