

Como Evitar Loops de Roteamento ao Usar NAT Dinâmico

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Conventions](#)

[Cenário de exemplo](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve um cenário em que os pacotes entram em loop entre o roteador NAT e o roteador vizinho na interface externa ao usar a NAT (Network Address Translation) dinâmica devido ao tráfego destinado a um endereço ip não utilizado em um pool NAT e à presença de uma rota padrão no roteador NAT que roteia esses pacotes de volta para o exterior.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

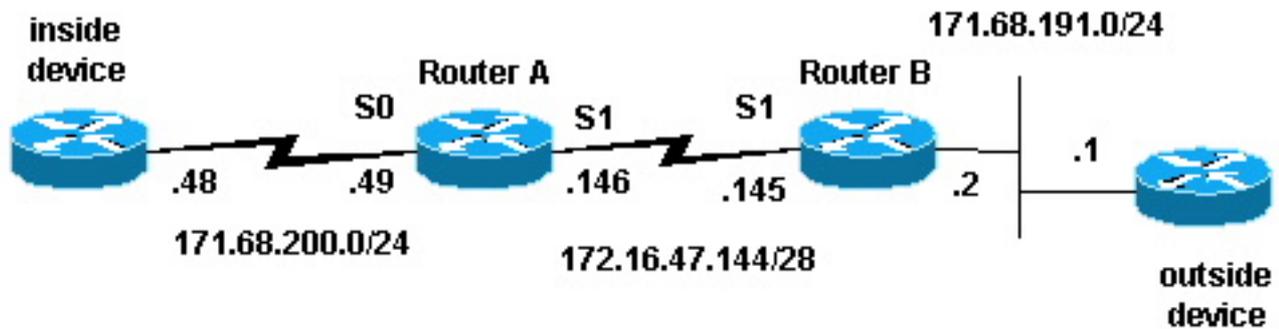
[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

[Diagrama de Rede](#)

A topologia a seguir foi usada para criar o cenário de exemplo.



Conventions

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Cenário de exemplo

Na topologia acima, o Roteador-A é configurado com NAT de modo que converta pacotes originados da rede 171.68.200.0/24 para um intervalo de endereços definidos pelo pool de NAT "test-loop". A configuração do Roteador-A é a seguinte (todos os outros roteadores são configurados com rotas estáticas para obter conectividade):

```
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
```

Ao usar a depuração da conversão NAT e os comandos de depuração do pacote de IP, foi gerado um ping do roteador no dispositivo interno. O ping funcionou e uma entrada da tabela de tradução foi gerada. Na saída abaixo, vemos que a depuração do pacote de IP e a do NAT de IP estão ativas e que não há entradas na tabela de conversão nesse momento.

Observação: os comandos **debug** geram uma quantidade significativa de saída. Use-os apenas quando o tráfego na rede IP estiver baixo, de modo que outra atividade no sistema não seja afetada de forma desfavorável.

```
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#
```

O roteador interno (dispositivo interno) origina um pacote ICMP com um endereço de origem de 171.68.200.48 e um endereço de destino de 171.68.191.1 (o endereço do dispositivo externo). A seguinte saída **debug** mostra um pacote IP com um endereço IP de origem 171.68.200.48 sendo convertido para 172.16.47.161. O pacote chega na interface Serial0 e segue para a interface Serial1.

```
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
```

A saída de depuração a seguir mostra o pacote IP de retorno com um endereço IP de destino de 172.16.47.161 sendo traduzido outra vez para 171.68.200.48. O pacote entra na interface Serial1 e é destinado à interface serial0.

```
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
```

A saída debug exibe a troca de ping bem-sucedida entre o dispositivo interno e o dispositivo externo.

```
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
```

Usando o comando `show ip nat translations`, podemos ver uma entrada na tabela de conversão para o dispositivo interno.

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

Agora que existe uma tradução para o dispositivo interno na tabela de tradução, é possível fazer o ping do dispositivo externo para o endereço global do dispositivo interno, conforme demonstrado na saída de debug gerada pelo Roteador A abaixo.

Observação: o pacote originado pelo dispositivo externo tem um endereço de origem 171.68.191.1 e um endereço de destino 172.16.47.161 (o endereço global interno na tabela de tradução).

```
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
```

A seguinte saída de depuração demonstra o que pode acontecer quando um dispositivo externo tenta iniciar a comunicação com um endereço de destino que é um endereço IP não utilizado no pool de loop de teste. O comando `clear ip nat translation` foi usado para limpar a tabela de tradução e um ping foi enviado para um endereço IP não utilizado dentro do pool de loop de teste.

O dispositivo externo envia um pacote ICMP com destino ao endereço global 172.16.47.161. No entanto, a interface de saída é a mesma da interface de entrada para esse pacote.

```
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
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
```

O NAT converte pacotes que vão de fora para dentro antes de roteá-los. Nesse caso, não há entrada na tabela de conversão, portanto o Roteador-A pode rotear o pacote apenas. O Roteador-A depende de sua rota padrão para rotear os pacotes, enviando os pacotes de volta para fora da interface Serial1, o que causa um loop que pode eventualmente derrubar a linha serial.

Para evitar esse tipo de circuito de roteamento, nunca origine pacotes de dispositivos externos aos endereços globais internos. Contudo, como isto é difícil de impor, você pode adicionar uma rota estática para os endereços globais internos com um Next Hop null0 no Router-A. Dessa forma, quando um dispositivo externo envia pacotes destinados a um endereço global interno e não há entrada na tabela de conversão, o Router-A encaminha o pacote para null0, evitando o loop. Usando o exemplo acima, a rota estática tem a seguinte aparência:

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

[Informações Relacionadas](#)

- [Página de suporte de NAT](#)
- [Página de suporte aos protocolos de roteamento IP](#)
- [Página de Suporte do IP Routing](#)
- [Suporte Técnico - Cisco Systems](#)