

중복 네트워크에서 NAT 사용

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 중복 네트워크에 NAT(Network Address Translation)를 사용하는 방법을 보여 줍니다. 네트워크가 중복되면 이미 법적으로 소유되어 인터넷이나 외부 네트워크의 다른 디바이스에 할당된 네트워크의 디바이스에 IP 주소를 할당할 수 있습니다. 네트워크가 중복되면 두 회사 모두 네트워크에서 [RFC 1918](#) IP 주소를 사용하는 두 회사가 병합됩니다. 이 두 네트워크는 모든 디바이스를 재조정할 필요 없이 통신을 수행해야 합니다.

사전 요구 사항

요구 사항

IP 주소 지정, IP 라우팅 및 DNS(Domain Name System)에 대한 기본적인 이해가 이 문서의 내용을 이해하는 데 도움이 됩니다.

사용되는 구성 요소

NAT 지원은 Cisco IOS[®] 소프트웨어 버전 11.2에서 시작되었습니다. 플랫폼 지원에 대한 자세한 내용은 [NAT FAQ를 참조하십시오](#).

표기 규칙

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

구성

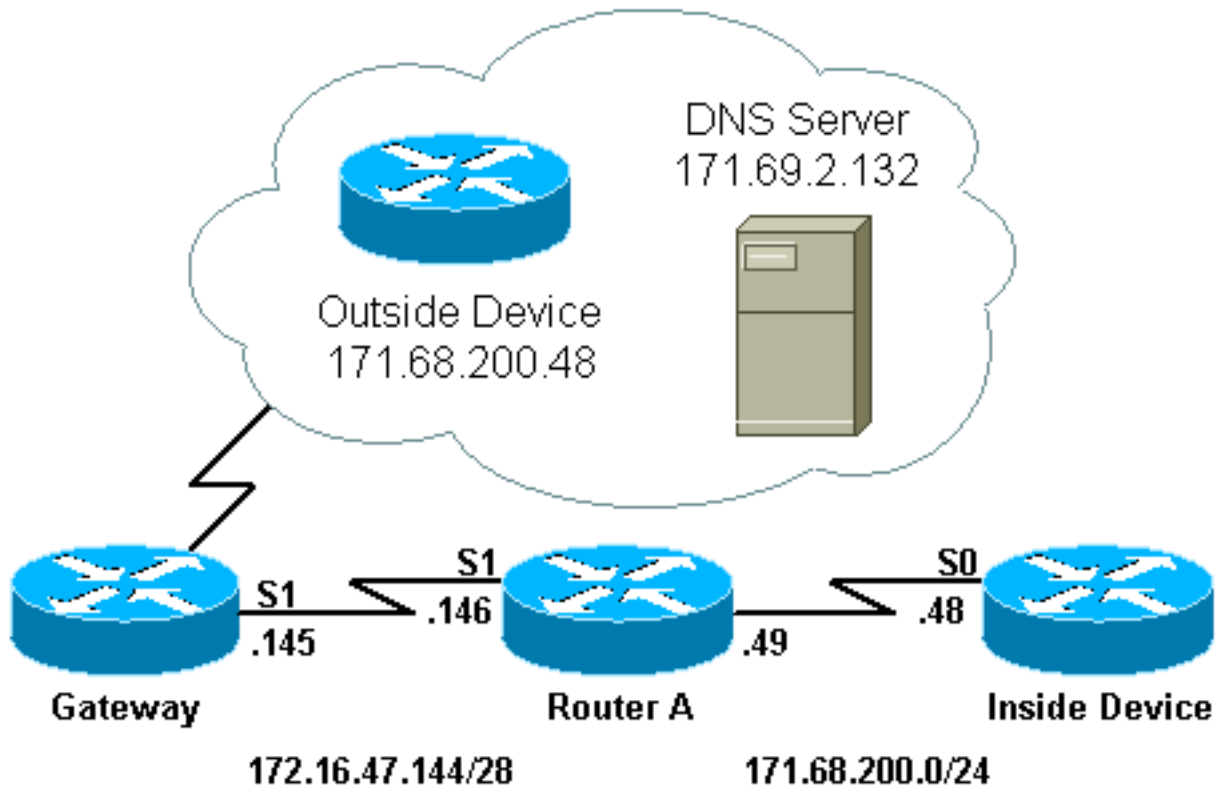
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.

내부 디바이스는 통신할 외부 디바이스와 동일한 IP 주소를 가지고 있습니다.



구성

라우터 A는 NAT에 대해 구성되어 있으므로 내부 디바이스를 풀 "test-loop"에서 주소로, 외부 디바이스는 풀 "test-dns"에서 주소로 변환합니다. 이 컨피그레이션이 겹치는 데 도움이 되는 방법에 대한 설명은 아래 컨피그레이션 표를 참조하십시오.

라우터 A
<pre>! version 11.2 no service udp-small-servers no service tcp-small-servers ! hostname Router-A ! ! ip domain-name cisco.com ip name-server 171.69.2.132 ! interface Loopback0 ip address 1.1.1.1 255.0.0.0</pre>

```

!
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 nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
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

```

내부 디바이스가 외부 디바이스와 통신할 때 위 컨피그레이션이 겹치는 데 도움이 되도록 하려면 외부 디바이스의 도메인 이름을 사용해야 합니다.

내부 디바이스는 자신에게 할당된 주소(내부 디바이스)와 동일하기 때문에 외부 디바이스의 IP 주소를 사용할 수 없습니다. 따라서 내부 디바이스는 외부 디바이스의 도메인 이름에 대한 DNS 쿼리를 보냅니다. 내부 디바이스의 IP 주소는 이 쿼리의 소스가 되며, **ip nat inside source list** 명령이 구성되어 있기 때문에 해당 주소는 "test-loop" 풀의 주소로 변환됩니다.

DNS 서버는 패킷의 페이로드에서 외부 디바이스의 도메인 이름과 연결된 IP 주소를 사용하여 풀 "test-loop"에서 가져온 주소에 응답합니다. 응답 패킷의 목적지 주소는 내부 디바이스의 주소로 다시 변환되고, 응답 패킷의 페이로드의 주소는 "test-dns" 풀의 주소로 변환됩니다. 이는 **ip nat outside source list** 명령으로 인해입니다. 따라서 내부 디바이스는 외부 디바이스의 IP 주소가 "test-dns" 풀의 주소 중 하나임을 알게 되며 외부 디바이스와 통신할 때 이 주소를 사용합니다. NAT를 실행하는 라우터가 이 시점에서 변환을 처리합니다.

이 프로세스는 Troubleshoot(문제 해결) 섹션에서 자세히 볼 수 [있습니다](#). 중복 주소를 사용하는 디바이스는 DNS를 사용하지 않고도 서로 통신할 수 있지만, 이 경우 고정 NAT를 구성해야 합니다. 이러한 작업을 수행하는 방법의 예는 다음과 같습니다.

라우터 A

```

!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!

ip domain-name cisco.com
ip name-server 171.69.2.132
!
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 nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop
ip nat outside source static 171.68.200.48 172.16.47.177
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
ip route 172.16.47.160 255.255.255.240 Serial0
!--- This line is necessary to make NAT work for return
traffic. !--- The router needs to have a route for the
pool to the inside !--- NAT interface so it knows that a
translation is needed. 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

```

위의 컨피그레이션을 사용하면 내부 디바이스가 외부 디바이스와 통신하려는 경우 이제 IP 주소 172.16.47.177을 사용할 수 있으며 DNS는 필요하지 않습니다. 위에 표시된 것처럼 내부 디바이스 주소의 변환은 여전히 동적으로 수행되므로, 라우터가 변환을 생성하기 전에 내부 디바이스에서 패킷을 가져와야 합니다. 따라서 내부 디바이스와 외부 디바이스가 통신하려면 내부 디바이스가 모든 연결을 시작해야 합니다. 외부 디바이스가 내부 디바이스에 대한 연결을 시작해야 하는 경우 내부 디바이스의 주소도 정적으로 구성해야 합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

위에서 설명한 대로 내부 디바이스가 외부 디바이스와 통신하는 데 DNS를 사용한 프로세스는 다음 트러블슈팅 프로세스를 통해 자세히 볼 수 있습니다.

현재 변환 테이블에 **show ip nat translations** 명령과 함께 볼 수 있는 변환이 없습니다. 아래 예에는 **debug ip packet** 및 **debug ip nat** 명령을 대신 사용합니다.

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

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

내부 디바이스가 NAT 도메인 외부에 있는 DNS 서버로 DNS 쿼리를 전송하면 DNS 쿼리의 소스 주소(내부 디바이스의 주소)가 **ip nat inside** 명령으로 변환됩니다. 아래 디버그 출력에서 확인할 수 있습니다.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
  UDP src=6988, dst=53
```

DNS 서버가 DNS 응답을 전송하면 **ip nat outside** 명령으로 인해 DNS 회신의 페이로드가 변환됩니다.

참고: NAT는 응답 패킷의 IP 헤더에서 변환이 발생하지 않는 한 DNS 회신의 페이로드를 조사하지 않습니다. 위의 라우터 컨피그레이션에서 **ip nat outside source list 7 pool** 명령을 참조하십시오.

아래 디버그 출력의 첫 번째 NAT 메시지는 라우터가 DNS 회신을 인식하고 페이로드 내의 IP 주소를 172.16.47.177으로 변환하는 것을 보여줍니다. 두 번째 NAT 메시지는 라우터가 DNS 회신의 대상을 변환하여 초기 DNS 쿼리를 수행한 내부 장치로 회신을 다시 전달할 수 있도록 합니다. 헤더의 목적지 부분인 내부 전역 주소는 내부 로컬 주소로 변환됩니다.

DNS 회신의 페이로드가 변환됩니다.

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
DNS 회신 패킷에 있는 IP 헤더의 목적지 부분은 변환됩니다.
```

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
  UDP src=53, dst=6988
```

다른 DNS 쿼리 및 응답을 살펴보겠습니다.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```

이제 DNS의 페이로드가 변환되었으므로 변환 테이블에는 외부 디바이스의 외부 로컬 및 전역 주소에 대한 항목이 있습니다. 표에 있는 이러한 항목을 사용하여 이제 내부 디바이스와 외부 디바이스 간에 교환되는 ICMP 패킷의 헤더를 완전히 변환할 수 있습니다. 아래 디버그 출력에서 이 교환을 살펴보겠습니다.

다음 출력은 변환되는 소스 주소(내부 디바이스 주소)를 보여줍니다.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
여기서 대상 주소(외부 장치의 외부 로컬 주소)가 변환됩니다.
```

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
변환 후 IP 패킷은 다음과 같습니다.
```

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

다음 출력은 반환 패킷에서 변환되는 소스 주소(외부 디바이스의 주소)를 보여줍니다.

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
이제 반환 패킷의 목적지 주소(내부 디바이스의 전역 주소)가 변환됩니다.
```

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
변환 후 반환 패킷은 다음과 같습니다.
```

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

내부 디바이스와 외부 디바이스 간에 패킷 교환이 계속됩니다.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]
IP: s=172.16.47.177 (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=172.16.47.177 [408]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]
```

```

NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]
IP: s=172.16.47.177 (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=172.16.47.177 [409]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]
IP: s=172.16.47.177 (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=172.16.47.177 [410]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0

```

외부 및 내부 간 패킷 교환이 완료되면 세 개의 항목이 있는 변환 테이블을 볼 수 있습니다. 내부 디바이스에서 DNS 쿼리를 전송했을 때 첫 번째 항목이 생성되었습니다. 두 번째 항목은 DNS 회신의 페이로드가 변환될 때 생성되었습니다. 세 번째 항목은 내부 디바이스와 외부 디바이스 간에 ping이 교환되었을 때 생성되었습니다. 세 번째 항목은 처음 두 항목의 요약이며 보다 효율적인 번역에 사용됩니다.

```
Router-A# show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.47.161	171.68.200.48	---	---
---	---	---	172.16.47.177	171.68.200.48
---	172.16.47.161	171.68.200.48	172.16.47.177	171.68.200.48

단일 Cisco 라우터에서 동적 NAT를 실행하여 겹치는 두 네트워크 간에 연결을 설정하려는 경우 DNS를 사용하여 외부 로컬 대 외부 글로벌 변환을 생성해야 합니다. DNS를 사용하지 않을 경우 고정 NAT를 사용하여 연결을 설정할 수 있지만 관리하기가 더 어렵습니다.

[관련 정보](#)

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