동적 NAT를 사용할 때 라우팅 루프 방지

목차

소개

이 문서에서는 NAT 풀에서 사용되지 않는 ip 주소로 향하는 트래픽으로 인해 동적 NAT(Network Address Translation)를 사용할 때 NAT 라우터와 외부 인터페이스의 인접 라우터 간에 패킷이 루프되는 시나리오와 이러한 패킷을 다시 외부로 라우팅하는 NAT 라우터에 기본 경로가 존재하는 시나리오를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

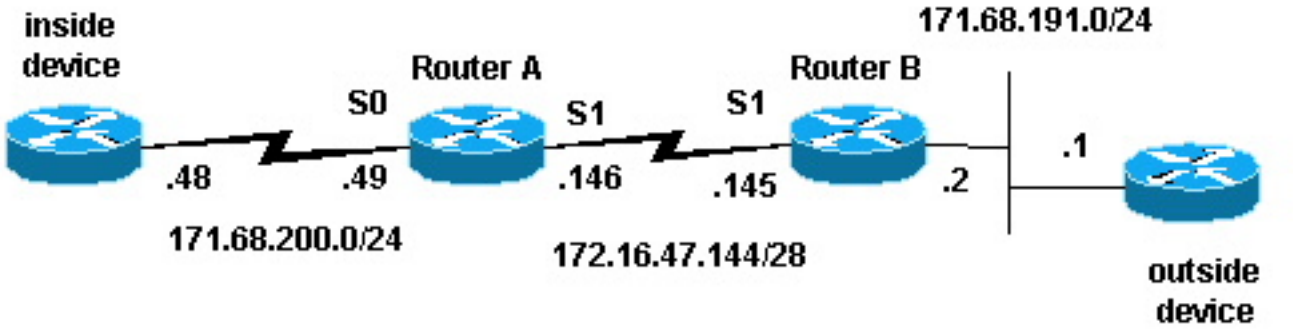
사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

네트워크 다이어그램

다음 토폴로지를 사용하여 예제 시나리오를 만들었습니다.



표기 규칙

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

예제 시나리오

위의 토폴로지에서 Router-A는 네트워크 171.68.200.0/24에서 제공된 패킷을 NAT 풀 "test-loop"에 의해 정의된 주소 범위로 변환하도록 NAT로 구성됩니다. Router-A의 컨피그레이션은 다음과 같습니다. 다른 모든 라우터는 연결을 얻기 위해 고정 경로로 구성됩니다.

```
hostname Router-A
!
!
ip nat pool test-loop 172.16.47.161 172.16.47.165 prefix-length 28
ip nat inside source list 7 pool test-loop
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 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
 no ip mroute-cache
 no ip route-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
```

```
!
end
```

NAT 변환 디버깅 및 IP 패킷 디버깅 명령을 사용하여 내부 디바이스의 라우터에서 ping을 생성했습니다. ping이 작동했고 변환 테이블 항목이 생성되었습니다. 아래 출력에서는 IP 패킷 디버깅 및 IP NAT 디버깅이 켜져 있으며 현재 변환 테이블에 항목이 없음을 확인할 수 있습니다.

참고: debug 명령은 상당한 양의 출력을 생성합니다. IP 네트워크의 트래픽이 낮기 때문에 시스템의 다른 활동이 부정적인 영향을 받지 않는 경우에만 사용하십시오.

```
Router-A# show debug
Generic IP:
  IP packet debugging is on (detailed)
  IP NAT debugging is on
Router-A# show ip nat translations
Router-A#
```

내부 라우터(내부 디바이스)는 소스 주소가 171.68.200.48이고 목적지 주소가 171.68.191.1(외부 디바이스의 주소)인 ICMP 패킷을 시작합니다. 다음 **디버그** 출력은 소스 IP 주소가 171.68.200.48인 IP 패킷이 172.16.47.161으로 변환되는 것을 보여줍니다. 패킷은 Serial0 인터페이스로 오며 Serial1 인터페이스로 이동됩니다.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [401]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

다음 **디버그** 출력은 목적지 IP 주소가 172.16.47.161인 반환 IP 패킷이 171.68.200.48으로 다시 변환되는 것을 보여줍니다. 패킷은 Serial1 인터페이스로 전송되며 serial0 인터페이스로 이동됩니다.

```
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [401]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

디버그 출력은 내부 디바이스와 외부 디바이스 간의 성공적인 ping 교환을 보여줍니다.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [402]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [402]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [403]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [403]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [404]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [404]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [405]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [405]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

show ip nat translations 명령을 사용하면 내부 디바이스의 변환 테이블에 항목이 표시됩니다.

```
Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
```

이제 내부 디바이스에 대한 변환이 변환 테이블에 있으므로 아래 라우터-A에서 생성된 디버그 출력에 표시된 대로 외부 디바이스에서 내부 디바이스의 전역 주소로 성공적으로 ping할 수 있습니다.

참고: 외부 디바이스에서 시작된 패킷은 소스 주소가 171.68.191.1이고 목적지 주소가 172.16.47.161(변환 테이블의 내부 전역 주소)입니다.

```
Router-A#
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [108]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [108]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [109]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [109]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [110]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [110]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [111]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [111]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [112]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [112]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
```

다음 디버그 출력은 외부 디바이스가 test-loop 풀에서 사용되지 않는 IP 주소인 대상 주소와의 통신을 시작하려고 시도할 때 발생할 수 있는 상황을 보여줍니다. clear **ip nat translation** 명령은 변환 테이블을 지우는 데 사용되었고 test-loop 풀 내의 사용되지 않는 IP 주소로 ping이 전송되었습니다.

외부 디바이스는 내부 전역 주소 172.16.47.161으로 향하는 ICMP 패킷을 전송합니다. 그러나 출력 인터페이스는 이 패킷의 입력 인터페이스와 동일합니다.

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

NAT는 패킷을 라우팅하기 전에 외부에서 내부에서 외부로 이동하는 패킷을 변환합니다. 이 경우 변환 테이블에 항목이 없으므로 Router-A는 패킷을 라우팅만 할 수 있습니다. Router-A는 기본 경로를 사용하여 패킷을 라우팅하고, 패킷을 Serial1 인터페이스로 다시 전송합니다. 이로 인해 루프가 결국 직렬 회선을 다운시킬 수 있습니다.

이러한 라우팅 루프를 방지하려면 외부 디바이스에서 내부 전역 주소로 패킷을 시작하지 마십시오. 그러나 이는 적용하기가 어렵기 때문에 라우터-A에서 다음 홉이 null0인 내부 전역 주소에 대한 고정 경로를 추가할 수 있습니다. 이렇게 하면 외부 디바이스가 내부 전역 주소로 향하는 패킷을 전송하고 변환 테이블에 항목이 없으면 Router-A는 패킷을 null0으로 라우팅하여 루프를 방지합니다. 위의 예를 사용하여 고정 경로는 다음과 같습니다.

```
ip route 172.16.47.160 255.255.255.252 null0.
```

관련 정보

- NAT 지원 페이지
- IP 라우팅 프로토콜 지원 페이지
- IP 라우팅 지원 페이지
- Technical Support - Cisco Systems