

Ordem de Operação NAT

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Visão geral de NAT](#)

[Configuração e saída de NAT](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento ilustra que a ordem em que as transações são processadas usando o Network Address Translation (NAT) está baseada sobre se um pacote vai da rede interna à rede externa, ou da rede externa à rede interna.

[Pré-requisitos](#)

[Requisitos](#)

Os leitores deste documento devem ter o conhecimento deste assunto:

- Network Address Translation (NAT). Para obter mais informações sobre do NAT, veja [como o NAT trabalha](#).

[Componentes Utilizados](#)

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

Note: A informação neste documento é baseada na versão de software, Software Release 12.2(27) de Cisco IOS®

[Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

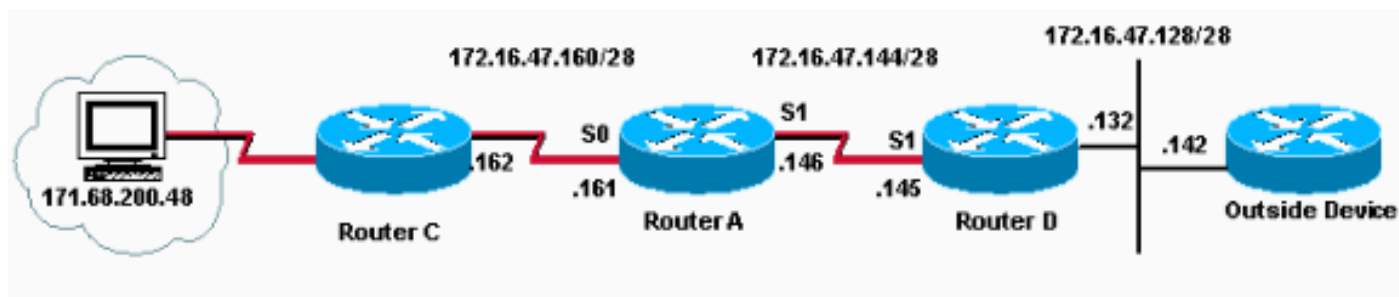
[Visão geral de NAT](#)

Nesta tabela, quando o NAT executa o global ao local, ou em local a global, a tradução é diferente em cada fluxo.

Dentro-à-parte externa	De fora para dentro
<ul style="list-style-type: none"> • Se for IPSec, verifique a lista de acesso de entrada •criptografia - para a tecnologia de criptografia Cisco (CET) ou o IPsec • check input access list • verificar limites de taxa de entrada • input accounting • redirecionar para o cache da Web • roteamento de política • roteamento • NAT para dentro à parte externa (local à tradução global) • crypto (verifique o mapa e a marca para criptografia) • verificar lista de acesso de saída • inspecione (Context-Based Access Control (CBAC)) • Interceptação de TCP • criptografia • Enfileiramento 	<ul style="list-style-type: none"> • Se for IPSec, verifique a lista de acesso de entrada •criptografia - para o CET ou o IPsec • check input access list • verificar limites de taxa de entrada • input accounting • redirecionar para o cache da Web • NAT fora ao interior (global à tradução local) • roteamento de política • roteamento • crypto (verifique o mapa e a marca para criptografia) • verificar lista de acesso de saída • inspecione o CBAC • Interceptação de TCP • criptografia • Enfileiramento

Configuração e saída de NAT

Este exemplo demonstra como o ordem de operação pode efetuar o NAT. Nesse caso, apenas a NAT e o roteamento são mostrados.



No exemplo anterior, o Roteador-A é configurado para traduzir o endereço local interno 171.68.200.48 a 172.16.47.150, segundo as indicações desta configuração.

```
!  
version 11.2  
no service udp-small-servers  
no service tcp-small-servers  
!  
hostname Router-A  
!  
enable password ww  
!  
ip nat inside source static 171.68.200.48 172.16.47.150  
!--- This command creates a static NAT translation !--- between 171.68.200.48 and 172.16.47.150  
ip domain-name cisco.com ip name-server 171.69.2.132 ! 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 171.68.200.0 255.255.255.0  
172.16.47.162 ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

A tabela de tradução indica que a tradução pretendida existe.

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

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.47.150	171.68.200.48	---	---

Esta saída é tomada do Roteador-A com [debuga o detalhe de pacote IP](#) e [debuga](#) permitida [nat IP](#), e um sibilo emitido do dispositivo 171.68.200.48 destinada para 172.16.47.142.

Note: Os comandos Debug gerenciam 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. Antes que você emita **comandos debug**, consulte a [informação toImportant em comandos Debug](#).

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

Pro	Inside global	Inside local	Outside local	Outside global
---	172.16.47.150	171.68.200.48	---	---

Desde que não há nenhum NAT debuga mensagens na saída precedente, você sabe que a tradução estática existente não está usada e que o roteador não tem uma rota para o endereço de destino (172.16.47.142) em sua tabela de roteamento. [O resultado de um pacote não roteável é uma mensagem que não chega a seu destino do ICMP, a qual é enviada para o dispositivo interno.](#)

Mas, Roteador-A tem uma rota padrão de 172.16.47.145, assim que porque a rota é considerada não-roteável?

O Roteador-A não tem **nenhum** configurado **sem classe IP**, que significa se um pacote destinado para um endereço de rede “principal” (neste caso, 172.16.0.0) para que as sub-redes existem na tabela de roteamento, o roteador não confia na rota padrão. Ou seja se você emite o **comando no ip classless**, isto desliga a capacidade do roteador para procurar a rota com o fósforo o mais longo do bit. A fim mudar este comportamento, você tem que configurar o [IP sem classe no Roteador-A](#). [O comando ip classless](#) é permitido à revelia em roteadores Cisco com Cisco IOS Software Release 11.3 e Mais Recente.

```
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      171.68.200.48    ---                ---
```

Quando você repete o mesmo teste de ping que feito previamente, você vê que o pacote obtém traduzido e o sibilo é bem sucedido.

Ping Response on device 171.68.200.48

```
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 171.68.200.48 are getting translated by NAT.

```
Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=171.68.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=171.68.200.48->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->171.68.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (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=171.68.200.48->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->171.68.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (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=171.68.200.48->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->171.68.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (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=171.68.200.48->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->171.68.200.48 [163]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (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=171.68.200.48->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->171.68.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
```

Router-A#**undebug all**

All possible debugging has been turned off

O exemplo anterior mostra que quando um pacote atravessa para dentro a fora, um roteador NAT verifica sua tabela de roteamento para ver se há uma rota ao endereço exterior antes que continue a traduzir o pacote. Portanto, é importante que o roteador NAT tenha uma rota válida para a rede externa. A rota à rede de destino deve ser sabida através de uma relação que seja definida como o [NAT fora na](#) configuração de roteador.

É importante notar que os pacotes de informação de retorno estão traduzidos antes que estejam distribuídos. [Por isso, o NAT Router também deve ter uma rota válida para o endereço interno local em sua tabela de roteamento.](#)

[Informações Relacionadas](#)

- [Configurando a tradução de endereço de rede: Introdução](#)
- [Verificando a Operação de NAT e Troubleshooting Básico de NAT](#)
- [NAT: Definições locais e globais](#)
- [Como o Multicast NAT trabalha em roteadores Cisco?](#)
- [Página de suporte de NAT](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)