FlexVPN ：在一星型网部署配置示例的IPv6

目录

简介

本文描述使用Cisco IOS FlexVPN发言和在IPv6环境的集线器部署的常见配置。它在FlexVPN讨论的概念展开 ：对LAN配置的IPv6基本LAN。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS FlexVPN
- 路由协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科集成服务路由器生成2 (ISR G2)
- Cisco IOS软件版本动态spoke-to-spoke通道的15.3 (或版本15.4T有IPv6的)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

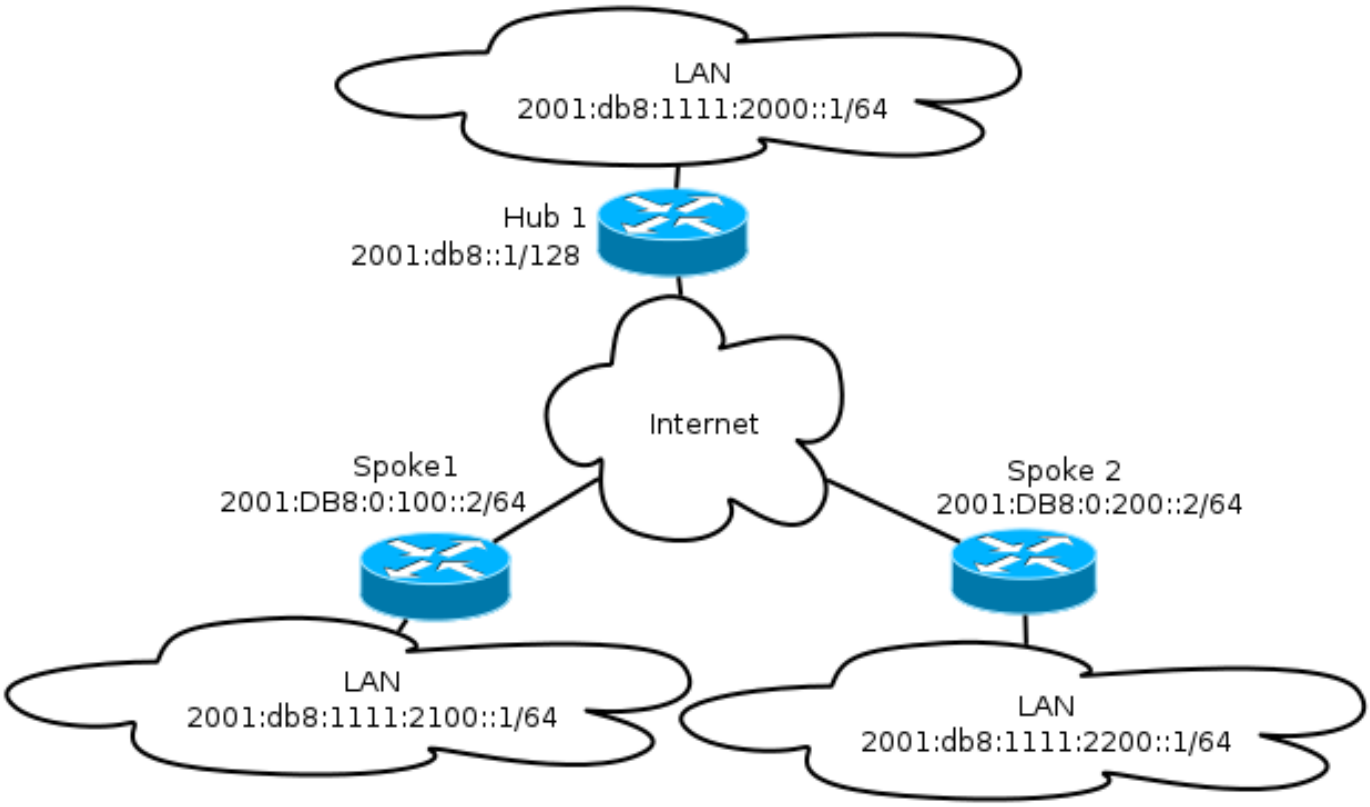
注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

当此配置示例和网络图使用IPv6作为传输网络时，通用路由封装(GRE)典型地用于FlexVPN部署。不管传输网络，使用而不是IPsec的GRE允许管理员运行IPv4或IPv6或者两个在同样通道。

网络图

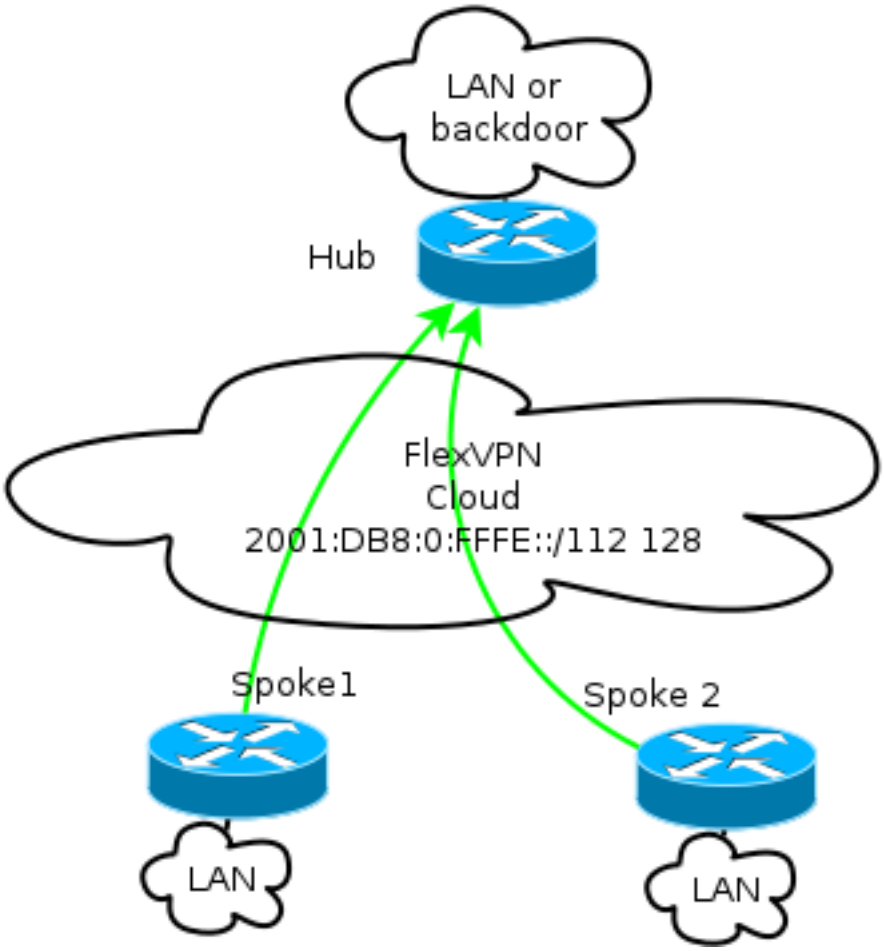
传输网络

这是用于此示例的传输网络的图表：



覆盖网络

这是用于此示例的基本重叠网络拓扑的图表：



每分支从地址池/112分配，但是收到/128地址。因此，符号'/112 128'用于集线器的IPv6池配置。

配置

在IPv6骨干网工作的此配置显示被覆盖的IPv4和IPv6。

当与使用IPv4作为骨干网的示例比较，请注意您应该使用**tunnel mode命令**为了节点更改和适应IPv6传输。

在IPv6的spoke-to-spoke通道功能在Cisco IOS软件版本15.4T将介绍，不是联机。

路由协议

思科建议您使用内部边界网关协议(iBGP)并列在分支和集线器之间大部署的，因为iBGP是多数可升级的路由协议。

边界网关协议(BGP)侦听范围不支持IPv6范围，但是简化与IPv4传输的使用情况。虽然可行使用BGP在这样环境，此配置说明基本示例，因此增强的内部网关路由选择协议(EIGRP)选择。

中心配置

与更旧的示例比较，此配置包括使用新的传输协议。

为了配置集线器，管理员需要：

- Enable (event)单播路由。
- 提供传输路由。
- 设置IPv6地址新池将动态地分配的。池是2001:DB8:0:FFFE::/112;16个位允许将寻址的65,535个设备。
- 使下一跳解析协议(NHRP)配置的IPv6为了允许在重叠的IPv6。
- 占IPv6寻址在钥匙圈以及配置文件在加密配置里。

在本例中，集线器通告EIGRP摘要对所有spoke。

思科不推荐使用在虚拟模板接口的一summary-address在FlexVPN部署;然而，在动态多点VPN (DMVPN)，这不仅普通，但是也认为最佳实践。请参阅FlexVPN迁移：从DMVPN的硬移动到在同样设备的FlexVPN ：更新集线器上配置关于详细信息。

```
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
```

分支配置

正如在集线器上配置，寻址的管理员需要设置IPv6，路由enable (event)的IPv6，并且添加NHRP和加密配置。

可行使用EIGRP和其他路由协议spoke-to-spoke同位体。然而，在典型方案，协议不是需要的，并且也许影响可扩展性和稳定性。

在本例中，路由配置保持在分支和集线器之间的仅EIGRP邻接，并且不被动的唯一的接口是Tunnel1接口：

```
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
```

当您创建在分支时的路由协议条目请遵从这些建议：

1. 允许路由协议通过连接建立关系(在这种情况下， Tunnel1接口)对集线器。因为这极大增加复杂性在大多数情况下，设立在spoke之间的路由邻接通常是不理想的。

2. 通告仅本地LAN子网，并且启用在集线器分配的IP地址的路由协议。因为也许影响spoke-to-spoke通信，小心不通告一大子网。

此示例反射EIGRP的两建议在分支1 ：

```
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
```

验证

使用本部分可确认配置能否正常运行。

> **注意**：命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

spoke-to-hub会话

在分支和集线器设备之间的一适当地配置的会话有启用的一互联网密钥交换版本2 (IKEv2)会话并且有能设立邻接的路由协议。在本例中，路由协议是EIGRP，那么那里是两个EIGRP命令：

- 显示crypto ikev2 sa
- 显示IPv6 eigrp 65001邻居
- show ip eigrp 65001邻居

```
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
```

在IPv4， EIGRP使用一个指定的IP地址并列;在前一个示例中，它是10.1.1.1的集线器IP地址。

IPv6使用一个链路本地地址;在本例中，集线器是FE80::A8BB:CCFF:FE00:6600。请使用ping命令为了验证集线器可以通过其链路本地IP:被到达

```
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
```

spoke-to-spoke会话

spoke-to-spoke会话启动动态地根据要求。请使用一简单的ping命令为了触发会话：

```
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
```

要确认直接spoke-to-spoke连接，管理员需要：

- 验证一动态spoke-to-spoke会话触发一个新的虚拟访问接口：

```
%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
```

- 验证IKEv2会话状态：

```
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 sec
```

注意两会话是可用的：一spoke-to-hub和一个spoke-to-spoke。

- 验证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
```

输出显示2001:DB8:1111:2200::/64 (分支2的LAN)通过2001:DB8:0:FFFE是可用的： ：是在Tunnel1接口的经过协商的IPv6地址分支2的。Tunnel1接口通过2001:db8:0:200::2非广播多路访问(NBMA)地址是可用的，是IPv6地址静态分配到分支2。

- 验证流量通过该接口通过：

```
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
(...)
```

- 验证路由路径和CEF设置：

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

> **注意**：使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

这些调试您排除故障问题的help命令：

- FlexVPN/IKEv2和IPsec ： **debug crypto ipsecdebug crypto ikev2 [数据包|内部]**
- NHRP (spoke-to-spoke) ：
  - **调试NHRP装箱**
  - **debug nhrp extension**
  - **调试NHRP缓存**
  - **调试NHRP路由**

参考Cisco IOS重要的List命令，所有版本关于这些命令的更多信息。