

Solucionar problemas de tradução de endereço de rede com perguntas frequentes

Contents

[Introduction](#)

[NAT genérico](#)

[P. O que é NAT?](#)

[P. Como o NAT funciona?](#)

[P. Como configuro o NAT?](#)

[P. Quais são as principais diferenças entre as implementações de NAT do Cisco IOS®Software e do Cisco Adaptive Security Appliance \(ASA\)?](#)

[Q. Em que hardware de roteamento da Cisco o Cisco IOS NAT está disponível? Como o hardware pode ser encomendado?](#)

[P. O NAT ocorre antes ou após o roteamento?](#)

[P. O NAT pode ser implantado em um ambiente de LAN sem fio público?](#)

[P. O NAT faz o balanceamento de carga TCP para servidores na rede interna?](#)

[P. Posso limitar a taxa do número de conversões de NAT?](#)

[P. Como o roteamento é aprendido ou propagado para sub-redes IP ou endereços que são usados pelo NAT?](#)

[P. Quantas sessões de NAT simultâneas têm suporte no Cisco IOS NAT?](#)

[P. Que tipo de desempenho de roteamento pode ser esperado com o NAT do Cisco IOS?](#)

[P. O NAT do Cisco IOS pode ser aplicado a subinterfaces?](#)

[P. O NAT do Cisco IOS pode ser usado com o Hot Standby Router Protocol \(HSRP\) para fornecer links redundantes para um ISP?](#)

[P. O NAT do Cisco IOS suporta conversões de entrada em uma interface do Frame Relay? Ele suporta traduções externas no lado da Ethernet?](#)

[P. Um único roteador habilitado para NAT permite que alguns usuários usem NAT e outros usuários na mesma interface Ethernet para continuar a usar seus próprios endereços IP?](#)

[P. Quando o PAT \(sobrecarga\) é configurado, qual é o número máximo de conversões que podem ser criadas por endereço IP global interno?](#)

[P. Como funciona o PAT?](#)

[P. O que são pools de IP de NAT?](#)

[P. Qual é o número máximo de pools IP de NAT configuráveis \(ip nat pool "name"\)?](#)

[P. Qual é a vantagem do mapa de rota vs ACL em um pool NAT?](#)

[P. O que é "sobreposição" de endereço IP no contexto do NAT?](#)

[P. O que são conversões NAT estáticas?](#)

[P. O que significa o termo sobrecarga de NAT; esse é PAT?](#)

[P. O que são conversões NAT dinâmicas?](#)

[P. O que é ALG?](#)

[P. É possível criar uma configuração com conversões NAT estáticas e dinâmicas?](#)

[P. Quando um traceroute é feito através de um roteador NAT, o traceroute deve mostrar o endereço NAT-Global ou deve vaziar o endereço NAT-Local?](#)

[P. Como o PAT aloca a porta?](#)

[P. Qual é a diferença entre a fragmentação IP e a segmentação TCP?](#)

P. O NAT oferece suporte fora de serviço para fragmentação de IP e segmentação de TCP?

P. Como depurar a fragmentação IP e a segmentação TCP?

P. Há um MIB NAT compatível?

P. O que é o timeout de TCP e como ele se relaciona com o temporizador de NAT TCP?

P. Posso alterar a quantidade de tempo que leva para que uma conversão de NAT expire da tabela de conversão de NAT?

P. Como faço para interromper o Lightweight Directory Access Protocol (LDAP) quando ele anexa bytes extras a cada pacote de resposta LDAP?

P. Qual é a recomendação de rota para o endereço IP global interno/local externo na caixa NAT?

P. O NAT do Cisco IOS suporta ACLs com uma palavra-chave de registro?

NAT por voz

P. O NAT é compatível com o Skinny Client Control Protocol (SCCP) v17 fornecido com o Cisco Unified Communications Manager (CUCM) V7?

P. Quais versões de carregamento de CUCM /SCCP/firmware são suportadas pelo NAT?

P. O que é o Service Provider PAT Port Allocation Enhancement para RTP e RTCP?

P. O que é o Session Initiation Protocol (SIP) e os pacotes SIP podem ser roteados com NAT?

P. O que é o suporte Hosted NAT Traversal para Session Border Controller (SBC)?

P. Quantas chamadas SIP, Skinny e H323 a memória e a CPU de um roteador podem lidar com NAT?

P. Um roteador NAT suporta segmentação TCP de pacotes Skinny e H323?

P. Há alguma advertência a ser observada quando você usa uma configuração de sobrecarga de NAT em uma implantação de voz?

P. Há algum problema conhecido causado quando você usa o comando `clear ip nat trans *` ou o comando `clear ip nat trans forced` em uma implantação de voz?

P. O NAT é compatível com a solução co-localizada de voz?

P. O NVI é compatível com Skinny ALG, H323 ALG e TCP SIP ALG?

NAT com VRF/MPLS

P. Um roteador NAT pode alguma vez suportar a si mesmo no mesmo espaço de endereço em um VRF e em um espaço de endereço global? No momento, eu recebo este aviso: "% entrada estática semelhante (10.1.1.1 —> 10.2.2.2) já existe" quando tento configurar isto:

P. O NAT legado suporta VRF-Lite (a rota de um VRF para um VRF diferente)?

NAT NVI

P. O que é NAT NVI?

P. O NAT NVI deve ser usado para rotear entre uma interface em global e uma interface em um VRF?

P. A segmentação TCP para NAT-NVI é suportada?

P. O NVI é compatível com Skinny ALG, H323 ALG e TCP SIP ALG?

P. A segmentação TCP é compatível com SNAT?

SNAT

P. O que é o NAT stateful (SNAT)?

P. A segmentação TCP é suportada com SNAT?

P. O SNAT é compatível com roteamento assimétrico?

NAT-PT (v6 a v4)

P. O que é NAT-PT?

P. O NAT-PT é suportado no caminho do Cisco Express Forwarding (CEF)?

P. Quais ALGs são suportados no NAT-PT?

[P. O ASR 1004 é compatível com NAT-PT?](#)

[Cisco 7600/6k dependente de plataforma](#)

[P. O NAT stateful \(SNAT\) está disponível no Catalyst 6500 no trem SX?](#)

[P. O NAT com reconhecimento de VRF é compatível com hardware no 6k?](#)

[P. O 7600 e o Cat6000 suportam NAT sensível a VRF?](#)

[Cisco 850 dependente da plataforma](#)

[P. O Cisco 850 suporta Skinny NAT ALG na versão 12.4T?](#)

[Implantação de NAT](#)

[P. Como faço para implementar o NAT?](#)

[P. Como faço para implementar o NAT com voz?](#)

[P. Como posso integrar o NAT com VPNs MPLS?](#)

[P. O mapeamento estático de NAT oferece suporte a HSRP para alta disponibilidade?](#)

[P. Como faço para implementar NAT NVI?](#)

[P. Como faço para implementar o balanceamento de carga com o NAT?](#)

[P. Como faço para implementar o NAT em conjunto com o IPSec?](#)

[P. Como faço para implementar o NAT-PT?](#)

[P. Como implemento o NAT multicast?](#)

[P. Como faço para implementar o NAT stateful \(SNAT\)?](#)

[Melhores práticas de NAT](#)

[P. Há alguma prática recomendada de NAT?](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como o processo do roteador de Tradução de Endereço de Rede (NAT - Network Address Translation) funciona e fornece respostas para algumas das perguntas comuns.

NAT genérico

P. O que é NAT?

R. A Network Address Translation (NAT) foi projetada para a conservação de endereços IP. Ela permite que as redes IP privadas que usam endereços IP não registrados se conectem à Internet. O NAT opera em um roteador, geralmente quando você conecta duas redes juntas, e converte os endereços privados (não globalmente exclusivos) na rede interna em endereços legais, antes que os pacotes sejam encaminhados para outra rede.

Outro aspecto desse recurso é que a NAT pode ser configurada para anunciar para o resto do mundo apenas um endereço para toda a rede, Isso efetivamente oculta toda a rede interna atrás desse endereço, o que fornece segurança adicional. A NAT disponibiliza funções duplas de segurança e conservação de endereço e é implementada em ambientes de acesso remoto.

P. Como o NAT funciona?

R. Basicamente, o NAT permite que um único dispositivo, como um roteador, atue como um agente entre a Internet (ou rede pública) e uma rede local (ou rede privada), o que significa que

apenas um único endereço IP exclusivo é necessário para representar um grupo inteiro de computadores para qualquer coisa fora de sua rede.

P. Como configuro o NAT?

R. Para configurar o NAT tradicional, você precisa fazer pelo menos uma interface em um roteador (NAT externo) e outra interface no roteador (NAT interno) e um conjunto de regras de conversão para os endereços IP nos cabeçalhos dos pacotes (e payloads, se desejado) e eles precisam ser configurados. Para configurar a Nat Virtual Interface (NVI), você precisa de pelo menos uma interface configurada com NAT habilitada junto com o mesmo conjunto de regras, conforme mencionado acima.

Para obter mais informações, consulte [o Guia de Configuração dos Serviços de Endereçamento IP do Cisco IOS](#) ou sua seção [sobre Configuração da Interface Virtual NAT](#).

P. Quais são as principais diferenças entre o Cisco IOS[®] Software e as implementações do Cisco Adaptive Security Appliance (ASA) de NAT?

R. O NAT baseado no software Cisco IOS não é fundamentalmente diferente da função NAT no Cisco ASA. As principais diferenças incluem os diferentes tipos de tráfego suportados nas implementações e nos requisitos do projeto. Consulte [Configuração de NAT](#) Exemplos para obter mais informações sobre a configuração de NAT em dispositivos Cisco ASA (inclui os tipos de tráfego suportados).

Q. Em que hardware de roteamento da Cisco o Cisco IOS NAT está disponível? Como o hardware pode ser encomendado?

R. A ferramenta Cisco Feature Navigator permite que os clientes identifiquem um recurso (NAT) e descubram em qual versão e versão de hardware esse recurso do Cisco IOS Software está disponível. Consulte [Cisco Feature](#) Navigator para usar esta ferramenta.

P. O NAT ocorre antes ou após o roteamento?

R. A ordem em que as transações são processadas pelo NAT é baseada em se um pacote viaja da rede interna para a rede externa ou da rede externa para a rede interna. A conversão de dentro para fora ocorre depois do roteamento, e de fora para dentro; a conversão ocorre antes do roteamento. Consulte [Ordem de Operação do NAT](#) para obter mais informações.

P. O NAT pode ser implantado em um ambiente de LAN sem fio público?

R. Sim. O recurso NAT - Static IP Support fornece suporte para usuários com endereços IP estáticos e permite que esses usuários estabeleçam uma sessão IP em um ambiente de LAN sem fio público.

P. O NAT faz o balanceamento de carga TCP para servidores na rede interna?

R. Sim. Com o NAT, você pode estabelecer um host virtual na rede interna que coordena balanceamentos de carga entre hosts reais.

P. Posso limitar a taxa do número de conversões de NAT?

R.Sim. O recurso de Conversão de NAT com limite de taxa oferece a capacidade de limitar o número máximo de operações simultâneas de NAT em um roteador. Isso dá aos usuários mais controle sobre como os endereços NAT são usados, o recurso de conversão NAT com limite de taxa pode ser usado para limitar os efeitos de vírus, worms e ataques de negação de serviço.

P. Como o roteamento é aprendido ou propagado para sub-redes IP ou endereços que são usados pelo NAT?

R.O roteamento para endereços IP criados pelo NAT é aprendido se:

- O pool de endereços global interno for derivado da sub-rede de um roteador de próximo salto.
- A entrada de rota estática for configurada no roteador de próximo salto e redistribuída dentro da rede do roteamento.

Quando o endereço global interno é correspondido com a interface local, o NAT instala um alias IP e uma entrada ARP, caso em que o roteador **pode proxy-arp** para esses endereços. Se esse comportamento não for desejado, use a **palavra-chave non-alias**.

Quando um pool de NAT está configurado, a opção add-route pode ser usada para a injeção de rota automática.

P. Quantas sessões de NAT simultâneas têm suporte no Cisco IOS NAT?

R.O limite da sessão de NAT é limitado pela quantidade de DRAM disponível no roteador. Cada conversão NAT consome cerca de 312 bytes da DRAM. Como resultado, 10.000 conversões (mais do que seria geralmente feito em um único roteador) consomem cerca de 3 MB. Sendo assim, o hardware de roteamento típico tem mais memória do que o suficiente para comportar milhares de conversões NAT. Entretanto, também é recomendável verificar as especificações da plataforma.

P. Que tipo de desempenho de roteamento pode ser esperado com o NAT do Cisco IOS?

R.O NAT do Cisco IOS suporta switching CEF (Cisco Express Forwarding), switching rápida e switching de processo. O caminho de switching rápido não é mais compatível com versões 12.4T e superior. Para a plataforma Cat6k, a ordem de switching é Netflow (caminho de switching de HW), CEF e caminho do processo.

O desempenho depende de vários fatores:

- O tipo de aplicação e o tipo de tráfego
- Se os endereços IP estão incorporados
- Troca e inspeção de várias mensagens
- Porta de origem obrigatória
- O número de conversões
- Outros aplicativos que são executados no momento
- O tipo de hardware e processador

P. O NAT do Cisco IOS pode ser aplicado a subinterfaces?

R.Sim. As conversões de NAT de origem e/ou destino podem ser aplicadas a qualquer interface ou subinterface que tenha um endereço IP (inclui interfaces de discador). A NAT não pode ser configurada usando a Interface virtual sem fio. A interface virtual sem fio não existe no momento em que ela grava na NVRAM. Assim, após a reinicialização, o roteador perde a configuração NAT na Interface Virtual Sem Fio.

P. O NAT do Cisco IOS pode ser usado com o Hot Standby Router Protocol (HSRP) para fornecer links redundantes para um ISP?

R.Sim. A NAT oferece HSRP redundante. Entretanto, é diferente da SNAT (Stateful NAT). A NAT com HSRP é um sistema stateless. A sessão atual não é mantida quando ocorre uma falha. Durante a configuração de NAT estática (quando um pacote não coincide com nenhuma configuração de regra ESTÁTICA), o pacote é enviado sem nenhuma conversão.

P. O NAT do Cisco IOS suporta conversões de entrada em uma interface do Frame Relay? Ele suporta traduções externas no lado da Ethernet?

R.Sim. O encapsulamento não importa para a NAT. A NAT pode ser feita onde houver um endereço IP em uma interface, e a interface é NAT de dentro ou NAT de fora. Deve haver um interior e um exterior para a NAT funcionar. Se você usar o NVI, deve haver pelo menos uma interface NAT habilitada. Consulte a pergunta anterior, [How do I configure NAT?](#) para obter mais detalhes.

P. Um único roteador habilitado para NAT permite que alguns usuários usem NAT e outros usuários na mesma interface Ethernet para continuar a usar seus próprios endereços IP?

R.Sim. Isso pode ser feito com o uso de uma lista de acesso que descreve o conjunto de hosts ou redes que exigem NAT. Todas as sessões no mesmo host podem ser traduzidas ou podem passar pelo roteador e não podem ser traduzidas.

Listas de acesso, listas de acesso estendidas e mapas de rotas podem ser usados para definir regras pelas quais os dispositivos IP são convertidos. O endereço de rede e a máscara de sub-rede apropriada sempre devem ser especificados. A palavra-chave any não deve ser usada no lugar do endereço de rede ou da máscara de sub-rede. Com a configuração de NAT estático, quando o pacote não corresponde a nenhuma configuração de regra ESTÁTICA, o pacote pode ser enviado sem nenhuma conversão.

P. Quando o PAT (sobrecarga) é configurado, qual é o número máximo de conversões que podem ser criadas por endereço IP global interno?

A.PAT (sobrecarga) divide as portas disponíveis por endereço IP global em três intervalos: 0-511, 512-1023 e 1024-65535. A PAT atribui uma porta de fonte única para cada sessão de UDP ou TCP. Ele tenta atribuir o mesmo valor de porta da solicitação original, mas se a porta de origem original já tiver sido usada, ele começa a verificar desde o início do intervalo de portas específico para encontrar a primeira porta disponível e a atribui à conversação.

P. Como funciona o PAT?

A.PAT funciona com um endereço IP global ou vários endereços.

PAT com uma tabela de endereços IP

Condição	Descrição
1	A NAT/PAT inspeciona o tráfego e o correlaciona a uma regra de conversão.
2	A regra corresponde a uma configuração da PAT.
3	Se o PAT souber sobre o tipo de tráfego e se esse tipo de tráfego tiver "um conjunto de portas específicas que negocia" que possa usar, o PAT os deixará de lado e não os alocará com identificadores exclusivos.
4	Se uma sessão sem requisitos especiais de porta tenta conectar-se para fora, a PAT converte endereço IP de origem e verifica a disponibilidade da porta de origem (433, por exemplo). Consulte a Nota.
5	Se a porta de origem solicitada estiver disponível, a PAT atribui a porta de origem e a sessão continua.
6	Se a porta de origem solicitada não estiver disponível, o PAT começa a pesquisar desde o início do grupo relevante (começa em 1 para aplicações TCP ou UDP e em 0 para ICMP).
7	Se uma porta estiver disponível, ela é atribuída, e a sessão continua.
8	Se nenhuma porta estiver disponível, o pacote será derrubado.

Observação: para o protocolo TCP e o protocolo UDP, os intervalos são: 1-511, 512-1023, 1024-65535. Para o Internet Control Message Protocol (ICMP), o primeiro grupo começa em 0.

PAT com vários endereços IP

Condição	Descrição
1-7	Para as sete primeiras condições, ocorre o mesmo que com um único endereço IP.
8	Se não houver portas disponíveis no grupo relevante no primeiro endereço IP, a NAT passa para o próximo endereço IP no pool e tenta alocar a porta de origem solicitada.
9	Se a porta de origem solicitada estiver disponível, o NAT atribui a porta de origem e a sessão continua.
10	Se a porta de origem solicitada não estiver disponível, o NAT começa a pesquisar desde o início do grupo relevante (começa em 1 para aplicações TCP ou UDP e em 0 para ICMP).
11	Se uma porta estiver disponível, ela será atribuída e a sessão continuará.
12	Se não houver portas disponíveis, o pacote é descartado, a menos que outro endereço IP esteja disponível no pool.

P. O que são pools de IP de NAT?

R.Os pools de IP de NAT são um intervalo de endereços IP alocados para conversão de NAT conforme necessário. Para definir um pool, é usado o comando de configuração:

```
ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type {rotary}]
```

Exemplo 1

O próximo exemplo traduz entre hosts internos endereçados da rede 192.168.1.0 ou 192.168.2.0

para a rede 10.69.233.208/28 globalmente exclusiva:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Exemplo 2

No próximo exemplo, o objetivo é definir um endereço virtual, cujas conexões são distribuídas entre um conjunto de hosts reais. O pool define os endereços dos hosts reais. A lista de acesso define o endereço virtual. Se uma conversão já não existir, pacotes TCP de interface serial 0 (a interface externa) cujo destino corresponde à lista de acesso são convertidos para um endereço do pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

P. Qual é o número máximo de pools IP de NAT configuráveis (ip nat pool "name")?

R. Na prática, o número máximo de pools de IP configuráveis é limitado pela quantidade de DRAM disponível no roteador específico. (A Cisco recomenda que você configure um tamanho de pool de 255). Cada pool não deve ter mais de 16 bits. Na versão 12.4(11)T e posteriores, o Cisco IOS introduziu o CCE (Common Classification Engine). Com isso, a NAT foi limitada para ter somente um máximo de 255 pools.

P. Qual é a vantagem do mapa de rota vs ACL em um pool NAT?

R. Um mapa de rotas protege usuários externos indesejados para acessar os usuários/servidores internos. Ele também tem a capacidade de mapear um único endereço IP interno para diferentes endereços globais internos segundo a regra. Consulte [Suporte de NAT para Pools Múltiplos Usando Mapas de Rota](#) para obter mais informações.

P. O que é "sobreposição" de endereço IP no contexto do NAT?

R. A sobreposição de endereços IP refere-se a uma situação em que dois locais que desejam

interconectar usam o mesmo esquema de endereços IP. Esta não é uma ocorrência incomum; acontece frequentemente quando as empresas se fundem ou são adquiridas. Sem suporte especial, os dois locais não podem se conectar e estabelecer sessões. O endereço IP sobreposto pode ser um endereço público atribuído a outra empresa, um endereço privado atribuído a outra empresa ou pode vir do intervalo de endereços privados conforme definido [no RFC 1918](#).

Os endereços IP privados não são roteáveis e exigem conversões NAT para permitir conexões com o mundo externo. A solução envolve a interceptação de respostas de consulta de nomes do Sistema de Nomes de Domínio (DNS) de fora para dentro, uma configuração de conversão para o endereço externo e a resposta DNS precisa ser corrigida antes de ser encaminhada para o host interno. É necessário que um servidor DNS esteja envolvido em ambos os lados do dispositivo NAT para resolver os usuários que desejam ter conexão entre as duas redes.

O NAT é capaz de inspecionar e executar a conversão de endereço no conteúdo dos registros DNS e PTR, como mostrado [em Uso do NAT em redes sobrepostas](#).

P. O que são conversões NAT estáticas?

R. As conversões NAT estáticas têm mapeamento um para um entre endereços locais e globais. Os usuários também podem configurar conversões de endereço estático para o nível de porta e usar o restante do endereço IP para outras conversões. Isso geralmente ocorre onde você executa a Conversão de endereço de porta (PAT).

O próximo exemplo mostra como configurar o mapa de rota para permitir a conversão de fora para dentro para NAT estático:

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

P. O que significa o termo *NAT Overloading*; esse PAT?

R. Sim. A sobrecarga de NAT é PAT, que envolve o uso de um pool com um intervalo de um ou mais endereços ou o uso de um endereço IP de interface em combinação com a porta. Quando sobrecarregar, você cria uma conversão totalmente estendida. Esta é uma entrada da tabela de tradução que contém informações de endereço IP e porta origem/destino, que geralmente é chamada de PAT ou sobrecarga.

O PAT (ou sobrecarga) é um recurso do NAT do Cisco IOS que é usado para *converter endereços privados internos* (locais internos) para um ou *mais endereços IP externos* (globais internos, normalmente registrados). Os números exclusivos de porta de origem em cada tradução são usados para diferenciar entre as conversações.

P. O que são conversões NAT dinâmicas?

A. Em conversões NAT dinâmicas, os usuários podem estabelecer mapeamento dinâmico entre os endereços locais e globais. O mapeamento dinâmico é realizado quando você define os endereços locais a serem convertidos e o pool de endereços ou o endereço IP da interface a

partir do qual alocar endereços globais e quando você associa os dois.

P. O que é ALG?

A.ALG é um Application Layer Gateway (ALG). A NAT faz serviços de conversão em qualquer tráfego de Transmission Control Protocol/User Datagram Protocol (TCP/UDP) que não tenha endereços IP de origem e/ou destino no fluxo de dados de aplicação.

Esses protocolos incluem FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, telnet,archie, finger, NTP, NFS, rlogin, rsh, rcp. Protocolos específicos que incorporam informações de endereço IP à carga exigem a ajuda de um ALG.

Consulte [Uso de Gateways de Nível de Aplicativo com NAT](#) para obter mais informações.

P. É possível criar uma configuração com conversões NAT estáticas e dinâmicas?

R.Sim. No entanto, o mesmo endereço IP não pode ser usado para a configuração estática da NAT ou no pool para configuração dinâmica da NAT. Todos os endereços IP públicos precisam ser exclusivos. Observe que os endereços globais usados em conversões estáticas não são automaticamente excluídos com pools dinâmicos que contêm esses mesmos endereços globais. Pools dinâmicos devem ser criados para excluir endereços atribuídos por entradas estáticas. Para obter mais informações, consulte [Configuração de NAT estático e dinâmico simultaneamente](#).

P. Quando um traceroute é feito através de um roteador NAT, o traceroute deve mostrar o endereço NAT-Global ou deve vazar o endereço NAT-Local?

R.Traceroute de fora deve sempre retornar o endereço global.

P. Como o PAT aloca a porta?

R.O NAT introduz recursos de porta adicionais: alcance completo e mapa de porta.

- A faixa completa permite que a NAT use todas as portas, independentemente da faixa de portas padrão.
- O mapa de portas permite que a NAT reserve uma faixa de portas definida pelo usuário para aplicações específicas.

Consulte [Intervalos de portas de origem definidos pelo usuário para PAT](#) para obter mais informações.

Da versão 12.4(20)T2 em diante, a NAT apresenta a randomização de porta para L3/L4 e porta simétrica.

- A randomização de porta permite que a NAT selecione aleatoriamente qualquer porta global para a solicitação de porta de origem.
- A porta simétrica permite que o NAT *suporte o endpoint independente*.

P. Qual é a diferença entre a fragmentação IP e a segmentação TCP?

R.A fragmentação de IP ocorre na Camada 3 (IP); a segmentação de TCP ocorre na Camada 4

(TCP). A fragmentação de IP ocorre quando os pacotes que são maiores do que a Unidade máxima de transmissão (MTU, Maximum Transmission Unit) de uma interface são enviados para fora desta interface. Esses pacotes precisam ser fragmentados ou descartados quando são enviados pela interface. Se a Don't Fragment (DF) bit não estiver definido no cabeçalho IP do pacote, o pacote poderá ser fragmentado. Se o bit DF estiver definido no cabeçalho IP do pacote, o pacote será descartado e uma mensagem de erro ICMP indicará o valor de MTU do próximo salto que é retornado ao remetente. Todos os fragmentos de um pacote IP carregam a mesma Ident no cabeçalho IP, o que permite que o receptor final remonte os fragmentos no pacote IP original. Consulte [Resolver problemas de fragmentação de IP, MTU, MSS e PMTUD com GRE e IPsec](#) para obter mais informações.

A segmentação do TCP ocorre quando um aplicativo em uma estação final envia dados. Os dados da aplicação são divididos no que o TCP considera os pedaços de melhor tamanho para enviar. Essa unidade de dados passada de TCP para IP é chamada de um segmento. Segmentos TCP são enviados em datagramas de IP. Esses datagramas de IP podem se tornar fragmentos de IP à medida que passam através da rede e encontram links de MTU menores do que podem fazer caber.

O TCP pode primeiro segmentar esses dados em segmentos TCP (com base no valor TCP MSS) e pode adicionar o cabeçalho TCP e passar esse segmento TCP para o IP. Em seguida, o IP pode adicionar um cabeçalho IP para enviar o pacote ao host final remoto. Se o pacote IP com o segmento TCP for maior que o IP MTU em uma interface de saída no caminho entre os hosts TCP, o IP poderá fragmentar o pacote IP/TCP para caber. Esses fragmentos de pacotes IP podem ser reagrupados no host remoto pela camada IP e o segmento TCP completo (que foi enviado originalmente) pode ser entregue à camada TCP. A camada TCP não tem ideia de que o IP tinha fragmentado o pacote durante o trânsito.

A NAT é compatível com fragmentos IP, mas não com segmentos TCP.

P. O NAT oferece suporte fora de serviço para fragmentação de IP e segmentação de TCP?

R.NAT suporta somente fragmentos IP fora de ordem porque **ofip virtual-reassembly**.

P. Como depurar a fragmentação IP e a segmentação TCP?

R.O NAT usa o mesmo CLI de depuração para a fragmentação de IP e a segmentação de TCP:**debug ip nat frag**.

P. Há um MIB NAT compatível?

R.Não. Não há MIB NAT suportado nem CISCO-IETF-NAT-MIB suportado.

P. O que é oTCP timeout e como ele se relaciona com o temporizador NAT TCP?

R.Se o handshake triplo não for concluído e o NAT vir um pacote TCP, o NAT poderá iniciar um temporizador de 60 segundos. Quando o handshake de três vias estiver concluído, a NAT usa um temporizador de 24 horas para uma entrada à NAT por padrão. Se um host final enviar um RESET, a NAT muda o temporizador padrão de 24 horas para 60 segundos. No caso de FIN, a NAT muda o temporizador padrão de 24 horas para 60 segundos quando ele recebe FIN e FIN-ACK.

P. Posso alterar a quantidade de tempo que leva para que uma conversão de NAT expire da tabela de conversão de NAT?

R.Sim. Você pode alterar os valores de tempo limite de NAT para todas as entradas ou para diferentes tipos de conversões de NAT (como udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout e arp-ping-timeout).

P. Como faço para interromper o Lightweight Directory Access Protocol (LDAP) quando ele anexa bytes extras a cada pacote de resposta LDAP?

R.O LDAP é definido para adicionar os bytes extras (resultados de pesquisa LDAP) enquanto processa mensagens do tipo Search-Res-Entry. O LDAP anexa 10 bytes de resultados de pesquisa para cada um dos pacotes de resposta do LDAP. Caso esses 10 bytes extras de dados resultem no pacote e excedam a Unidade Máxima de Transmissão (MTU) em uma rede, o pacote será descartado. Nesse caso, a Cisco recomenda que você desative esse comportamento LDAP com o comando **CLIno ip nat service append-ldap-search-respara** que os pacotes sejam enviados e recebidos.

P. Qual é a recomendação de rota para o endereço IP global interno/local externo na caixa NAT?

R.Uma rota deve ser especificada na caixa configurada de NAT para o endereço IP global interno para recursos como NAT-NVI. Da mesma forma, uma rota também deve ser especificada na caixa NAT para o endereço IP local externo. Nesse caso, qualquer pacote de uma direção de entrada para saída com a regra estática externa requer esse tipo de rota. Nesses cenários, enquanto fornece a rota para IG/OL, o endereço IP do próximo salto também deve ser configurado. Se a configuração do próximo salto não for encontrada, isso é considerado um erro de configuração e resulta em um comportamento indefinido.

O NVI-NAT só está presente no caminho de recurso de saída. Se você tiver conectado a sub-rede diretamente com NAT-NVI ou a regra de conversão NAT externa configurada na caixa, então, nesses casos, você precisa apresentar um endereço IP de próximo salto fictício e também um ARP associado para o próximo salto. É necessário para a infraestrutura subjacente entregar o pacote à NAT para conversão.

P. O NAT do Cisco IOS suporta ACLs com uma palavra-chave *log*?

R.Quando você configura o NAT do Cisco IOS para conversão de NAT dinâmico, uma ACL é usada para identificar os pacotes que podem ser convertidos. A arquitetura NAT atual não suporta ACLs com uma palavra-chave **log**.

NAT por voz

P. O NAT é compatível com o Skinny Client Control Protocol (SCCP) v17 fornecido com o Cisco Unified Communications Manager (CUCM) V7?

R.O CUCM 7 e todas as cargas de telefone padrão para o CUCM 7 suportam SCCPv17. A versão do SCCP usada é determinada pela versão comum mais alta entre CUCM e o telefone quando o telefone é registrado.

A NAT não é mais compatível com o SCCP v17. Até que o suporte NAT para SCCP v17 seja implementado, o firmware deve ser rebaixado para a versão 8-3-5 ou inferior para que o SCCP v16 seja negociado. O CUCM6 não pode encontrar o problema de NAT com qualquer carga de telefone, desde que use o SCCP v16. O Cisco IOS não é compatível com o SCCP versão 17.

P. Quais versões de carregamento de CUCM /SCCP/firmware são suportadas pelo NAT?

A.NAT suporta CUCM versão 6.x e versões anteriores. Essas versões do CUCM são lançadas com a carga de firmware de telefone de versão padrão 8.3.x (ou anterior) de firmware do telefone compatível com SCCP v15 (ou anterior).

A NAT não é compatível com CUCM versões 7.x ou posterior. Essas versões do CUCM são lançados com a carga de firmware de telefone 8.4.x padrão que é compatível com o SCCP v17 (ou posterior).

Se o CUCM 7.x ou posterior for usado, uma carga de firmware mais velha deve ser instalada no servidor CUCM TFTP para que os telefones usem uma carga de firmware com o SCCP v15 ou anterior para serem compatíveis com a NAT.

P. O que é o Service Provider PAT Port Allocation Enhancement para RTP e RTCP?

R.O recurso Aprimoramento de Alocação de Porta PAT do Provedor de Serviços para RTP e RTCP garante que para chamadas de voz SIP, H.323 e Skinny. Os números de porta usados para fluxos RTP são números de porta pares, e os fluxos RTCP são o próximo número da porta ímpar subsequente. O número da porta é convertido em um número dentro do intervalo especificado e que está em conformidade com o RFC-1889. Uma chamada com um número de porta dentro do intervalo pode resultar em uma conversão PAT para outro número de porta dentro desse intervalo. Da mesma forma, uma conversão PAT para um número de porta fora desse intervalo não pode resultar em uma conversão para um número dentro do intervalo especificado.

P. O que é o Session Initiation Protocol (SIP) e os pacotes SIP podem ser roteados com NAT?

R.O SIP (Session Initiation Protocol) é um protocolo de controle da camada de aplicação baseado em ASCII que pode ser usado para estabelecer, manter e terminar chamadas entre dois ou mais pontos finais. O SIP é um protocolo alternativo desenvolvido pela Internet Engineering Task Force (IETF) para conferência multimídia sobre IP. A implementação do Cisco SIP permite que plataformas compatíveis com a Cisco sinalizem a instalação de chamadas de voz e multimídia por redes IP. Os pacotes de SIP podem ser submetidos à NAT.

P. O que é o suporte Hosted NAT Traversal para Session Border Controller (SBC)?

R.O recurso Cisco IOS Hosted NAT Traversal for SBC permite que um roteador Cisco IOS NAT SIP Application-Level Gateway (ALG) atue como um SBC em um Cisco Multiservice IP-to-IP Gateway, o que ajuda a garantir uma entrega sem problemas de serviços de voz sobre IP (VoIP).

Consulte [Configurando o Cisco IOS Hosted NAT Traversal para Session Border Controller](#) para obter mais informações.

P. Quantas chamadas SIP, Skinny e H323 a memória e a CPU de um roteador podem lidar com NAT?

R.O número de chamadas tratadas por um roteador NAT depende da quantidade de memória disponível na caixa e da potência de processamento da CPU.

P. Um roteador NAT suporta segmentação TCP de pacotes Skinny e H323?

R.O Cisco IOS-NAT suporta segmentação TCP para H323 e segmentação TCP para SKINNY.

P. Há alguma advertência a ser observada quando você usa uma configuração de sobrecarga de NAT em uma implantação de voz?

R.Sim. Quando você tem configurações de sobrecarga de NAT e uma implantação de voz, você precisa da mensagem de registro para passar pela NAT e criar uma associação para out->in para chegar a este dispositivo interno. O dispositivo interno envia esse registro periodicamente e o NAT atualiza esse pin-hole/associação a partir das informações como na mensagem de sinalização.

P. Há algum problema conhecido causado quando você usa o comando `clear ip nat trans *` ou o comando `clear ip nat trans forced` em uma implantação de voz?

R.Em implantações de voz quando você executa o comando `clear ip nat trans *` ou o comando `clear ip nat trans forced` possui NAT dinâmico, você elimina o pin-hole/associação e deve aguardar o próximo ciclo de registro do dispositivo interno para estabelecer isso novamente. A Cisco recomenda que você não use esses comandos claros em uma implantação de voz.

P. O NAT é compatível com a solução co-localizada de voz?

R.Não. A solução colocalizada não é compatível no momento. A próxima implantação com NAT (na mesma caixa) é considerada uma solução co-localizada: CME/DSP-Farm/SCCP/H323.

P. O NVI é compatível com Skinny ALG, H323 ALG e TCP SIP ALG?

R.Não. Observe que o ALG UDP SIP (usado pela maioria das implantações) não é afetado.

NAT com VRF/MPLS

P. Um roteador NAT pode alguma vez suportar a si mesmo no mesmo espaço de endereço em um VRF e em um espaço de endereço global? No momento, eu recebo este aviso: "*% entrada estática semelhante (10.1.1.1 —> 10.2.2.2) já existe*" quando tento configurar isto:

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

R.O NAT legado suporta a sobreposição de configuração de endereço sobre VRFs diferentes. Você teria que configurar a sobreposição na regra com a opção `match-in-vrfoption` e configurar

upip nat inside/outside no mesmo VRF para o tráfego sobre esse VRF específico. A compatibilidade de sobreposição não inclui a tabela de roteamento global.

Você deve adicionar a **palavra-chave match-in-vrf** para as entradas de NAT estático VRF sobrepostas para VRFs diferentes. Entretanto, não é possível sobrepor endereços de NAT global e de vrf.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

P. O NAT legado suporta VRF-Lite (a rota de um VRF para um VRF diferente)?

R.Não. Você deve usar NVI para NAT entre VRFs diferentes. Você pode usar o NAT legado para fazer NAT de VRF para global ou NAT dentro do mesmo VRF.

NAT NVI

P. O que é NAT NVI?

A.NVI significa NAT Virtual Interface. Ele permite que a NAT converta entre dois VRFs diferentes. Essa solução deve ser usada em vez da Network Address Translation on a Stick.

P. O NAT NVI deve ser usado para rotear entre uma interface em global e uma interface em um VRF?

R.A Cisco recomenda que você use o NAT legado para VRF para NAT global (ip nat inside/out) e entre interfaces no mesmo VRF. A NVI é usada para NAT entre VRFs diferentes.

P. A segmentação TCP para NAT-NVI é suportada?

R.Não há suporte para segmentação TCP para NAT-NVI.

P. O NVI é compatível com Skinny ALG, H323 ALG e TCP SIP ALG?

R.Não. Observe que o ALG UDP SIP (usado pela maioria das implantações) não é afetado.

P. A segmentação TCP é compatível com SNAT?

R.SNAT não suporta nenhum ALG TCP (como SIP, SKINNY, H323 ou DNS). Portanto, a segmentação TCP não é compatível. No entanto, o UDP SIP e DNS são compatíveis.

SNAT

P. O que é o NAT stateful (SNAT)?

R.SNAT permite que dois ou mais tradutores de endereço de rede funcionem como um grupo de conversão. Um membro do grupo de conversão manipula o tráfego que exige a conversão de

informações de endereço IP. Além disso, ele informa o conversor de backup sobre os fluxos ativos à medida que eles ocorrem. O conversor de backup pode usar informações do conversor ativo para preparar entradas da tabela de conversão duplicada. Portanto, se o conversor ativo for prejudicado por uma falha crítica, o tráfego pode rapidamente ser alternado para o backup. O fluxo de tráfego continua, uma vez que as mesmas conversões de endereço de rede são utilizadas e o estado dessas conversões foi definido anteriormente.

P. A segmentação TCP é suportada com SNAT?

R.SNAT não suporta nenhum ALG TCP (como SIP, SKINNY, H323 ou DNS). Portanto, a segmentação TCP não é compatível. No entanto, o UDP SIP e DNS são compatíveis.

P. O SNAT é compatível com o roteamento assimétrico?

A. O roteamento assimétrico suporta NAT quando permite `as-queuing`. Por padrão, o enfileiramento como é habilitar. No entanto, a partir do ponto 24 da seção 12.4, `as-queuing` não é mais suportado. Os clientes devem se certificar de que os pacotes são roteados corretamente, e um atraso apropriado é adicionado para que o roteamento assimétrico funcione corretamente.

NAT-PT (v6 a v4)

P. O que é NAT-PT?

A.NAT-PT é a conversão de v4 para v6 para NAT. A Conversão de Protocolo (NAT-PT) é um mecanismo de conversão IPv6-IPv4, como definido [no RFC 2765](#) e [no RFC 2766](#), e permite que dispositivos somente IPv6 se comuniquem com dispositivos somente IPv4 e vice-versa.

P. O NAT-PT é suportado no caminho do Cisco Express Forwarding (CEF)?

A.NAT-PT não é suportado no caminho CEF.

P. Quais ALGs são suportados no NAT-PT?

R.O NAT-PT suporta TFTP/FTP e DNS. Voz e SNAT não são compatíveis na NAT-PT.

P. O ASR 1004 é compatível com NAT-PT?

R.Os roteadores de serviços de agregação (ASR) usam NAT64.

Cisco 7600/6k dependente de plataforma

P. O NAT stateful (SNAT) está disponível no Catalyst 6500 no trem SX?

A.SNAT não está disponível no Catalyst 6500 no trem SX.

P. O NAT com reconhecimento de VRF é compatível com hardware no 6k?

R.A NAT sensível a VRF não é suportada no hardware nesta plataforma.

P. O 7600 e o Cat6000 suportam NAT sensível a VRF?

R.Na plataforma 65xx/76xx, a NAT sensível a VRF não é suportada e as CLIs são bloqueadas.

Observação: você pode implementar um design se aproveitar um FWSM executado no modo transparente de contexto virtual.

Cisco 850 dependente da plataforma

P. O Cisco 850 suporta Skinny NAT ALG na versão 12.4T?

R.Não. Não há compatibilidade com NAT ALG Skinny em 12.4T no 850 Series.

Implantação de NAT

P. Como faço para implementar o NAT?

R.O NAT permite que redes IP privadas que usam endereços IP não registrados se conectem à Internet. A NAT converte o endereço privado (RFC1918) na rede interna em endereços roteáveis legais antes que os pacotes sejam encaminhados para outra rede.

P. Como implemento NAT com voz?

R.O suporte de NAT para o recurso de voz permite que as mensagens incorporadas de SIP que passam por um roteador configurado com Network Address Translation (NAT) sejam convertidas de volta para o pacote. Um gateway de camada de aplicativo (ALG) é usado com NAT para converter os pacotes de voz.

P. Como posso integrar o NAT com VPNs MPLS?

R.A integração de NAT com o recurso de VPNs MPLS permite que várias VPNs MPLS sejam configuradas em um único dispositivo para funcionar em conjunto. A NAT pode se diferenciar da VPN MPLS da qual recebe tráfego IP mesmo se todas as VPNs MPLS usarem o mesmo esquema de endereçamento IP. Esse aprimoramento permite que vários clientes de VPN MPLS compartilhem serviços enquanto garante que cada VPN MPLS seja completamente separada da outra.

P. O mapeamento estático de NAT oferece suporte a HSRP para alta disponibilidade?

R.Quando uma consulta ARP (Address Resolution Protocol) é disparada para um endereço configurado com o mapeamento estático NAT (Network Address Translation) e de propriedade do roteador, o NAT responde com o endereço MAC BIA na interface para a qual o ARP aponta. Dois roteadores atuam como HSRP ativo e em espera. Suas interfaces com NAT no interior devem ser habilitadas e configuradas para pertencer a um grupo.

P. Como implemento a NAT NVI?

R.O recurso NAT virtual interface (NVI) remove o requisito de configurar uma interface como NAT interno ou NAT externo.

P. Como implemento o balanceamento de carga com o NAT?

R.Há dois tipos de balanceamento de carga que podem ser feitos com o NAT: você pode balancear a carga de entrada para um conjunto de servidores para distribuir a carga nos servidores e pode balancear a carga do seu tráfego de usuário para a Internet através de dois ou mais ISPs.

Para obter mais informações sobre balanceamento de carga de saída, consulte [Balanceamento de Carga NAT do Cisco IOS para Duas Conexões ISP](#).

P. Como faço para implementar o NAT em conjunto com o IPSec?

R.Há suporte para IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT e transparência de NAT de IPSec.

O ESP de IPSec, por meio do recurso de NAT, possibilita a compatibilidade com vários túneis ou conexões de ESP de IPSec concomitantes por meio de um dispositivo de NAT do Cisco IOS configurado em modo de sobrecarga ou Conversão de Endereço de Porta (PAT). O recurso de transparência de NAT de IPSec apresenta suporte para tráfego de IPSec para trafegar através de pontos NAT ou PAT na rede quando aborda muitas incompatibilidades conhecidas entre NAT e IPSec.

P. Como faço para implementar o NAT-PT?

A.NAT-PT (Network Address Translation—Protocol Translation) é um mecanismo de tradução IPv6-IPv4, como definido [noRFC 2765](#)e noRFC 2766, **que permite que dispositivos somente IPv6 se comuniquem com dispositivos somente IPv4 e vice-versa.**

P. Como implemento o NAT multicast?

R.É possível fazer NAT do IP de origem para um fluxo multicast. Um mapa de rota não pode ser usado quando um NAT dinâmico para multicast é feito, somente uma lista de acesso é suportada para isso.

Para obter mais informações, consulte [Como o NAT Multicast Funciona nos Roteadores Cisco](#). O grupo multicast de destino usa NAT com uma solução Multicast Service Reflection.

P. Como faço para implementar o NAT stateful (SNAT)?

A.SNAT permite o serviço contínuo para sessões NAT mapeadas dinamicamente. As sessões definidas estaticamente têm o benefício da redundância sem a necessidade de SNAT. Na ausência de SNAT, as sessões que usam mapeamentos de NAT dinâmico serão interrompidas em caso de falha crítica e precisarão ser restabelecidas. Apenas a configuração mínima da SNAT é compatível. As implantações futuras devem ser executadas somente depois que você conversar com sua equipe de conta da Cisco para validar o projeto relativo às restrições atuais.

A SNAT é recomendada para os próximos cenários:

- O modo primário/backup não é recomendado, pois há alguns recursos ausentes em comparação ao HSRP.
- Para situações de failover e de configuração do roteador 2. Ou seja, se um roteador falhar, o outro roteador assume sem problemas. (A arquitetura da SNAT não é projetada para lidar com oscilação de interface.)
- O cenário de roteamento não assimétrico é compatível. O roteamento assimétrico pode ser tratado apenas se a latência no pacote de resposta for maior do que entre 2 roteadores SNAT para trocar mensagens de SNAT.

Atualmente, a arquitetura SNAT não é projetada para lidar com a robustez; portanto, não se espera que esses testes sejam bem-sucedidos:

- Quando as entradas NAT são apagadas enquanto há tráfego.
- Quando os parâmetros da interface (como alteração de endereço IP, shut/no-shut, etc.) são alterados enquanto houver tráfego.
- Não se espera que os comandos `clearorshovespecíficos` de SNAT sejam executados corretamente e não são recomendados. Alguns dos comandos SNAT `relatedclearandshows` são os seguintes:

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>
```

- Se o usuário quiser limpar as entradas, os comandos **clear ip nat trans forced** ou **clear ip nat trans *** podem ser usados. Se o usuário quiser ver as entradas, os comandos **show ip nat translation**, **show ip nat translations verbose**, e **show ip nat stats** podem ser usados. Se o serviço interno estiver configurado, ele também poderá mostrar informações específicas de SNAT.
- As conversões de NAT são apagadas no roteador de backup não é recomendado. Sempre limpe as entradas NAT no roteador SNAT principal.
- SNAT não é HA; portanto, as configurações em ambos os roteadores devem ser as mesmas. Ambos os roteadores devem executar a mesma imagem. Além disso, certifique-se de que a plataforma subjacente usada para ambos os roteadores SNAT seja a mesma.

Melhores práticas de NAT

P. Há alguma prática recomendada de NAT?

R. Sim. Estas são as melhores práticas de NAT:

1. Quando você usa NAT dinâmico e estático, a ACL que define a regra para NAT dinâmico deve excluir os hosts locais estáticos para que não haja sobreposição.

2. Se você usar ACL para NAT **com permit ip any any**, poderá obter resultados imprevisíveis. Depois da versão 12.4(20)T, o NAT pode converter pacotes HSRP e de protocolo de roteamento gerados localmente se eles forem enviados pela interface externa, bem como pacotes criptografados localmente que correspondam à regra NAT.
3. Quando houver redes sobrepostas para NAT, use a **palavra-chave match-in-vrfkeyword**. Você deve adicionar a palavra-chave **match-in-vrf** para as entradas de NAT estático VRF sobrepostas para VRFs diferentes, mas não é possível sobrepor endereços de NAT global e vrf.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
```

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

4. Pools NAT com o mesmo intervalo de endereços não podem ser usados em VRFs diferentes, a menos que a palavra-chave **match-in-vrf** seja usada. Por exemplo:

```
ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
ip nat pool poolB 172.31.1.1 172.31.1.10 prefix-length 24
ip nat inside source list 1 poolA vrf A match-in-vrf
ip nat inside source list 2 poolB vrf B match-in-vrf
```

Observação: embora a configuração da CLI seja válida, sem a palavra-chave **match-in-vrf**, a configuração não é suportada.

5. Quando você implanta o balanceamento de carga dos ISPs com a sobrecarga da interface NAT, a prática recomendada é usar o mapa de rota com correspondência de interface sobre correspondência de ACL.
6. Ao usar o mapeamento de pool, você não deve usar dois mapeamentos diferentes (ACL ou mapa de rota) para compartilhar o mesmo endereço de pool de NAT.
7. Ao implantar as mesmas regras de NAT em dois roteadores diferentes no cenário de failover, você deve usar a redundância de HSRP.
8. Não defina o mesmo endereço global interno em NAT estática e um pool dinâmico. Essa ação gerar resultados indesejáveis.

Informações Relacionadas

- [Suporte Técnico e Documentação - 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.