

FlexVPN：ハブ アンド スポーク導入における IPv6 の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[トランスポート層 ネットワーク](#)

[オーバーレイ ネットワーク](#)

[設定](#)

[ルーティング プロトコル](#)

[ハブの設定](#)

[スポーク設定](#)

[確認](#)

[スポークとハブの間のセッション](#)

[スポーク間のセッション](#)

[トラブルシューティング](#)

概要

このドキュメントでは、IPv6 環境での Cisco IOS^(R) FlexVPN スポークおよびハブの導入を使用する一般的な設定について説明します。これは、「[FlexVPN: IPv6 の基本的な LAN-to-LAN 設定](#)」(英語)で説明する概念から展開されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS FlexVPN
- ルーティング プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- シスコ第 2 世代サービス統合型ルータ (ISR G2)
- Cisco IOS ソフトウェア リリース 15.3 (または IPv6 の動的なスポーク間トンネル向けのリリース 15.4T)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

この設定例とネットワーク図では、転送ネットワークとして IPv6 を使用していますが、FlexVPN の導入では、Generic Routing Encapsulation (GRE) が一般的に使用されます。IPSec ではなく、GRE を使用すると、管理者は、転送ネットワークに関係なく、同じトンネルで IPv4、IPv6、またはその両方を実行できます。

ネットワーク図

転送ネットワーク

これは、この例で使用される転送ネットワークの図です。

オーバーレイ ネットワーク

これは、この例で使用される基本的なオーバーレイ ネットワーク トポロジの図です。

各スポークは、/112 のアドレスのプールから割り当てられますが、/128 アドレスを受け取ります。したがって、ハブの IPv6 プール設定では、「/112 128」という表記が使用されます。

設定

この設定は、IPv6 バックボーン上で動作する IPv4 および IPv6 オーバーレイを示します。

バックボーンとして IPv4 を使用する例と比較した場合、**tunnel mode** コマンドを使用して、ノードを変更し、IPv6 転送に対応する必要があることに注意してください。

IPv6 でのスポーク間トンネル機能は、まだリリースされていない Cisco IOS ソフトウェア リリース 15.4T で導入されます。

ルーティング プロトコル

シスコでは、大規模な導入でのスポークとハブの間のピアリングには内部ボーダー ゲートウェイ プロトコル (iBGP) を使用することを推奨しています。これは、iBGP が、最もスケーラブルなルーティング プロトコルであるためです。

ボーダー ゲートウェイ プロトコル (BGP) のリッスン範囲は IPv6 範囲をサポートしていませんが、IPv4 転送での使用を簡素化します。このような環境で BGP を使用することはできますが、この設定は基本的な例を示しているため、Enhanced Interior Gateway Routing Protocol (EIGRP) が選択されています。

ハブの設定

古い例と比較して、この設定では、新しい転送プロトコルが使用されます。

ハブを設定するために管理者は、以下を実行する必要があります。

- ユニキャスト ルーティングを有効にする。
- 転送ルーティングをプロビジョニングする。
- 動的に割り当てる IPv6 アドレスの新しいプールをプロビジョニングする。プールは 2001:DB8:0:FFFE::/112 です。16 ビットで、65,535 のデバイスのアドレスを設定できます。
- Next Hop Resolution Protocol (NHRP) 設定用に IPv6 を有効にして、オーバーレイで IPv6 を許可します。
- キーリングの IPv6 アドレス設定と暗号設定のプロファイルを構成します。

この例では、ハブが、すべてのスポークに EIGRP サマリーをアドバタイズします。

シスコでは、FlexVPN の導入の仮想テンプレート インターフェイスでのサマリー アドレスの使用を推奨していません。ただし、Dynamic Multipoint VPN (DMVPN) では、これが一般的であるだけでなく、ベスト プラクティスとも見なされています。詳細については、「[FlexVPN の移行：同じデバイスでの DMVPN から FlexVPN への完全移行](#)」(英語) の「[更新されたハブ設定](#)」を参照してください。

```
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-Templatel 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-Templatel
  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-Templatel
  redistribute static metric 1500 10 10 1 1500

```

スポークの設定

「[ハブの設定](#)」にあるように、管理者は、IPv6 アドレスをプロビジョニングし、IPv6 ルーティングを有効にし、NHRP とクリプト設定を追加する必要があります。

スポーク間のピアリングには、EIGRP およびその他のルーティング プロトコルを使用できません。ただし、一般的なシナリオでは、プロトコルは不要であり、スケーラビリティと安定性に影響を与える可能性があります。

この例では、ルーティング設定により、スポークとハブの間の EIGRP 隣接関係だけが保持され、パッシブでないインターフェイスは Tunnel1 インターフェイスだけです。

```
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-Templatel 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
```

スポークでルーティング プロトコル エントリを作成する場合は、次の推奨事項に従ってください

。

1. ルーティングプロトコルが、ハブへの接続（この場合は Tunnel1 インターフェイス）を介して関係を確認できるようにします。ほとんどの場合は複雑さが大幅に増すため、一般的には、スポーク間のルーティング隣接関係を確認することは望ましくありません。

2. ローカル LAN のサブネットだけをアドバタイズし、ハブで割り当てられた IP アドレスでルーティングプロトコルを有効にします。大規模なサブネットは、スポーク間の通信に影響を及ぼす可能性があるため、アドバタイズしないように注意してください。

この例には、Spoke1 での EIGRP の推奨事項が両方とも反映されています。

```
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-Templatel 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
```

確認

ここでは、設定が正常に動作していることを確認します。

注: 特定の show コマンドが [アウトプット インタープリタ ツール \(登録ユーザ専用\)](#) でサポートされています。show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

スポークとハブの間のセッション

スポークとハブ デバイス間の適切に設定されたセッションでは、Internet Key Exchange バージョン 2 (IKEv2) セッションが稼働しており、これには、隣接関係を確立できるルーティング プロトコルが含まれます。この例では、ルーティング プロトコルは EIGRP であるため、2 つの EIGRP コマンドがあります。

- **show crypto ikev2 sa**
- **show ipv6 eigrp 65001 neighbor**
- **show ip eigrp 65001 neighbor**

```
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
```

IPv4 では、EIGRP が、ピアに割り当てられた IP アドレスを使用します。前の例では、これは、

10.1.1.1 というハブの IP アドレスです。

IPv6 はリンクローカル アドレスを使用します。この例では、ハブは FE80::A8BB:CCFF:FE00:6600 です。ping コマンドを使用して、リンクローカル IP を介してハブに到達できることを確認します。

```
Spokel#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnell
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%Tunnell
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

スポーク間のセッション

スポーク間のセッションは、必要に応じて動的に開始されます。単純な ping コマンドを使用してセッションをトリガーします。

```
Spokel#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnell
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%Tunnell
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

直接のスポーク間接続を確認するために、管理者は、以下を実行する必要があります。

- 動的なスポーク間セッションで新しい仮想アクセス インターフェイスがトリガーされることを確認する。

```
%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
```

- IKEv2 セッションの状態を確認する。

```
Spokel#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 2つのセッションが使用可能であることに注意してください。1つはスポークとハブの間、もう1つはスポーク間です。

- NHRPを確認する。

```
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出力は、2001:DB8:1111:2200::/64 (Spoke2 の LAN) が 2001:DB8:0:FFFE:: を介して使用可能であることを示します。2001:DB8:0:FFFE:: は、Spoke2 の Tunnel1 インターフェイスでネゴシエートされた IPv6 アドレスです。Tunnel1 インターフェイスは、2001:db8:0:200::2 という非ブロードキャスト マルチアクセス (NBMA) アドレスを介して使用できます。このアドレスは、Spoke2 に静的に割り当てられた IPv6 アドレスです。

- トラフィックがこのインターフェイスを通過していることを確認する。

```
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
(...)
```

- ルーティングパスとCEF設定を確認する。

```
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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

次の debug コマンドが、問題のトラブルシューティングに役立ちます。

- FlexVPN/IKEv2 と IPsec : `debug crypto ipsecdebug crypto ikev2 [packet|internal]`
- NHRP (スポーク間) :
 - `debug nhrp pack`
 - `debug nhrp extension`
 - `debug nhrp cache`
 - `debug nhrp route`

これらのコマンドの詳細については、「[Cisco IOS マスター コマンド リスト、すべてのリリース](#)」(英語) を参照してください。