DMVPN 経由の IPv6

このマニュアルでは、Dynamic Multipoint VPN for IPv6 機能の実装方法について説明します。この機能を使用すると、ユーザは、総称ルーティング カプセル化（GRE）トンネル、IP Security（IPsec）暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせることにより、目的に合わせて大小さまざまな規模の IPsec バーチャル プライベート ネットワーク（VPN）を構築できます。Dynamic Multipoint Virtual Private Network（DMVPN）for IPv6 では、パブリック ネットワーク（インターネット）は純粋な IPv4 ネットワークであり、プライベート ネットワーク（イントラネット）は IPv6 に対応しています。

DMVPN での IPv6 サポートは、インターネット サービス プロバイダー（ISP）方向のパブリック ネットワーク（インターネット）に拡張されました。DMVPN 用の IPv6 トランスポート機能は、IPv6 WAN 側の機能を NHRP トンネルと基礎となる IPsec 暗号化に構築して、IPv6 がインターネットでペイロードを転送できるようにします。

DMVPN 用の IPv6 トランスポート機能はデフォルトでイネーブルにされます。DMVPN 用の IPv6 トランスポート機能を機能させるために、プライベート内部ネットワークを IPv6 にアップグレードする必要はありません。ローカル ネットワークで IPv4 または IPv6 のいずれかのアドレスを使用できます。

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

DMVPN 経由の IPv6 の前提条件

- IPv6 用の DMVPN が機能するには、ボーダー ゲートウェイ プロトコル（BGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、オンデマンド ルーティング（ODR）、Open Shortest Path First（OSPF）、およびルーティング情報プロトコル（RIP）のいずれかのプロトコルがイネーブルになっている必要があります。
- すべての IPv6 NHRP インターフェイスに、1 つの IPv6 ユニキャスト アドレスを設定します。このアドレスは、グローバルに到達可能なアドレスか、または一意のローカル アドレスにすることができます。
- すべての IPv6 NHRP インターフェイスに、DMVPN クラウド内のすべての DMVPN ホスト（つまり、ハブおよびスポーク）で一意である 1 つの IPv6 リンクローカル アドレスを設定します。

DMVPN 経由の IPv6 について

DMVPN for IPv6 の概要

DMVPN 機能は、NHRP ルーティング、マルチポイント総称ルーティング カプセル化（mGRE）トンネル、IPsec 暗号化を組み合わせて、ユーザが暗号プロファイル（スタティック クリプトマップを定義するための要件を上書きします）とトンネルエンドポイントのダイナミック ディスカバリを使用して容易に設定できるようにします。

この機能は、シスコが開発した次の拡張標準テクノロジーがベースになっています。

- NHRP：クライアント/サーバ プロトコル（ハブがサーバで、スポークはクライアント）。ハブには、各スポークのパブリック インターフェイス アドレスが格納された NHRP データベースが保持されます。各スポークでは、起動時にそれぞれの実際のアドレスが登録され、ダイレクト トンネルを確立する場合には、NHRP サーバに対し、宛先スポークの実際のアドレスに関する照会が行われます。

- mGRE トンネル インターフェイス：1 つの GRE インターフェイスで複数の IPsec トンネルをサポートできるため、設定のデータ量が少なくなり、設定操作も簡単になります。
- IPsec 暗号化：IPsec トンネル インターフェイスは、ネイティブ カプセル化によってサイト間 IPv6 トラフィックの保護を容易にします。

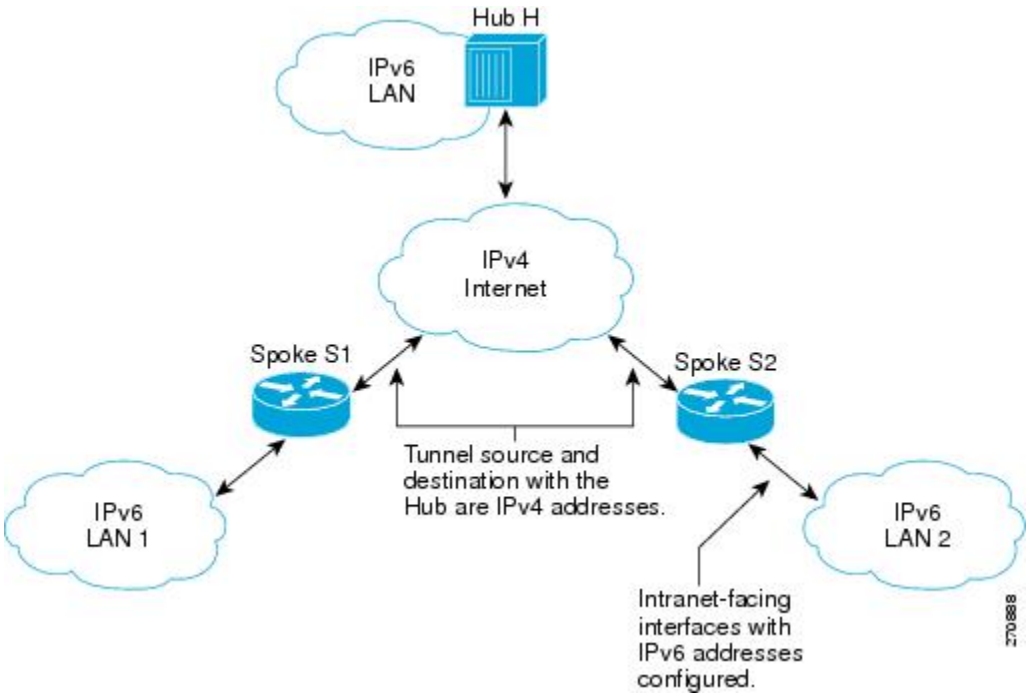
DMVPN for IPv6 では、パブリック ネットワーク（インターネット）は純粋な IPv4 ネットワークであり、プライベート ネットワーク（イントラネット）は IPv6 に対応しています。イントラネットには、DMVPN テクノロジーを使用して相互に接続された IPv4 クラウドまたは IPv6 クラウドを混在させて、基礎となるキャリアを従来の IPv4 ネットワークにすることができます。

NHRP ルーティング

NHRP プロトコルは、特定のイントラネット アドレス（IPv4 または IPv6）をインターネット アドレス（IPv4 非ブロードキャスト マルチアクセス（NBMA）アドレス）に解決します。

下の図で、DMVPN ネットワークを介して接続されているイントラネットは IPv6 クラウド、インターネットは純粋な IPv4 クラウドです。スポーク S1 および S2 は、スタティックに設定されたトンネルを使用してインターネット経由でハブ H に接続されています。トンネルはイントラネット上の別のノードであるため、トンネル自体のアドレスは IPv6 ドメインです。ただし、トンネル（mGRE エンドポイント）の送信元アドレスと宛先アドレスは、常にインターネット ドメイン内の IPv4 にあります。mGRE トンネルは、IPv6 ネットワークを認識します。これは、GRE パッセンジャ プロトコルが IPv6 パケットであり、GRE トランスポート（またはキャリア）プロトコルが IPv4 パケットであるからです。

図 *1*：*NHRP* をトリガーする *IPv6* トポロジ



LAN L1 内の IPv6 ホストが LAN L2 内の IPv6 ホスト宛てのパケットを送信すると、パケットはまず LAN L1 内のゲートウェイ（スポーク S1）にルーティングされます。スポーク S1 はデュアル スタック デバイスです。つまり、IPv4 と IPv6 の両方がこのスポーク上で設定されています。S1 の IPv6 ルーティング テーブルは、スポーク S2 上のトンネルの IPv6 アドレスであるネクスト ホップを指します。これは、NBMA アドレスにマッピングする必要がある VPN アドレスであり、NHRP をトリガーします。

IPv6 NHRP リダイレクトおよびショートカット機能

IPv6 NHRP リダイレクトがイネーブルになっている場合、NHRP は出力機能パス内のすべてのデータ パケットを調べます。データ パケットが同じ論理ネットワーク上で出入りする場合、NHRP は、NHRP トラフィック指示メッセージをデータ パケットの送信元に送信します。NHRP では、論理ネットワークは、複数の物理インターフェイスを 1 つの論理ネットワークにグループ化する NHRP ネットワーク ID によって識別されます。

IPv6 NHRP ショートカットがイネーブルになっている場合、NHRP は出力機能パス内のすべてのデータ パケットを代行受信します。データ パケットの宛先への NHRP キャッシュ エントリがあるかどうかをチェックし、ある場合は、現在の出力隣接を NHRP キャッシュ内の隣接に置き換えます。そのため、データ パケットは、NHRP によって提供された新しい隣接を使用してスイッチングされます。

IPv6 ルーティング

NHRP は、IPv6 パッセンジャ プロトコルを伝送する mGRE トンネルでは自動的に呼び出されます。パケットをルーティングしてスイッチング パスに送信すると、NHRP は特定のネクスト ホップを検索して、必要に応じて NHRP 解決クエリーを開始します。解決に成功した場合、NHRP はトンネル エンドポイント データベースにデータを入力します。これにより、シスコ エクスプレス フォワーディングの隣接関係テーブルにデータが入力されます。シスコエクスプレス フォワーディングがイネーブルになっている場合、後続のパケットについては、シスコエクスプレス フォワーディング スイッチングが行われます。

IPv6 アドレッシングと制約事項

IPv6 では、特定の IPv6 インターフェイス上で複数のユニキャスト アドレスを使用できます。また、エニーキャスト、マルチキャスト、リンクローカルアドレス、ユニキャストアドレスなどの特殊なアドレス タイプも使用できます。

DMVPN for IPv6 には、アドレッシングについて次の制約事項があります。

- すべての IPv6 NHRP インターフェイスに、1 つの IPv6 ユニキャスト アドレスを設定します。このアドレスは、グローバルに到達可能なアドレスか、または一意のローカルアドレスにすることができます。
- すべての IPv6 NHRP インターフェイスに、DMVPN クラウド内のすべての DMVPN ホスト（つまり、ハブおよびスポーク）で一意である 1 つの IPv6 リンクローカル アドレスを設定します。

- デバイス上に同じトンネル送信元を使用する他のトンネルがない場合は、トンネル送信元アドレスを IPv6 アドレスに埋め込むことができます。
- デバイスに DMVPN IPv6 トンネルが 1 つしかない場合は、IPv6 リンクローカル アドレスを手動で設定する必要はありません。代わりに、**ipv6enable** コマンドを使用してリンクローカル アドレスを自動生成します。
- デバイスに複数の DMVPN IPv6 トンネルがある場合は、**ipv6addressfe80::2001link-local** コマンドを使用してリンクローカル アドレスを手動で設定する必要があります。

DMVPN 経由の IPv6 の設定方法

DMVPN for IPv6 の IPsec プロファイルの設定

（注） セキュリティに対する脅威とそれに対抗するための暗号化技術は絶えず変化しています。暗号化に関するシスコの最新の推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IPsecプロファイルには、クリプトマップの設定に使用するほとんどのコマンドが使用されます。ただし、それらすべてのコマンドが、各 IPsec プロファイルで有効であるわけではありません。IPsec プロファイルの下で発行できるのは、IPsec ポリシーに使用されているコマンドだけです。したがって、IPsec ピア アドレスや、パケットを暗号化するかどうかを照合するためのアクセス コントロール リスト（ACL）は指定できません。

はじめる前に

IPsec プロファイルを設定する前に、次の作業を実行する必要があります。

- **cryptoipsectransform-set** コマンドを使用して、トランスフォーム セットを定義します。
- Internet Security Association Key Management Protocol（ISAKMP）プロファイルがデフォルトの ISAKMP 設定を使用して設定されていることを確認します。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoidentity***name*
4. **exit**
5. **cryptoipsecprofile***name*
6. **settransform-set***transform-set-name*
7. **setidentity**
8. **setsecurity-associationlifetimeseconds***seconds* | **kilobytes***kilobytes*
9. **setpfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
10. end

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cryptoidentity***name* 例： `Device(config)# crypto identity device1`	デバイスの証明書内にある識別名（DN）リストを使用してデバイスのアイデンティティを設定します。
ステップ 4	**exit** 例： `Device(config-crypto-identity)# exit`	クリプト ID コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**cryptoipsecprofile***name* 例： `Device(config)# crypto ipsec profile example1`	「スポークとハブ」および「スポークとスポーク」ルータ間での IPsec 暗号化に使用する IPsec パラメータを定義します。 このコマンドによって、デバイスはクリプト マップ コンフィギュレーション モードになります。

	コマンドまたはアクション	目的
ステップ 6	**settransform-set***transform-set-name* 例： `Device(config-crypto-map)# set transform-set example-set`	IPsec プロファイルで使用できるトランスフォーム セットを指定します。
ステップ 7	**setidentity** 例： `Device(config-crypto-map)# set identity router1`	（任意）IPsec プロファイルに対するアイデンティティの制限事項を指定します。
ステップ 8	**setsecurity-associationlifetimeseconds***seconds* | **kilobytes***kilobytes* 例： `Device(config-crypto-map)# set security-association lifetime seconds 1800`	（任意）IPsec プロファイルに使用するグローバル ライフタイムの値を上書きします。
ステップ 9	**setpfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**] 例： `Device(config-crypto-map)# set pfs group14`	（任意）IPsecにおいて、このIPsecプロファイルに対する新しいセキュリティアソシエーションが要求される際に、完全転送秘密（PFS）が必須となるよう指定します。このコマンドを指定しない場合は、デフォルトのDiffie-Hellman（DH）グループ（**group1**）が有効になります。 • **1**：768 ビット DH（非推奨）。 • **2**：1024 ビット DH（非推奨）。 • **5**：1536 ビット DH（非推奨）。 • **14**：2048 ビット DH グループを指定します。 • **15**：3072 ビット DH グループを指定します。 • **16**：4096 ビット DH グループを指定します。 • **19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 • **20**：384 ビット ECDH グループを指定します。 • **24**：2048 ビット DH/DSA グループを指定します。

	コマンドまたはアクション	目的
ステップ 10	end 例： `Device(config-crypto-map)# end`	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN 経由の IPv6 用のハブの設定

DMVPN 経由の IPv6 用にハブ デバイスを設定して mGRE と IPsec を統合する（つまり、前述の手順で設定した IPsec プロファイルとトンネルを関連付ける）には、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length*
5. **ipv6address***ipv6-address*/*prefix-length***link-local**
6. **ipv6mtu***bytes*
7. **ipv6nhrpauthentication***string*
8. **ipv6nhrpmapmulticastdynamic**
9. **ipv6nhrpnetwork-id***network-id*
10. **tunnelsource***ip-address* | *ipv6-address* | *interface-typeinterface-number*
11. **tunnelmode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gremultipoint**[**ipv6**] | **greipv6** | **ipipdecapsulate-any**] | **ipsecipv4** | **iptalk** | **ipv6**| **ipsecipv6** | **mpls** | **nos** | **rbscp**
12. 次のいずれかを実行します。
    - **tunnelprotectionipsecprofile***name* [**shared**]
    - **tunnelprotectionpsk***key*
13. **bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]}
14. **ipv6nhrpholdtime***seconds*
15. end

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacetunnel***number* 例： `Device(config)# interface tunnel 5`	トンネル インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • number 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。
ステップ 4	**ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1:1::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**ipv6address***ipv6-address*/*prefix-length***link-local** 例： `Device(config-if)# ipv6 address fe80::2001 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。 • （DMVPN ネットワーク内のすべての DMVPN ノードで）一意の IPv6 リンクローカル アドレスを設定する必要があります。
ステップ 6	**ipv6mtu***bytes* 例： `Device(config-if)# ipv6 mtu 1400`	各インターフェイスにおいて送信される IPv6 パケットの最大伝送単位（MTU）サイズを設定します。
ステップ 7	**ipv6nhrpauthentication***string* 例： `Device(config-if)# ipv6 nhrp authentication examplexx`	NHRP を使用するインターフェイス用の認証文字列を設定します。 （注） 同一の DMVPN ネットワーク内に存在するハブおよびスポークに対しては、すべて同じ NHRP 認証文字列を設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**ipv6nhrpmapmulticastdynamic** 例： `Device(config-if)# ipv6 nhrp map multicast dynamic`	NHRP において、ルータが自動的にマルチキャスト NHRP マッピングへ追加されるようにします。 （注） Cisco IOS XE Denali 16.3 では、**ipv6nhrpmapmulticastdynamic** がデフォルトでイネーブルになっています。
ステップ 9	**ipv6nhrpnetwork-id***network-id* 例： `Device(config-if)# ipv6 nhrp network-id 99`	インターフェイスに対して NHRP をイネーブルにします。 Cisco IOS XE Denali 16.3 では、**ipv6nhrpnetwork-id** がデフォルトでイネーブルになっています。
ステップ 10	**tunnelsource***ip-address* | *ipv6-address* | *interface-typeinterface-number* 例： `Device(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 11	**tunnelmode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gremultipoint**[**ipv6**] | **greipv6** | **ipipdecapsulate-any**] | **ipsecipv4** | **iptalk** | **ipv6**| **ipsecipv6** | **mpls** | **nos** | **rbscp** 例： `Device(config-if)# tunnel mode gre multipoint`	トンネル インターフェイスのカプセル化モードを mGRE に設定します。

ステップ 12	次のいずれかを実行します。
	
	• **tunnelprotectionipsecprofile***name* [**shared**]
	• **tunnelprotectionpsk***key*
	
	例：
	`Router(config-if)# tunnel protection ipsec profile vpnprof`
	
	例：
	`Router(config-if)# tunnel protection psk test1`
		トンネル インターフェイスを IPsec プロファイルに関連付けます。
		
		• *name* 引数には、IPsec プロファイルの名前を指定します。この値は、**cryptoipsecprofile***name* コマンドで指定した *name* と一致する必要があります。
		
		または
		
		デフォルトの IPsec プロファイルを作成して、事前共有キー（PSK）用のトンネル保護設定を簡略化します。

	コマンドまたはアクション	目的
ステップ 13	**bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]} 例： `Device(config-if)# bandwidth 1200`	上位レベルプロトコルのインターフェイスに対する現在の帯域幅を設定します。 • *bandwidth-size* 引数には、キロビット/秒単位の帯域幅を指定します。デフォルト値は 9 です。帯域幅の推奨値は 1000 以上です。
ステップ 14	**ipv6nhrpholdtime***seconds* 例： `Device(config-if)# ipv6 nhrp holdtime 3600`	信頼できる NHRP 応答により NHRP NBMA アドレスが有効としてアドバタイズされる秒数を変更します。
ステップ 15	end 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ハブでの NHRP リダイレクトおよびショートカット機能の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnelnumber**
4. **ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length*
5. 次のいずれかを実行します。
   - **ipv6nhrpredirect** [**timeout***seconds*]
   - **ipv6nhrpredirect** [**interest***acl*]
6. **ipv6nhrpshortcut**
7. end

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacetunnelnumber** 例： `Device(config)# interface tunnel 5`	トンネル インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • number 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。
ステップ 4	**ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1:1::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

ステップ 5	次のいずれかを実行します。
	• **ipv6nhrpredirect** [**timeout***seconds*]
	• **ipv6nhrpredirect** [**interest***acl*]
	例：
	`Device(config-if)# ipv6 nhrp redirect`
	例：
	`Device(config-if)# ipv6 nhrp redirect interest`
		NHRP リダイレクトをイネーブルにします。
		または
		ユーザが ACL を指定できるようにします。
		（注） ハブで **ipv6nhrpredirect** コマンドを設定する必要があります。

ステップ 6	**ipv6nhrpshortcut** 例： `Device(config-if)# ipv6 nhrp shortcut`	NHRP ショートカット スイッチングをイネーブルにします。 • スポークで **ipv6nhrpshortcut** コマンドを設定する必要があります。

	コマンドまたはアクション	目的
		（注） Cisco IOS XE Denali 16.3 では、**ipv6nhrpshortcut** がデフォルトでイネーブルになっています。
ステップ 7	end 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN 経由の IPv6 用のスポークの設定

DMVPN を介した IPv6 用のスポークを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length*
5. **ipv6address***ipv6-address*/*prefix-length***link-local**
6. **ipv6mtu***bytes*
7. **ipv6nhrpauthentication***string*
8. **ipv6nhrpmap***ipv6-addressnbma-address*
9. **ipv6nhrpmapmulticast***ipv4-nbma-address*
10. **ipv6nhrpnhs***ipv6-nhs-address*
11. **ipv6nhrpnetwork-id***network-id*
12. **tunnelsource***ip-address* | *ipv6-address* | *interface-typeinterface-number*
13. 次のいずれかを実行します。
    - **tunnelmode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gremultipoint** [**ipv6**] | **greipv6** | **ipipdecapsulate-any**] | **ipsecipv4** | **iptalk** | **ipv6**| **ipsecipv6** | **mpls** | **nos** | **rbscp**
    - **tunneldestination** {*host-name* | *ip-address* | *ipv6-address*}
14. 次のいずれかを実行します。
    - **tunnelprotectionipsecprofile***name* [**shared**]
    - **tunnelprotectionpsk***key*
15. **bandwidth** {**interzone** | **total** | **session**} {**default** | **zone***zone-name*} *bandwidth-size*
16. **ipv6nhrpholdtime***seconds*
17. end

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interfacetunnel***number* 例： `Device(config)# interface tunnel 5`	トンネル インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • *number* 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。
ステップ 4	**ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length* 例： `Device(config-if) ipv6 address 2001:DB8:1:1::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**ipv6address***ipv6-address*/*prefix-length***link-local** 例： `Device(config-if)# ipv6 address fe80::2001 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。 • （DMVPN ネットワーク内のすべての DMVPN ノードで）一意の IPv6 リンクローカル アドレスを設定する必要があります。
ステップ 6	**ipv6mtu***bytes* 例： `Device(config-if)# ipv6 mtu 1400`	インターフェイス上で送信する IPv6 パケットの MTU サイズを設定します。
ステップ 7	**ipv6nhrpauthentication***string* 例： `Device(config-if)# ipv6 nhrp authentication examplexx`	NHRP を使用するインターフェイス用の認証文字列を設定します。 （注） 同一の DMVPN ネットワーク内に存在するハブおよびスポークに対しては、すべて同じ NHRP 認証文字列を設定する必要があります。
ステップ 8	**ipv6nhrpmap***ipv6-addressnbma-address* 例： `Device(config-if)# ipv6 nhrp map 2001:DB8:3333:4::5 10.1.1.1`	NBMA ネットワークに接続された IPv6 宛先の IPv6 アドレスと NBMA アドレスのマッピングをスタティックに設定します。 （注） IPv4 NBMA アドレスだけがサポートされ、ATM またはイーサネット アドレスはサポートされません。

	コマンドまたはアクション	目的
ステップ 9	**ipv6nhrpmapmulticast***ipv4-nbma-address* 例： `Device(config-if)# ipv6 nhrp map multicast 10.11.11.99`	宛先 IPv6 アドレスを IPv4 NBMA アドレスにマッピングします。
ステップ 10	**ipv6nhrpnhs***ipv6-nhs-address* 例： `Device(config-if)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 2001:0DB8::/64`	1 つ以上の IPv6 NHRP サーバのアドレスを指定します。
ステップ 11	**ipv6nhrpnetwork-id***network-id* 例： `Device(config-if)# ipv6 nhrp network-id 99`	インターフェイスに対して NHRP をイネーブルにします。 （注） Cisco IOS XE Denali 16.3 では、**ipv6nhrpnetwork-id** がデフォルトでイネーブルになっています。
ステップ 12	**tunnelsource***ip-address* | *ipv6-address* | *interface-typeinterface-number* 例： `Device(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元アドレスを設定します。

ステップ 13	次のいずれかを実行します。
	
	• **tunnelmode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gremultipoint** [**ipv6**] | **greipv6** | **ipipdecapsulate-any**] | **ipsecipv4** | **iptalk** | **ipv6**| **ipsecipv6** | **mpls** | **nos** | **rbscp**
	
	• **tunneldestination** {*host-name* | *ip-address* | *ipv6-address*}
	
	例：
	
	`Device(config-if)# tunnel mode gre multipoint`
	
	例：
	
	`Device(config-if)# tunnel destination 10.1.1.1`
		トンネル インターフェイスのカプセル化モードを mGRE に設定します。
		
		• **tunnelmode** コマンドを使用するのは、データ トラフィックにダイナミック スポークツースポーク トラフィックを使用できる場合です。
		
		または
		
		トンネル インターフェイスの宛先を指定します。
		
		• **tunneldestination** コマンドを使用するのは、データ トラフィックにハブアンドスポーク トンネルを使用できる場合です。

	コマンドまたはアクション	目的

ステップ 14	次のいずれかを実行します。
	• **tunnelprotectionipsecprofile***name* [**shared**]
	• **tunnelprotectionpsk***key*
	例：
	`Router(config-if)# tunnel protection ipsec profile vpnprof`
	例：
	`Router(config-if)# tunnel protection psk test1`
		トンネルインターフェイスを IPsec プロファイルに関連付けます。
		• *name* 引数には、IPsec プロファイルの名前を指定します。この値は、**cryptoipsecprofile***name* コマンドで指定した *name* と一致する必要があります。
		または
		デフォルトの IPsec プロファイルを作成して、事前共有キー（PSK）用のトンネル保護設定を簡略化します。

ステップ 15	**bandwidth** {**interzone** | **total** | **session**} {**default** | **zone***zone-name*} *bandwidth-size* 例： `Device(config-if)# bandwidth total 1200`	上位レベル プロトコルのインターフェイスに対する現在の帯域幅を設定します。 • *bandwidth-size* 引数には、キロビット/秒単位の帯域幅を指定します。デフォルト値は 9 です。帯域幅の推奨値は 1000 以上です。 • スポークの帯域幅設定は、DMVPN ハブの帯域幅設定と同じである必要はありません。通常は、すべてのスポークに対して、同一または類似の帯域幅を使用する方が便利です。
ステップ 16	**ipv6nhrpholdtime***seconds* 例： `Device(config-if)# ipv6 nhrp holdtime 3600`	信頼できる NHRP 応答により NHRP NBMA アドレスが有効としてアドバタイズされる秒数を変更します。
ステップ 17	end 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN for IPv6 設定の確認

手順の概要

1. **enable**
2. **showdmvpn** [**ipv4** [**vrf***vrf-name*] | **ipv6** [**vrf***vrf-name*]] [**debug-condition** | [**interfacetunnel***number* | **peer** {**nbma***ip-address* | **network***network-mask* | **tunnel***ip-address*}] [**static**] [**detail**]]
3. **showipv6nhrp** [**dynamic** [*ipv6-address*] | **incomplete** | **static**] [*address* | *interface*] [**brief** | **detail**] [**purge**]
4. **showipv6nhrpmulticast**[*ipv4-address* | *interface* | *ipv6-address*]
5. **showipnhrpmulticast** [*nbma-address* | *interface*]
6. **showipv6nhrpsummary**
7. **showipv6nhrptraffic** [*interface***tunnel***number*
8. **showipnhrpshortcut**
9. **showiproute**
10. **showipv6route**
11. **shownhrpdebug-condition**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showdmvpn** [**ipv4** [**vrf***vrf-name*]	**ipv6** [**vrf***vrf-name*]] [**debug-condition**	[**interfacetunnel***number*	**peer** {**nbma***ip-address*	**network***network-mask*	**tunnel***ip-address*}] [**static**] [**detail**]] 例： `Device# show dmvpn 2001:0db8:1:1::72/64`	DMVPN 固有のセッション情報を表示します。
ステップ 3	**showipv6nhrp** [**dynamic** [*ipv6-address*]	**incomplete**	**static**] [*address*	*interface*] [**brief**	**detail**] [**purge**] 例： `Device# show ipv6 nhrp`	NHRP マッピング情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**showipv6nhrpmulticast**[*ipv4-address* | *interface* | *ipv6-address*] 例： `Device# show ipv6 nhrp multicast`	NHRP マルチキャスト マッピング情報を表示します。
ステップ 5	**showipnhrpmulticast** [*nbma-address* | *interface*] 例： `Device# show ip nhrp multicast`	NHRP マルチキャスト マッピング情報を表示します。
ステップ 6	**showipv6nhrpsummary** 例： `Device# show ipv6 nhrp summary`	NHRP マッピング サマリー情報を表示します。
ステップ 7	**showipv6nhrptraffic** [*interface***tunnel***number* 例： `Device# show ipv6 nhrp traffic`	NHRP トラフィック統計情報を表示します。
ステップ 8	**showipnhrpshortcut** 例： `Device# show ip nhrp shortcut`	NHRP ショートカット情報を表示します。
ステップ 9	**showiproute** 例： `Device# show ip route`	IPv4 ルーティング テーブルの現在の状態を表示します。
ステップ 10	**showipv6route** 例： `Device# show ipv6 route`	IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 11	**shownhrpdebug-condition** 例： `Device# show nhrp debug-condition`	NHRP 条件付きデバッグ情報を表示します。

DMVPN for IPv6 の設定と動作のモニタリングおよび維持

手順の概要

1. **enable**
2. **cleardmvpnsession** [**interfacetunnel***number* | **peer** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **vrf***vrf-name*] [**static**]
3. **clearipv6nhrp** [*ipv6-address* | **counters**
4. **debugdmvpn** {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*}
5. **debugnhrp** [**cache** | **extension** | **packet** | **rate**]
6. **debugnhrpcondition**[**interfacetunnel***number* | **peer** {**nbma** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf***vrf-name*]
7. **debugnhrperror**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**cleardmvpnsession** [**interfacetunnel***number*	**peer** {*ipv4-address*	*fqdn-string*	*ipv6-address*}	**vrf***vrf-name*] [**static**] 例： `Device# clear dmvpn session`	DMVPN セッションをクリアします。
ステップ 3	**clearipv6nhrp** [*ipv6-address*	**counters** 例： `Device# clear ipv6 nhrp`	NHRP キャッシュからすべてのダイナミックエントリを削除します。
ステップ 4	**debugdmvpn** {**all**	**error**	**detail**	**packet**} {**all**	*debug-type*} 例： `Device# debug dmvpn`	デバッグの DMVPN セッション情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	**debugnhrp** [**cache** | **extension** | **packet** | **rate**] 例： `Device# debug nhrp ipv6`	NHRP デバッグをイネーブルにします。
ステップ 6	**debugnhrpcondition**[**interfacetunnel***number* | **peer** {**nbma** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf***vrf-name*] 例： `Device# debug nhrp condition`	NHRP 条件付きデバッグをイネーブルにします。
ステップ 7	**debugnhrperror** 例： `Device# debug nhrp ipv6 error`	NHRP エラー レベル デバッグ情報を表示します。

例

debug nhrp コマンドの出力例

次に、**ipv6** キーワードを指定した **debugnhrp** コマンドの出力例を示します。

```
Device# debug nhrp ipv6
Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST
   - 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.
Aug  9 13:13:41.486: NHRP: Tunnel NBMA addr 11.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486: src: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32,
          dst: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
```

DMVPN 経由の IPv6 の設定例

例：IPsec プロファイルの設定

```
Device(config)# crypto identity router1
Device(config)# crypto ipsec profile example1
```

```
Device(config-crypto-map)# set transform-set example-set
Device(config-crypto-map)# set identity router1

Device(config-crypto-map)# set security-association lifetime seconds 1800

Device(config-crypto-map)# set pfs group14
```

例：DMVPN 用のハブの設定

```
Device# configure terminal
Device(config)# interface tunnel 5

Device(config-if)# ipv6 address 2001:DB8:1:1::72/64
Device(config-if)# ipv6 address fe80::2001 link-local
Device(config-if)# ipv6 mtu 1400
Device(config-if)# ipv6 nhrp authentication examplexx
Device(config-if)# ipv6 nhrp map multicast dynamic
Device(config-if)# ipv6 nhrp network-id 99
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode gre multipoint
Device(config-if)# tunnel protection ipsec profile example_profile
Device(config-if)# bandwidth 1200
Device(config-if)# ipv6 nhrp holdtime 3600
```

次に、ハブで **ipv6** および **detail** キーワードを指定した **show dmvpn** コマンドの出力例を示します。

```
Device# show dmvpn ipv6 detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.3, VRF ""
   Tunnel Src./Dest. addr: 192.169.2.9/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "test_profile"
Type:Hub, Total NBMA Peers (v4/v6): 2
    1.Peer NBMA Address: 192.169.2.10
        Tunnel IPv6 Address: 2001::4
        IPv6 Target Network: 2001::4/128
        # Ent: 2, Status: UP, UpDn Time: 00:01:51, Cache Attrib: D
Type:Hub, Total NBMA Peers (v4/v6): 2
    2.Peer NBMA Address: 192.169.2.10
        Tunnel IPv6 Address: 2001::4
        IPv6 Target Network: FE80::2/128
        # Ent: 0, Status: UP, UpDn Time: 00:01:51, Cache Attrib: D
Type:Hub, Total NBMA Peers (v4/v6): 2
    3.Peer NBMA Address: 192.169.2.11
Tunnel IPv6 Address: 2001::5
        IPv6 Target Network: 2001::5/128
        # Ent: 2, Status: UP, UpDn Time: 00:26:38, Cache Attrib: D
Type:Hub, Total NBMA Peers (v4/v6): 2
    4.Peer NBMA Address: 192.169.2.11
        Tunnel IPv6 Address: 2001::5
        IPv6 Target Network: FE80::3/128
        # Ent: 0, Status: UP, UpDn Time: 00:26:38, Cache Attrib: D
Pending DMVPN Sessions:

Interface: Tunnel1
  IKE SA: local 192.169.2.9/500 remote 192.169.2.10/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.169.2.10
  IPSEC FLOW: permit 47 host 192.169.2.9 host 192.169.2.10
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x BB0ED02, transform : esp-aes esp-sha-hmac
```

```
    Socket State: Open

Interface: Tunnel1
  IKE SA: local 192.169.2.9/500 remote 192.169.2.11/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.169.2.11
  IPSEC FLOW: permit 47 host 192.169.2.9 host 192.169.2.11
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xB79B277B, transform : esp-aes esp-sha-hmac
    Socket State: Open
```

例：DMVPN 用のスポークの設定

```
Device# configure terminal
Device(config)# crypto ikev2 keyring DMVPN
Device(config)# peer DMVPN
Device(config)# address 0.0.0.0 0.0.0.0
Device(config)# pre-shared-key cisco123
Device(config)# peer DMVPNv6
Device(config)# address ::/0
Device(config)# pre-shared-key cisco123v6
Device(config)# crypto ikev2 profile DMVPN
Device(config)# match identity remote address 0.0.0.0
Device(config)# match identity remote address ::/0
Device(config)# authentication local pre-share
Device(config)# authentication remote pre-share
Device(config)# keyring DMVPN
Device(config)# dpd 30 5 on-demand
Device(config)# crypto ipsec transform-set DMVPN esp-aes esp-sha-hmac
Device(config)# mode transport
Device(config)# crypto ipsec profile DMVPN
Device(config)# set transform-set DMVPN
Device(config)# set ikev2-profile DMVPN
Device(config)# interface tunnel 5

Device(config-if)# bandwidth 1000
Device(config-if)# ip address 10.0.0.11 255.255.255.0
Device(config-if)# ip mtu 1400
Device(config-if)# ip nhrp authentication test
Device(config-if)# ip nhrp network-id 100000
Device(config-if)# ip nhrp nhs 10.0.0.1 nbma 2001:DB8:0:FFFF:1::1 multicast
Device(config-if)# vip nhrp shortcut
Device(config-if)# delay 1000
Device(config-if)# ipv6 address 2001:DB8:0:100::B/64
Device(config-if)# ipv6 mtu 1400
Device(config-if)# ipv6 nd ra mtu suppress
Device(config-if)# no ipv6 redirects
Device(config-if)# ipv6 eigrp 1
Device(config-if)# ipv6 nhrp authentication testv6
Device(config-if)# ipv6 nhrp network-id 100006
Device(config-if)# ipv6 nhrp nhs 2001:DB8:0:100::1 nbma 2001:DB8:0:FFFF:1::1 multicast
Device(config-if)# ipv6 nhrp shortcut
Device(config-if)# tunnel source Ethernet0/0
Device(config-if)# tunnel mode gre multipoint ipv6
Device(config-if)# tunnel key 100000
Device(config-if)# end
.
.
```

次に、スポークで **ipv6** および **detail** キーワードを指定した **show dmvpn** コマンドの出力例を示します。

```
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
```

```
==============================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.1, VRF ""
   Tunnel Src./Dest. addr: 192.169.2.10/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "test_profile"

IPv6 NHS: 2001::6 RE
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 192.169.2.9
        Tunnel IPv6 Address: 2001::6
        IPv6 Target Network: 2001::/112
        # Ent: 2, Status: NHRP, UpDn Time: never, Cache Attrib: S

IPv6 NHS: 2001::6 RE
Type:Unknown, Total NBMA Peers (v4/v6): 1
    2.Peer NBMA Address: 192.169.2.9
        Tunnel IPv6 Address: FE80::1
        IPv6 Target Network: FE80::1/128
        # Ent: 0, Status: UP, UpDn Time: 00:00:24, Cache Attrib: D

Pending DMVPN Sessions:

Interface: Tunnel1
  IKE SA: local 192.169.2.10/500 remote 192.169.2.9/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.169.2.9
  IPSEC FLOW: permit 47 host 192.169.2.10 host 192.169.2.9
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x6F75C431, transform : esp-aes esp-sha-hmac
    Socket State: Open
```

例：ハブでの NHRP リダイレクトおよびショートカット機能の設定

```
Device(config)# interface tunnel 5
Device(config-if)# ipv6 address 2001:DB8:1:1::72/64

Device(config-if)# ipv6 nhrp redirect

Device(config-if)# ipv6 nhrp shortcut
```

例：ハブとスポークでの NHRP の設定

ハブ

```
Device# show ipv6 nhrp

2001::4/128 via 2001::4
   Tunnel1 created 00:02:40, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.10
2001::5/128 via 2001::5
   Tunnel1 created 00:02:37, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.11
FE80::2/128 via 2001::4
   Tunnel1 created 00:02:40, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.10
FE80::3/128 via 2001::5
   Tunnel1 created 00:02:37, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.11
```

スポーク

```
Device# show ipv6 nhrp

2001::8/128
   Tunnel1 created 00:00:13, expire 00:02:51
   Type: incomplete, Flags: negative
   Cache hits: 2
2001::/112 via 2001::6
   Tunnel1 created 00:01:16, never expire
   Type: static, Flags: used
   NBMA address: 192.169.2.9
FE80::1/128 via FE80::1
   Tunnel1 created 00:01:15, expire 00:00:43
   Type: dynamic, Flags:
   NBMA address: 192.169.2.9
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
ダイナミック マルチポイント VPN	『*Dynamic Multipoint VPN* コンフィギュレーション ガイド』
Cisco IOS コマンド	『Master Command List, All Releases』
IPv6 コマンド	『*IPv6 Command Reference*』
Cisco IOS IPv6 機能	『IPv6 Feature Mapping』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DMVPN 経由の IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*DMVPN* 経由の *IPv6* の機能情報

機能名	リリース	機能情報
DMVPN 経由の IPv6	Cisco IOS XE Release 3.7S	

機能名	リリース	機能情報
		DMVPN機能を使用すると、総称ルーティング カプセル化（GRE）トンネル、IP Security（IPsec）暗号化、Next Hop Resolution Protocol（NHRP）を組み合わせることにより、目的に合わせて大小さまざまな規模の IPsec バーチャル プライベート ネットワーク（VPN）を構築できます。Dynamic Multipoint Virtual Private Network（DMVPN）for IPv6 では、パブリック ネットワーク（インターネット）は純粋な IPv4 ネットワークであり、プライベート ネットワーク（イントラネット）は IPv6 に対応しています。 次のコマンドが導入または変更されました。**clear dmvpn session**、**clear ipv6 nhrp**、**crypto ipsec profile**、**debug dmvpn**、**debug dmvpn condition**、**debug nhrp condition**、**debug nhrp error**、**ipv6 nhrp authentication**、**ipv6 nhrp holdtime**、**ipv6 nhrp interest**、**ipv6 nhrp map**、**ipv6 nhrp map multicast**、**ipv6 nhrp map multicast dynamic**、**ipv6 nhrp max-send**、**ipv6 nhrp network-id**、**ipv6 nhrp nhs**、**ipv6 nhrp record**、**ipv6 nhrp redirect**、**ipv6 nhrp registration**、**ipv6 nhrp responder**、**ipv6 nhrp server-only**、**ipv6 nhrp shortcut**、**ipv6 nhrp trigger-svc**、**ipv6 nhrp use**、**set pfs**、**set security-association lifetime**、**set transform-set**、**show dmvpn**、**show ipv6 nhrp**、**show ipv6 nhrp**

機能名	リリース	機能情報
		multicast、**show ipv6 nhrp nhs**、**show ipv6 nhrp summary**、**show ipv6 nhrp traffic**
DMVPN 用の IPv6 トランスポート	Cisco IOS XE Release 3.8S	DMVPN 用の IPv6 トランスポート機能は、IPv6 WAN 側の機能を NHRP トンネルと基礎となる IPsec 暗号化に構築して、IPv6 がインターネットでペイロードを転送できるようにします。 DMVPN 用の IPv6 トランスポート機能はデフォルトでイネーブルにされます。