

NAT 작동 순서 이해

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[NAT 개요](#)

[NAT 구성 및 출력](#)

[관련 정보](#)

소개

이 문서에서는 패킷이 네트워크 내부 또는 외부로 이동하는 방향을 기준으로 NAT를 통해 처리되는 순서 트랜잭션에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- NAT(Network Address Translation)에 대해 자주 묻는 질문 중 일부에 대한 답변을 제공합니다. NAT에 대한 자세한 내용은 [NAT 작동 방식을 참조하십시오](#).

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® Software 릴리스 12.2(27)를 기반으로 합니다.

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

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

이 문서에서는 트랜잭션이 NAT(Network Address Translation)로 처리되는 순서가 패킷이 내부 네트워크에서 외부 네트워크로 이동하는지, 또는 외부 네트워크에서 내부 네트워크로 이동하는지에 따라 결정된다는 점을 설명합니다.

NAT 개요

이 표에서 NAT가 전역-로컬 또는 로컬-전역 변환을 수행하는 경우 각 흐름에서 변환이 달라집니다.

안과 밖

- IPSec인 경우 입력 액세스 목록을 확인합니다.
- 암호 해독 - CET(Cisco Encryption Technology) 또는 IPSec
- 입력 액세스 목록 확인
- 입력 속도 제한 확인
- 입력 회계
- 웹 캐시로 리디렉션
- 정책 라우팅
- 경로 지정
- **NAT 내부-외부(로컬-전역 변환)**
- crypto(map 및 mark for encryption 확인)
- 출력 액세스 목록 확인
- inspect(CBAC(Context-based Access Control))
- TCP 가로채기
- 암호화
- 큐

외부에서 내부로

- IPSec인 경우 입력 액세스 목록을 확인합니다.
- 암호 해독 - CET 또는 IPSec용
- 입력 액세스 목록 확인
- 입력 속도 제한 확인
- 입력 회계
- 웹 캐시로 리디렉션
- **NAT outside to inside(전역-로컬 변환)**
- 정책 라우팅
- 경로 지정
- crypto(map 및 mark for encryption 확인)
- 출력 액세스 목록 확인
- CBAC 검사
- TCP 가로채기
- 암호화
- 큐

NAT 구성 및 출력

이 예에서는 작업 순서가 NAT에 미치는 영향을 보여 줍니다. 이 경우 NAT 및 라우팅만 표시됩니다.

이전 예에서 Router-A는 이 컨피그레이션에 표시된 대로 내부 로컬 주소 172.31.200.48을 172.16.47.150으로 변환하도록 구성됩니다.

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname Router-A  
!  
enable password ww  
!  
ip nat inside source static 172.31.200.48 172.16.47.150  
  
!--- This command creates a static NAT translation  
!--- between 172.31.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server  
172.31.2.132 ! interface Ethernet0 no ip address shutdown ! interface Serial0 ip address  
172.16.47.161 255.255.255.240 ip nat inside  
  
!--- Configures Serial0 as the NAT inside interface no ip mroute-cache no ip route-cache no  
fair-queue ! interface Serial1 ip address 172.16.47.146 255.255.255.240 ip nat outside  
  
!--- Configures Serial1 as the NAT outside interface no ip mroute-cache no ip route-cache ! no  
ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145  
  
!--- Configures a default route to 172.16.47.145 ip route 172.31.200.0 255.255.255.0
```

172.16.47.162 !! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
변환 테이블은 원하는 변환이 존재함을 나타냅니다.

Router-A#**show ip nat translation**

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.47.150	172.31.200.48	---	---

이 출력은 **debug ip packet detail** 및 **debug ip nat**가 활성화된 라우터-A에서, 그리고 172.16.47.142로 향하는 디바이스 172.31.200.48에서 실행된 ping에서 가져옵니다.

참고: Debug 명령은 상당한 양의 출력을 생성합니다. IP 네트워크의 트래픽이 낮아 시스템의 다른 활동에 부정적인 영향을 주지 않는 경우에만 사용하십시오. debug 명령을 실행하기 전에 [Debug 명령에 대한 중요 정보를 참조하십시오.](#)

```
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

이전 출력에는 NAT 디버그 메시지가 없으므로 현재 고정 변환이 사용되지 않으며 라우터의 라우팅 테이블에 대상 주소(172.16.47.142)에 대한 경로가 없습니다. 라우팅할 수 없는 패킷의 결과는 [ICMP Unreachable 메시지](#)이며, 이는 내부 장치로 전송됩니다.

그러나 Router-A의 기본 경로는 172.16.47.145입니다. 그러면 경로가 라우팅할 수 없는 것으로 간주되는 이유는 무엇입니까?

Router-A에 **ip 클래스**가 구성되지 않았습니다. 즉, 서브넷이 라우팅 테이블에 있는 "주요" 네트워크 주소(이 경우 172.16.0.0)를 목적지로 하는 패킷이 있으면 라우터가 기본 경로를 사용하지 않습니다. 즉, **no ip classless** 명령을 실행하면 라우터가 가장 긴 비트 일치로 경로를 찾는 기능이 꺼집니다. 이 동작을 변경하려면 Router-A에서 **ip 클래스**를 구성해야 합니다. **ip classless** 명령은 Cisco IOS Software Releases 11.3 이상을 사용하는 Cisco 라우터에서 기본적으로 활성화됩니다.

Router-A#**configure terminal**

Enter configuration commands, one per line. End with CTRL/Z.

Router-A(config)#**ip classless**

Router-A(config)#**end**

Router-A#**show ip nat translation**

%SYS-5-CONFIG_I: Configured from console by console nat tr

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.47.150	172.31.200.48	---	---

이전에 수행한 것과 동일한 ping 테스트를 반복하면 패킷이 변환되고 ping이 성공한 것을 확인할 수 있습니다.

Ping Response on device 172.31.200.48

```
D:\>ping 172.16.47.142
```

```
Pinging 172.16.47.142 with 32 bytes of data:
```

```
Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
```

```
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
```

```
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
```

```
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
```

```
Ping statistics for 172.16.47.142:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Debug messages on Router A indicating that the packets generated by device 172.31.200.48 are getting translated by NAT.

```
Router-A#
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.31.200.48 (Serial0), d=172.16.47.142 (Serial1), routed via RIB
```

```
*Mar 28 03:34:28: NAT: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [160]
```

```
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1), g=172.16.47.145, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=8, code=0
```

```
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [160]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), g=172.16.47.162, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [161]
```

```
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [161]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), g=172.16.47.162, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [162]
```

```
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [162]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), g=172.16.47.162, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [163]
```

```
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [163]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), g=172.16.47.162, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [164]
```

```
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [164]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0), g=172.16.47.162, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
Router-A#undebg all
```

```
All possible debugging has been turned off
```

앞의 예에서는 패킷이 내부에서 외부로 이동할 때 NAT 라우터가 라우팅 테이블에서 계속해서 패킷을 변환하기 전에 외부 주소로의 경로를 확인하는 것을 보여 줍니다. 따라서 NAT 라우터에 외부 네트워크에 대한 유효한 경로가 있어야 합니다. 목적지 네트워크로의 경로는 라우터 컨피그레이션에서 NAT outside로 정의된 [인터페이스](#)를 통해 알아야 합니다.

반환 패킷은 라우팅되기 전에 변환됩니다. 따라서 NAT 라우터에는 라우팅 테이블의 [내부 로컬](#) 주소에 대한 유효한 [경로도](#) 있어야 합니다.

관련 정보

- [Network Address Translation 설정](#)
- [NAT 작동 확인 및 기본 NAT 문제 해결](#)
- [NAT: 로컬 및 글로벌 정의](#)
- [멀티캐스트 NAT는 Cisco 라우터에서 어떻게 작동합니까?](#)
- [NAT 지원 페이지](#)
- [Cisco 기술 지원 및 다운로드](#)

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.