

Verificar e solucionar problemas de operações básicas de NAT

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Problema](#)

[Pode fazer ping em um roteador, mas não em outro](#)

[Fora dos dispositivos da rede não é possível se comunicar com roteadores internos](#)

[Lista de verificação de problemas comuns](#)

Introduction

Este documento descreve como solucionar problemas de conectividade IP em um ambiente NAT.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Para obter mais informações sobre convenções de documentos, consulte [as Convenções de Dicas Técnicas da Cisco](#).

Problema

Este documento apresenta soluções para esses problemas:

- Pode fazer ping em um roteador, mas não em outro

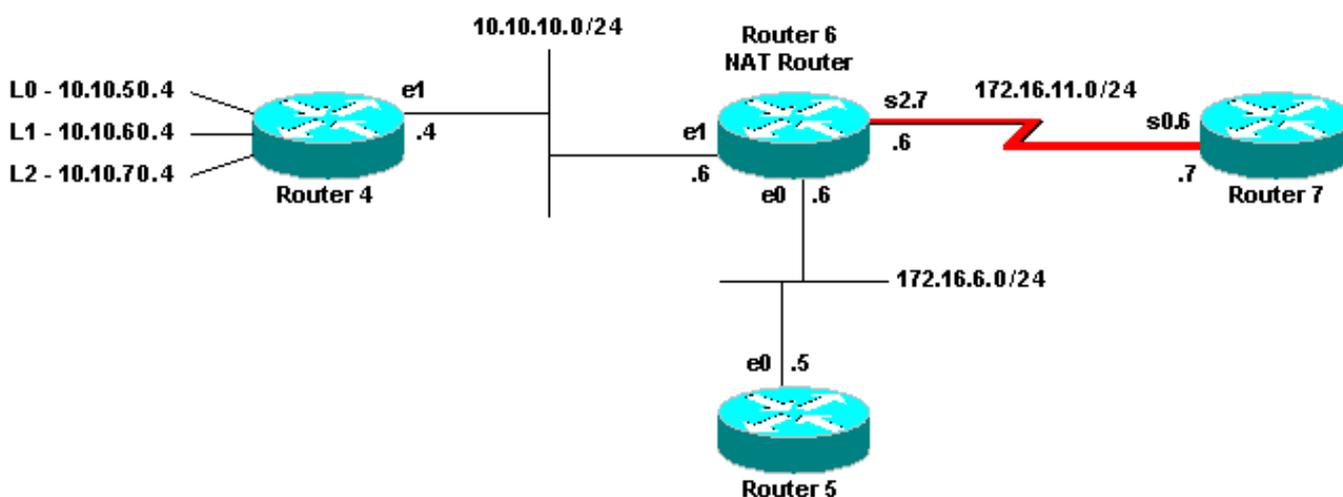
- Fora dos dispositivos da rede não é possível se comunicar com roteadores internos

Para determinar se o problema está nas operações de NAT:

1. Com base na configuração, defina claramente o que o NAT deve realizar. Você pode determinar que há um problema com a configuração. Para obter informações sobre a configuração do NAT, consulte [Configuração da conversão de endereço de rede: Introdução](#).
2. Verifique se as conversões corretas existem na tabela de conversão.
3. Use os comandos **show** e **debug** para verificar se a conversão ocorre.
4. Revise em detalhes o que acontece com o pacote e verifique se os roteadores têm as informações de roteamento corretas para levar o pacote adiante.

- **Pode fazer ping em um roteador, mas não em outro**

Neste diagrama de rede, o roteador 4 pode fazer ping no roteador 5 (172.16.6.5), mas não no roteador 7 (172.16.11.7):



O Roteador 4 não pode fazer ping no Roteador 7

Os protocolos de roteamento não executam os roteadores. O gateway padrão do roteador 4 é o roteador 6. O roteador 6 está configurado com NAT:

```
interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside !
interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside ! interface Serial2.7
point-to-point ip address 172.16.11.6 255.255.255.0 ip nat outside frame-relay interface-dlci
101 ! ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source list 7
pool test ip nat inside source static 10.10.10.4 172.16.6.14 ! access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4 access-list 7 permit 10.10.70.4
```

Para solucionar problemas:

1. Você precisa determinar que o NAT funciona corretamente. Você sabe, pela configuração, que o endereço IP do roteador 4 (10.10.10.4) é convertido estaticamente para 172.16.6.14. Você pode usar o comando **show ip nat translation** no roteador 6 para verificar se a conversão existe na tabela de conversão:

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global ---
172.16.6.14 10.10.10.4 --- ---
```

2. Certifique-se de que essa conversão ocorra quando o Roteador 4 originar tráfego IP. Você pode fazer isso de duas maneiras a partir do Roteador 6, executar o NAT **debug** ou monitorar as

estatísticas do NAT com o comando **show ip nat statistics**. Como os comandos **debug** são o último recurso, comece com o comando **show**.

3. Monitore o contador para garantir que ele aumente à medida que recebe tráfego do Roteador 4.
4. O contador é incrementado toda vez que a tabela de conversão é usada para converter um endereço.

4. Limpe as estatísticas, depois exiba as estatísticas, depois tente fazer ping no Roteador 7 a partir do Roteador 4 e, em seguida, exiba as estatísticas novamente.

```
router-6#clear ip nat statistics router-6# router-6# show ip nat statistics Total active translations: 1 (1 static, 0 dynamic; 0 extended) Outside interfaces: Ethernet0, Serial2.7 Inside interfaces: Ethernet1 Hits: 0 Misses: 0 Expired translations: 0 Dynamic mappings: -- Inside Source access-list 7 pool test refcount 0 pool test: netmask 255.255.255.0 start 172.16.11.70 end 172.16.11.71 type generic, total addresses 2, allocated 0 (0%), misses 0 router-6#
```

Depois de usar o comando **ping 172.16.11.7** no roteador 4, as estatísticas de NAT no roteador 6 são:

```
router-6#show ip nat statistics Total active translations: 1 (1 static, 0 dynamic; 0 extended) Outside interfaces: Ethernet0, Serial2.7 Inside interfaces: Ethernet1 Hits: 5 Misses: 0 Expired translations: 0 Dynamic mappings: -- Inside Source access-list 7 pool test refcount 0 pool test: netmask 255.255.255.0 start 172.16.11.70 end 172.16.11.71 type generic, total addresses 2, allocated 0 (0%), misses 0
```

Você pode ver, pelos comandos **show** que o número de pressionamentos aumentou em cinco. Em um **ping** bem-sucedido de um roteador Cisco, o número de acertos aumenta em dez. Os cinco ecos do Internet Control Message Protocol (ICMP) enviados pelo roteador de origem (Roteador 4) são convertidos e as cinco respostas de eco para pacotes do roteador de destino (Roteador 7) precisam ser convertidas, totalizando dez acertos. A perda de cinco acertos ocorre porque as respostas de eco não são convertidas ou não são enviadas do Roteador 7.

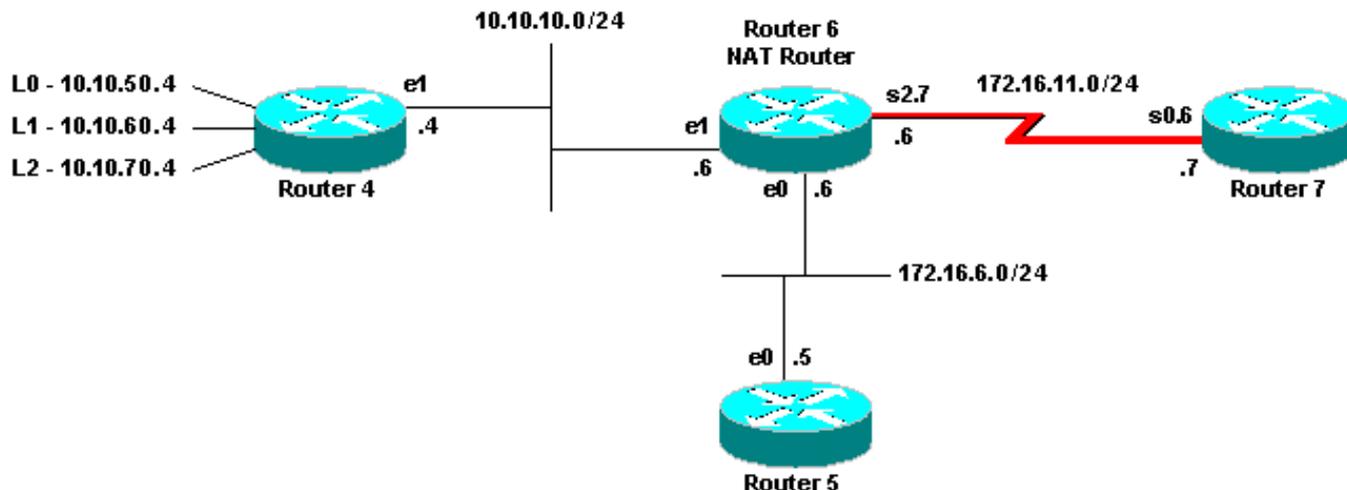
Veja se você pode encontrar alguma razão para o Roteador 7 não enviar pacotes de resposta de eco para o Roteador 4. Você revisa o que o NAT faz com o pacote. O Roteador 4 envia pacotes de eco ICMP com um endereço origem de 10.10.10.4 e um endereço destino de 172.16.11.7. Depois que o NAT ocorre, o pacote recebido pelo Roteador 7 tem um endereço origem de 172.16.6.14 e um endereço destino de 172.16.11.7. O Roteador 7 precisa responder a 172.16.6.14 e desde 172.16.16.14 não está diretamente conectado ao Roteador 7, ele precisa de uma rota para essa rede para responder. Verifique a tabela de roteamento do roteador 7 para verificar se a rota existe.

```
router-7#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.12.0 is directly connected, Serial0.8 C 172.16.9.0 is directly connected, Serial0.5 C 172.16.11.0 is directly connected, Serial0.6 C 172.16.5.0 is directly connected, Ethernet0
```

Você pode ver que a tabela de roteamento do Roteador 7 não tem uma rota para 172.16.6.14. Depois de adicionar essa rota, o ping funciona. É útil monitorar estatísticas de NAT com o comando **show ip nat statistics**. Em um ambiente NAT mais complexo com várias conversões, esse comando **show** não é mais útil. Você pode executar **deparações** no roteador.

- Fora dos dispositivos da rede não é possível se comunicar com roteadores internos

Nesse problema, o Roteador 4 pode fazer ping no Roteador 5 e no Roteador 7, mas os dispositivos na rede 10.10.50.0 não podem se comunicar com o Roteador 5 ou com o Roteador 7. O diagrama de rede é:



A rede não pode se comunicar com o roteador

```
interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside
media-type 10BaseT ! interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside
media-type 10BaseT ! interface Serial2.7 point-to-point ip address 172.16.11.6 255.255.255.0 ip
nat outside frame-relay interface-dlci 101 ! ip nat pool test 172.16.11.70 172.16.11.71 prefix-
length 24 ip nat inside source list 7 pool test ip nat inside source static 10.10.10.4
172.16.6.14 ! access-list 7 permit 10.10.50.4 access-list 7 permit 10.10.60.4 access-list 7
permit 10.10.70.4
```

Afirme o comportamento esperado do NAT. A partir da configuração do Roteador 6, você sabe que o NAT deve converter dinamicamente 10.10.50.4 para o primeiro endereço disponível no "teste" do pool de NAT. O pool consiste nos endereços 172.16.11.70 e 172.16.11.71. Com base nesse problema, você pode entender que os pacotes que os Roteadores 5 e 7 recebem têm um endereço origem 172.16.11.70 ou 172.16.11.71. Esses endereços estão na mesma sub-rede que o Roteador 7, portanto, o Roteador 7 deve ter uma rota diretamente conectada; no entanto, se ainda não tiver uma, o Roteador 5 precisará rotear para a sub-rede .

Você pode usar o comando `show ip route` para ver se a tabela de roteamento do roteador 5 lista 172.16.11.0:

```
router-5#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.9.0 is directly connected, Serial1 S
172.16.11.0 [1/0] via 172.16.6.6 C 172.16.6.0 is directly connected, Ethernet0 C 172.16.2.0 is
directly connected, Serial0
```

Você pode usar o comando `show ip route` para ver se a tabela de roteamento do roteador 7 lista 172.16.11.0 como uma sub-rede conectada diretamente:

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global ---
172.16.6.14 10.10.10.4 --- --- --- 172.16.11.70 10.10.50.4 --- ---
```

Verifique a tabela de conversão NAT e verifique se a conversão esperada existe. Como a conversão desejada é criada dinamicamente, você deve primeiro enviar o tráfego IP originado no endereço apropriado. Após um **ping** enviado, originado de 10.10.50.4 e destinado a 172.16.11.7, a tabela de conversão no Roteador 6 mostra:

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global ---
172.16.6.14 10.10.10.4 --- --- --- 172.16.11.70 10.10.50.4 --- ---
```

Como a conversão esperada está na tabela de conversão, você sabe que os pacotes de eco ICMP estão traduzidos adequadamente. Uma opção é que você pode monitorar as estatísticas de NAT, mas isso não é útil em um ambiente complexo. Outra opção é executar a depuração de NAT no roteador NAT (Roteador 6). Você pode executar **debug ip nat** no Roteador 6 enquanto envia um **ping** originado de 10.10.50.4 e destinado a 172.16.11.7. Os resultados de **debug** estão no próximo exemplo de código.

Note: Quando você usar qualquer comando debug em um roteador, pode sobrecarregá-lo, o que o tornará inoperante. Sempre tenha muito cuidado e, se possível, nunca execute uma **depuração** em um roteador de produção crítico sem a supervisão de um engenheiro do Suporte Técnico da Cisco.

:

```
router-6# show log Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console
logging: level debugging, 39 messages logged Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 39 messages logged Trap logging: level informational, 33
message lines logged Log Buffer (4096 bytes): 05:32:23: NAT: s=10.10.50.4->172.16.11.70,
d=172.16.11.7 [70] 05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70] 05:32:25:
NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71] 05:32:25: NAT*: s=172.16.11.7,
d=172.16.11.70->10.10.50.4 [71] 05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72]
05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72] 05:32:29: NAT*: s=10.10.50.4-
>172.16.11.70, d=172.16.11.7 [73] 05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73]
05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74] 05:32:31: NAT*: s=172.16.11.7,
d=172.16.11.70->10.10.50.4 [74]
```

Como você pode ver na saída de **depuração** anterior, a primeira linha mostra o endereço de origem de 10.10.50.4 convertido em 172.16.11.70. A segunda linha mostra o endereço de destino de 172.16.11.70 é convertido de volta em 10.10.50.4. Esse padrão se repete pelo resto da **depuração**. Isso significa que o Roteador 6 converte os pacotes em ambas as direções.

Revisão:

1. O Roteador 4 envia um pacote com origem em 10.10.50.4 destinado a 172.16.11.7.
2. O Roteador 6 executa o NAT no pacote e encaminha um pacote com uma origem 172.16.11.70 e um destino 172.16.11.7.
3. O Roteador 7 envia uma resposta com uma origem 172.16.11.7 e um destino 172.16.11.70.
4. O Roteador 6 executa o NAT no pacote, o que resulta em um pacote com endereço origem 172.16.11.7 e endereço destino 10.10.50.4.
5. O roteador 6 roteia o pacote para 10.10.50.4 com base nas informações da tabela de roteamento do roteador 6. Você precisa usar o mostrar rota do IP de para confirmar se o roteador 6 tem a rota necessária na sua tabela de roteamento.

```
router-6#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.8.0 is directly connected, Serial1 C
172.16.10.0 is directly connected, Serial2.8 C 172.16.11.0 is directly connected, Serial2.7 C
172.16.6.0 is directly connected, Ethernet0 C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets C 10.10.10.0 is directly connected, Ethernet1
```

Lista de verificação de problemas comuns

Use esta lista de verificação para solucionar problemas comuns:

• Tradução não instalada na tabela de tradução

Se você achar que a tradução apropriada não está instalada na tabela de tradução, verifique:

1. A configuração está correta. Às vezes, é difícil obter o NAT para obter o que você deseja. Para obter ajuda com a configuração, consulte Configuração de Network Address Translation: [Introdução](#).
2. Não há nenhuma lista de acesso de entrada que negue a entrada de pacotes do roteador NAT.
3. O roteador NAT tem a rota apropriada na tabela de roteamento se o pacote for enviado de dentro para fora. Consulte Pedido de Operação da NAT para obter mais informações.
4. A lista de acesso consultada pelo comando NAT permite todas as redes necessárias.
5. Existem endereços suficientes no pool NAT. Isso só será um problema se o NAT não estiver configurado para congestionamento.
6. As interfaces de roteadores são apropriadamente definidas como NAT interna ou NAT externa.
7. Para a conversão do payload dos pacotes do Domain Name System (DNS), certifique-se de que a conversão ocorra no endereço no cabeçalho IP do pacote. Se isso não acontecer, então o NAT não examinará o payload do pacote.

• A entrada de tradução correta não está sendo usada

Se a entrada de tradução correta estiver instalada na tabela de tradução, mas não for usada, verifique:

1. Verifique se não há nenhuma lista de acesso de entrada que negue a entrada dos pacotes do roteador NAT.
2. Para pacotes que vão de dentro para fora, verifique se há uma rota para o destino, pois isso é verificado antes da conversão. Consulte Pedido de Operação da NAT para obter mais informações.

• Operação correta da NAT, mas ainda há problemas de conectividade

Solucionar o problema de conectividade:

1. Verifique a conectividade da camada 2.
2. Verifique as informações de roteamento do Layer 3.
3. Procure filtros de pacotes que causam o problema.

- **Conversão de NAT para a porta 80 não funciona**

Isso significa que a conversão de NAT para a porta 80 não funciona, mas a conversão para outras portas funciona normalmente.

Para resolver esse problema:

1. Execute os comandos **debug ip nat translations** e **debug ip packet** para ver se as conversões estão corretas e se a entrada de conversão correta está instalada na tabela de conversão.
2. Verifique se o servidor responde.
3. Desative o servidor HTTP.
4. Desmarque as tabelas ARP e NAT.

- **%NAT: System busy. Try later**

A mensagem de erro try later aparece quando um comando **show** relacionado ao NAT ou um comando **show running-config** ou **write memory** é executado. Isso é causado pelo aumento no tamanho da tabela NAT. Quando o tamanho da tabela NAT aumenta, o roteador fica com memória insuficiente.

1. Recarregue o roteador para solucionar esse problema.
2. Se a mensagem de erro aparece quando HSRP SNAT é configurado, configure esses comandos para resolver o problema: Router(config)#standby mínimo de atraso 20 recarga 20 Router(config)#standby 2 preempt delay minimum 20 reload 20 sync 10

- **Tabela de conversão grande aumenta a CPU**

Um host pode enviar centenas de conversões, o que causa um alto uso da CPU. Em outras palavras, ele pode tornar a tabela tão grande que faz com que a CPU seja executada em 100%. O comando **ip nat translation max-entries 300** cria o limite de 300 por host ou um limite agregado da quantidade de conversões no roteador. A solução alternativa é usar o comando **ip nat translation max-entries all-hosts 300**.

- **% Public ip-address already mapped (Internal ip-address -> Public ip-address)**

Essa mensagem aparece quando você tenta configurar dois endereços IP internos em um endereço IP público que escuta nas mesmas portas.

```
% X.X.X.X already mapped (172.30.62.101 -> X.X.X.X)
```

Para corrigir isso, configure o endereço IP público para ter dois endereços IP internos e use dois endereços IP públicos no DNS.

- **Nenhuma entrada na tabela ARP**

Este é um resultado da **no-alias** nas entradas de NAT. O **no-alias** opção significa que o roteador não responde pelos endereços e não instala uma entrada ARP. Se outro roteador usar um pool NAT como um pool global interno que consista em endereços em uma sub-rede conectada, um alias será gerado para esse endereço, de modo que o roteador possa atender às solicitações do protocolo ARP (Address Resolution Protocol) para esses endereços. Isso faz com que o roteador tenha entradas ARP para os endereços falsos.

- **Token inválido 0, TOK_NUMBER|TOK_PUNCT desejado**

Essa mensagem de erro é apenas uma mensagem informativa e não afeta o comportamento normal do dispositivo.

Bad token 0, wanted TOK_NUMBER|TOK_PUNCT

O erro significa que o NAT tenta fazer uma correção de camada 4 no endereço em um FTP aberto e não consegue encontrar os endereços IP que ele precisa traduzir no pacote. O motivo pelo qual a mensagem inclui tokens é que os endereços IP no pacote são encontrados pela pesquisa de um token, ou um conjunto de símbolos, no pacote IP, para encontrar os detalhes necessários para a conversão.

Quando uma sessão FTP é iniciada, ela negocia dois canais, um canal de comando e um canal de dados. Esses são os dois endereços IP com números de porta diferente. O cliente e o servidor FTP negociam um segundo canal de dados para o qual transferir arquivos. O pacote trocado através do canal de controle tem o formato "PORT,i,i,i,i,p,p", onde i,i,i,i são os quatro bytes de um endereço IP e p,p especifica a porta. O NAT tenta corresponder esse padrão e converter endereço/porta, se necessário. O NAT deve converter ambos os esquemas de canal. A NAT verifica os números no fluxo de comando até achar que encontrou um comando de porta que requer conversão. Em seguida, ele analisa a tradução, que calcula com o mesmo formato.

Se o pacote estiver corrompido ou o servidor FTP ou o cliente tiver comandos mal formados, o NAT não poderá calcular corretamente a conversão e gerará esse erro. Você pode definir o cliente FTP como "passivo" para que inicie ambos os canais.

Informações Relacionadas

- [Página de suporte de NAT](#)
- [Suporte Técnico - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.