FlexVPN: IPv6 em um exemplo da configuração de distribuição do hub and spoke

Índice

Introdução

Este documento descreve uma configuração comum que use o Cisco IOS que o ® FlexVPN falou e desenvolvimento do hub em um ambiente do IPv6. Expande nos conceitos discutidos em FlexVPN: IPv6 LAN básico à configuração LAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS FlexVPN
- Protocolos de Roteamento

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Geração 2 do Roteadores dos Serviços integrados de Cisco (ISR G2)
- Cisco IOS Software Release 15.3 (ou liberação 15.4T para túneis spoke-to-spoke dinâmicos com IPv6)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

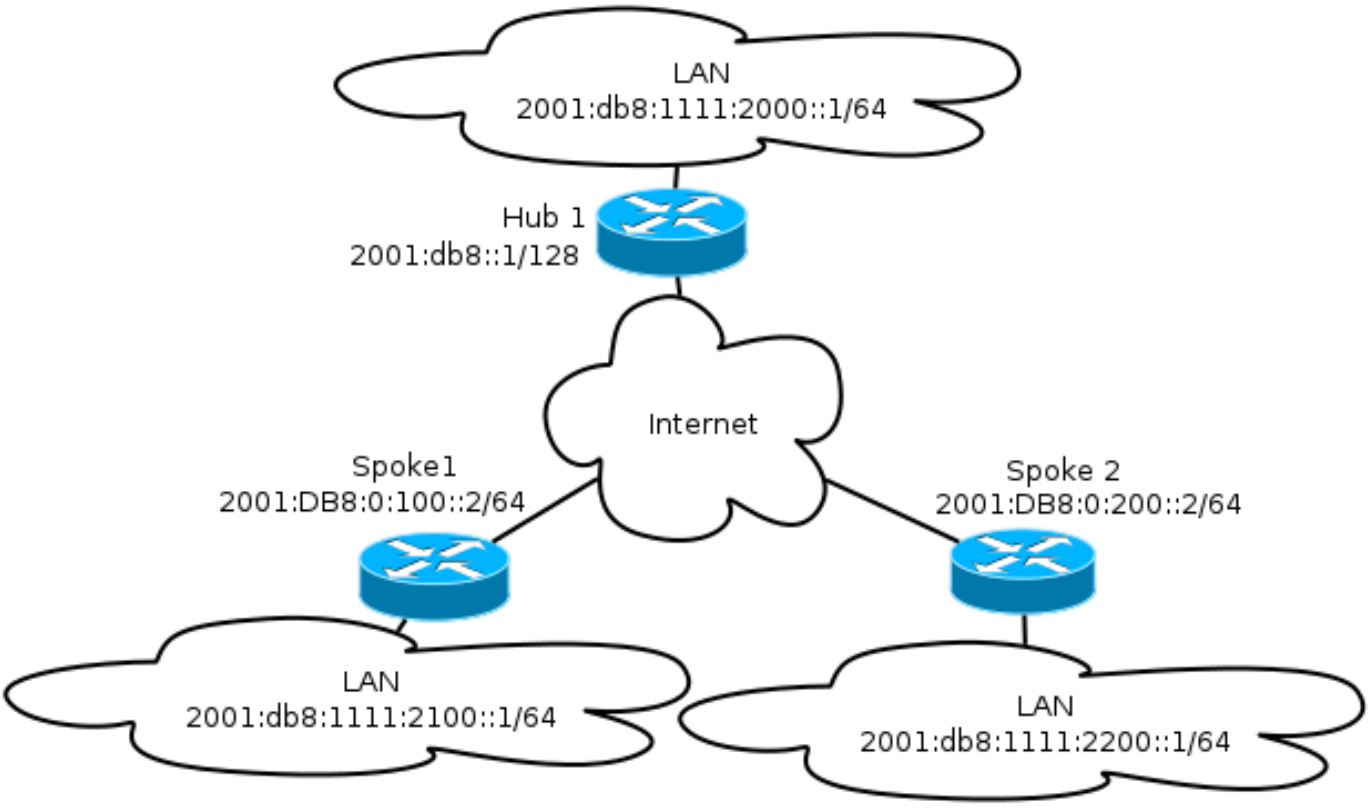
> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Quando estes exemplo de configuração e diagrama da rede usarem o IPv6 como a rede de transporte, o Generic Routing Encapsulation (GRE) está usado tipicamente em disposições de FlexVPN. O uso do GRE em vez do IPsec permite que os administradores executem o IPv4 ou o IPv6 ou ambos sobre os mesmos túneis, apesar da rede de transporte.

Diagrama de Rede

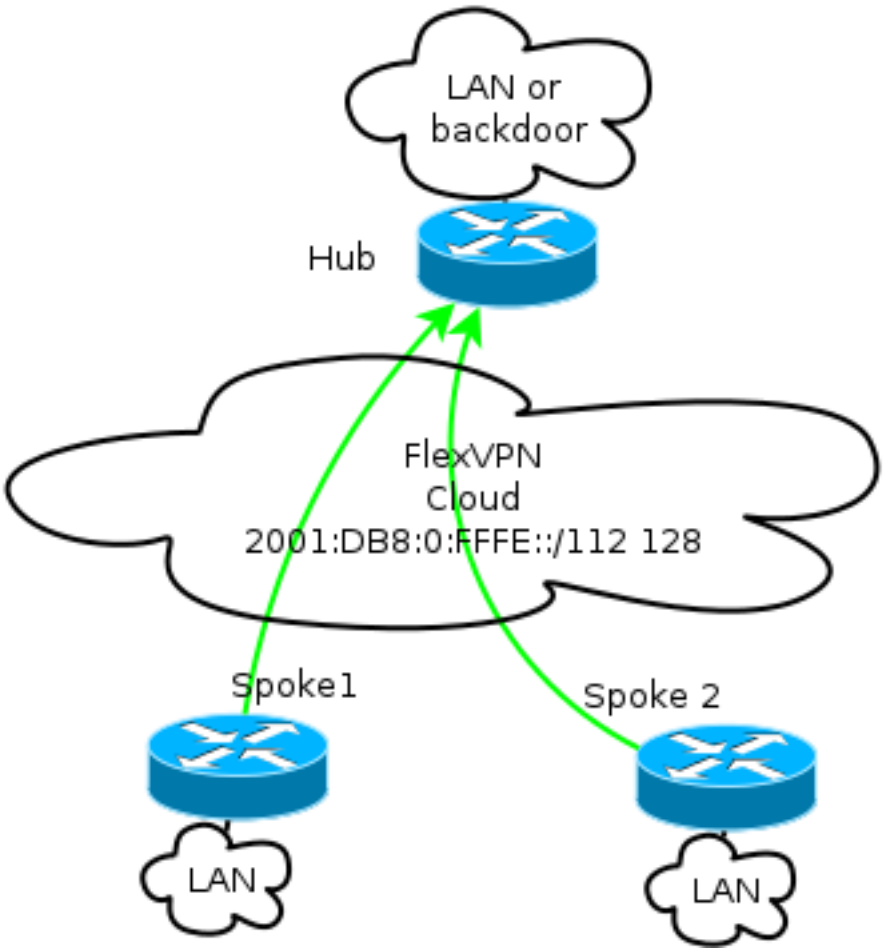
Rede de transporte

Este é um diagrama da rede de transporte usada neste exemplo:



Rede de folha de prova

Este é um diagrama da topologia de rede básica da folha de prova usada neste exemplo:



Cada spoke é atribuído de um conjunto de endereço de /112, mas recebe um endereço de /128. Assim, a notação '/112 128' é usada na configuração de pool do IPv6 do hub.

Configurações

Esta configuração mostra um IPv4 e o IPv6 overlay que trabalha sobre um backbone do IPv6.

Quando comparado aos exemplos que usam o IPv4 como um backbone, note que você deve usar a mudança do nó do **comando tunnel mode** e para acomodar o transporte do IPv6.

A característica spoke-to-spoke do túnel sobre o IPv6 será introduzida no Cisco IOS Software Release 15.4T, que não está ainda disponível.

Protocolos de Roteamento

Cisco recomenda que você usa o internal border gateway protocol (iBGP) espreitando entre o spoke e o Hubs para grandes disposições porque o iBGP é a maioria de protocolo do roteamento escalável.

O Border Gateway Protocol (BGP) escuta escala não apoia a escala do IPv6, mas simplifica o uso com um transporte do IPv4. Embora seja praticável usar o BGP em tal ambiente, esta configuração ilustra um exemplo básico, assim que o Enhanced Interior Gateway Routing Protocol (EIGRP) foi escolhido.

Configuração do hub

Comparado a uns exemplos mais velhos, esta configuração inclui o uso de protocolos de transporte novos.

A fim configurar o hub, o administrador precisa:

- Permita o roteamento do unicast.
- Provision o roteamento do transporte.
- Provision um pool novo dos endereços do IPv6 a ser atribuídos dinamicamente. O pool é 2001:DB8:0:FFFE::/112; 16 bit permitem 65,535 dispositivos ser endereçados.
- Permita o IPv6 para a configuração do Next Hop Resolution Protocol (NHRP) a fim permitir o IPv6 na folha de prova.
- Esclareça o IPv6 que endereça no keyring assim como no perfil na configuração de criptografia.

Neste exemplo, o hub anuncia um sumário EIGRP a todo o spokes.

Cisco não recomenda o uso de um endereço sumário na interface de molde virtual no desenvolvimento de FlexVPN; contudo, em um Dynamic Multipoint VPN (DMVPN), isto é não somente comum mas é considerado igualmente um melhor prática. Veja a migração de FlexVPN: Movimento duro do DMVPN a FlexVPN nos mesmos dispositivos: Configuração actualizado do hub para detalhes.

```
ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
 ipv6 pool FlexSpokesv6
pool FlexSpokes
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

interface Virtual-Template1 type tunnel
```

```
ip unnumbered Loopback100
ip mtu 1400
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Loopback100
ipv6 enable
ipv6 eigrp 65001
 ipv6 nhrp network-id 2
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
 distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Template1
 network 10.1.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 redistribute static metric 1500 10 10 1 1500

ipv6 router eigrp 65001
 distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1
 redistribute static metric 1500 10 10 1 1500
```

Configuração de raio

Como na configuração do hub, o administrador precisa de provision o IPv6 que endereça, de permitir o IPv6 que distribui, e de adicionar o NHRP e a configuração de criptografia.

Épraticável usar o EIGRP e os outros protocolos de roteamento para espreitar spoke-to-spoke. Contudo, em um cenário típico, os protocolos não são precisados e puderam impactar a escalabilidade e a estabilidade.

Neste exemplo, a configuração de roteamento mantém somente a adjacência EIGRP entre o spoke e o hub, e a única relação que não é passiva é a relação Tunnel1:

```
ipv6 unicast-routing
ipv6 cef

crypto logging session
```

```
crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

interface Tunnel1
description FlexVPN tunnel
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel source Ethernet0/0
 tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Ethernet1/0
ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

Siga estas recomendações quando você cria entradas do protocolo de roteamento em um spoke:

1. Permita que o protocolo de roteamento estabeleça um relacionamento através da conexão (neste caso, a relação Tunnel1) ao hub. Não é geralmente desejável estabelecer a adjacência do roteamento entre o spokes porque este aumenta significativamente a complexidade na maioria dos casos.

2. Anuncie sub-redes do LAN local somente, e permita o protocolo de roteamento em um endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído pelo hub. Seja cuidadoso não anunciar uma grande sub-rede porque pôde impactar uma comunicação spoke-to-spoke.

Este exemplo reflete ambas as recomendações para o EIGRP em Spoke1:

```
ipv6 unicast-routing
ipv6 cef

crypto logging session

crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto ikev2 dpd 30 5 on-demand

interface Tunnel1
description FlexVPN tunnel
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel source Ethernet0/0
 tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
```

```
 ipv6 unnumbered Ethernet1/0
ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

> Nota: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Sessão spoke-to-hub

Uma sessão corretamente configurada entre o spoke e os dispositivos do hub tem uma sessão da versão 2 do intercâmbio de chave de Internet (IKEv2) que seja ascendente e tem um protocolo de roteamento que possa estabelecer a adjacência. Neste exemplo, o protocolo de roteamento é EIGRP, tão lá é dois comandos eigrp:

- mostre ikev2 criptos sa
- mostre o vizinho do eigrp 65001 do IPv6
- mostre o vizinho do eigrp 65001 IP

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none            READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/1945 sec

Spoke1#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   Link-local address:     Tu1                  14 00:32:29   72  1470  0  10
   FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                              (sec)         (ms)       Cnt Num
0   10.1.1.1                Tu1                  11 00:21:05   11  1398  0  26
```

No IPv4, o EIGRP usa um endereço IP atribuído para espreitar; no exemplo anterior, é o endereço IP de Um ou Mais Servidores Cisco ICM NT do hub de 10.1.1.1.

O IPv6 usa um endereço local de link; neste exemplo, o hub é FE80::A8BB:CCFF:FE00:6600. Use o **comando ping** a fim verificar que o hub pode ser alcançado através de seu IP do link local:

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

Sessão spoke-to-spoke

As sessões spoke-to-spoke são trazidas acima dinamicamente por encomenda. Use um comando de ping simples a fim provocar uma sessão:

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

Para confirmar a Conectividade spoke-to-spoke direta, o administrador precisa:

- Verifique que uma sessão spoke-to-spoke dinâmica provoca uma interface de acesso virtual nova:

  ```
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
  state to up
  %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.
  Peer 2001:DB8:0:200::2:500       Id: 2001:DB8:0:200::2
  ```

- Verifique o estado de sessão IKEv2:

  ```
  Spoke1#show crypto ikev2 sa
   IPv4 Crypto IKEv2  SA

   IPv6 Crypto IKEv2  SA

  Tunnel-id    fvrf/ivrf              Status
  1          none/none             READY
  Local  2001:DB8:0:100::2/500
  Remote  2001:DB8::1/500
       Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
  Auth verify: PSK
       Life/Active Time: 86400/3275 sec

  Tunnel-id    fvrf/ivrf              Status
  2          none/none             READY
  Local  2001:DB8:0:100::2/500
  Remote  2001:DB8:0:200::2/500
       Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
  Auth verify: PSK
       Life/Active Time: 86400/665 secNote que duas sessões estão disponíveis: um spoke-to-hub e um spoke-to-spoke.
  ```

- Verifique o NHRP:

```
Spoke1#show ipv6 nhrp
2001:DB8:0:FFFE::/128 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
2001:DB8:1111:2200::/64 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
NBMA address: 2001:DB8:0:200::2
```

A saída mostra que 2001:DB8:1111:2200::/64 (o LAN para Spoke2) está disponível através de 2001:DB8:0:FFFE:: , que é o endereço negociado do IPv6 na relação Tunnel1 para Spoke2. A relação Tunnel1 está disponível através do endereço do multiacesso sem broadcast (NBMA) de 2001:db8:0:200::2, que é o endereço do IPv6 atribuído a Spoke2 estaticamente.

- Verifique que o tráfego está passando através dessa relação:

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0)
  remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0)
  current_peer 2001:DB8:0:200::2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196
   #pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195
(...)
```

- Verifique o caminho de roteamento e ajustes CEF:

```
Spoke1#show ipv6 route
(...)
D   2001:DB8:1111:2200::/64 [90/27161600]
    via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut]
    via FE80::A8BB:CCFF:FE00:6600, Tunnel1
(...)
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
 nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

> Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Estes comandos debug ajudam-no a pesquisar defeitos edições:

- FlexVPN/IKEv2 e IPsec: debug crypto ipsecdebug crypto ikev2 [pacote|interno]
- NHRP (spoke-to-spoke):

- debugar o bloco do nhrp
- debugar a extensão do nhrp
- debugar o esconderijo do nhrp
- debugar a rota do nhrp

Refira o Cisco IOS comando list mestre, todas as liberações para obter mais informações sobre destes comandos.