Dynamic Multipoint VPN コンフィギュレーション ガイド

初版：2011 年 10 月 14 日

最終更新：2014 年 01 月 10 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

強力な Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースは、コンバージド リリース バージョンとして Cisco IOS XE 16 にマージされました。Cisco IOS XE 16 は、スイッチングおよびルーティング ポートフォリオの幅広いアクセス範囲とエッジ製品を網羅する単一のリリースとなります。

（注） 技術構成ガイドの機能情報テーブルには、いつ機能が導入されたかが記載されています。他のプラットフォームでその機能がいつサポートされていたかについて、記載されている場合と記載されていない場合があります。お使いのプラットフォームで特定の機能がサポートされているかどうかを確認するには、製品ランディング ページにある技術構成ガイドを参照してください。お使いの製品のランディング ページに技術構成ガイドが表示されている場合、その機能がそのプラットフォームでサポートされていることを示します。

第 2 章

ダイナミック マルチポイント VPN

Dynamic Multipoint VPN 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、および Next Hop Resolution Protocol（NHRP）を組み合わせることにより、目的に合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。

（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。

Dynamic Multipoint VPN の前提条件

- マルチポイント GRE（mGRE）および IPsec トンネルを確立するには、**crypto isakmp policy** コマンドを使用して、インターネット キー交換（IKE）ポリシーを定義しておく必要があります。
- DMVPN 内のトラフィック セグメンテーション機能（2547oDMVPN）を使用するには、**mpls ip** コマンドを使用して、マルチプロトコル ラベル スイッチング（MPLS）を設定する必要があります。

Dynamic Multipoint VPN の制約事項

- この機能の特長であるDynamic Multipoint VPN の制約事項, （4 ページ）を活用するためには、Internet Security Association Key Management Protocol（ISAKMP）認証に対して、IKE 証明書またはワイルドカード事前共有キーを使用する必要があります。

（注） ただし、スポーク ルータが 1 つでもセキュリティを突破されると外部から VPN へ侵入できるため、ワイルドカード事前共有キーは使用しないことを強く推奨します。

- DMVPN ネットワークのポイントツーポイント GRE トンネルまたはマルチポイント GRE トンネルでは、GRE トンネル キープアライブ（GRE インターフェイスでの **keepalive** コマンド）はサポートされていません。
- ネットワーク アドレス変換（NAT）のタイプが共にポート アドレス変換（PAT）である 2 つの NAT デバイスの背後にそれぞれスポークが配置されている場合、その 2 つのスポーク間で開始されるセッションは確立できません。

  次に、NAT インターフェイスにおける PAT の 1 つの設定例を示します。

```
ip nat inside source list nat_acl interface FastEthernet0/0/1 overload
```

Dynamic Multipoint VPN について

Dynamic Multipoint VPN の利点

ハブ ルータ設定の軽減

- ハブ ルータでは、クリプト マップ特性、暗号アクセス リスト、および GRE トンネル インターフェイスを定義するための設定行が、スポーク ルータごとに個別に用意されています。DMVPN 機能を使用すれば、ハブ ルータ上で mGRE トンネル インターフェイスおよび IPsec プロファイルをそれぞれ 1 つずつ設定するだけで、すべてのスポーク ルータに対応できるようになり、暗号アクセス リストを設定する必要もなくなります。そのため、ネットワークに新たなスポーク ルータが追加された場合でも、ハブ ルータにおける設定の情報量は変わりません。
- DMVPN アーキテクチャでは、複数のスポークを 1 つのマルチポイント GRE インターフェイスにまとめることができます。これにより、IPsec のネイティブ インストールで、物理インターフェイスまたは論理インターフェイスをスポークごとに別々に設定する必要はなくなります。

IPsec 暗号化の自動実行

- GRE では、送信元および宛先のピア アドレスは、NHRP により設定または解決されます。これによって、直ちに、またはマルチポイント GRE トンネルに対し GRE のピア アドレスが NHRP を介して解決された時点で、ポイントツーポイント GRE トンネリングに対して IPsec がトリガーされます。

ダイナミックにアドレス指定されるスポーク ルータのサポート

- ポイントツーポイント GRE および IPsec ハブアンドスポークによる VPN ネットワークでは、ハブ ルータを設定する際にスポーク ルータの物理インターフェイス IP アドレスが必要となります。これは、IP アドレスが GRE トンネル宛先アドレスとして設定される必要があるためです。一方、DMVPN 機能を使用すれば、スポーク ルータに対して、ダイナミック物理インターフェイス IP アドレス（通常はケーブル接続や DSL 接続に使用）を設定できます。スポーク ルータは、オンライン状態になると、ハブ ルータへ登録パケットを送信します。これらの登録パケットには、このスポークの現在の物理インターフェイス IP アドレスが記述されています。

スポークツースポーク トンネルのダイナミック作成

- DMVPN 機能を使用すると、ダイレクト トンネルに対するスポークツースポーク設定を行う必要がなくなります。現在、スポーク ルータ間でパケットを送信する必要がある場合は、要求されたターゲット スポーク ルータの宛先アドレスを NHRP を使用してダイナミックに指定できるようになっています（ハブ ルータが NHRP サーバとして動作し、送信元スポーク

ルータの要求を処理します）。2 つのスポーク ルータ間には、データが直接転送されるように、IPsec トンネルがダイナミックに作成されます。

Dynamic Multipoint VPN の機能設計

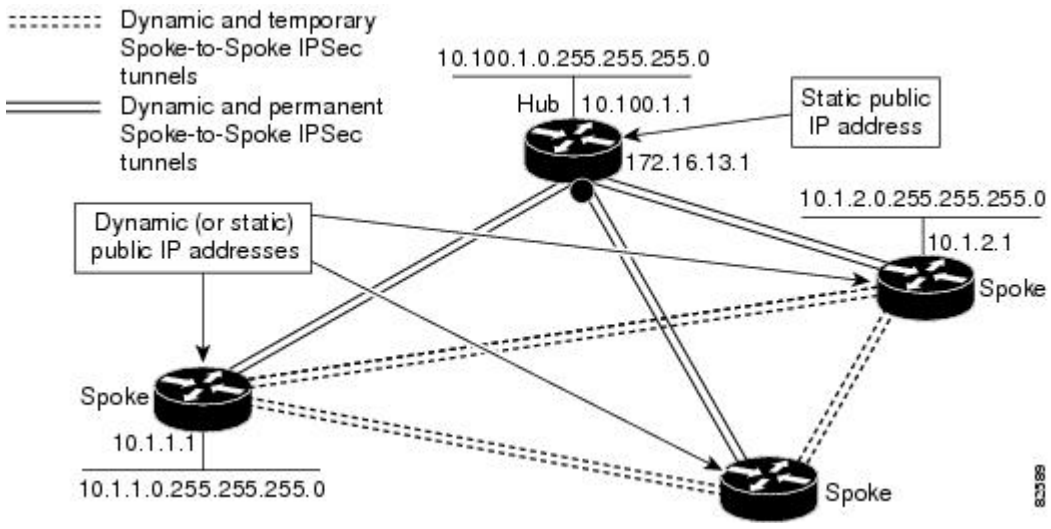
Dynamic Multipoint VPN 機能は、GRE トンネル、IPsec 暗号化、および NHRP ルーティングを組み合わせることで、ユーザの設定操作を容易にするためのものです。設定は、暗号プロファイル、およびトンネルエンドポイントのダイナミックディスカバリを介して行われ、このうち暗号プロファイルを使用することで、スタティック クリプト マップを定義する必要がなくなります。

この機能は、シスコが開発した次の 2 つ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。

次の図に示したトポロジとそれに続く箇条書きは、この機能のしくみを説明したものです。

図 *1*：*mGRE* および *IPsec* の統合トポロジの例



- 各スポークとハブの間は、永続的な IPsec トンネルで接続されています。ネットワーク内に存在するスポーク間を接続するのは、永続的な IPsec トンネルではありません。各スポークは、NHRP サーバのクライアントとして登録されます。

- 各スポークでは、他のスポーク上にある宛先（プライベート）サブネットへパケットを送信する場合、NHRP サーバに対し、宛先（ターゲット）スポークの実際（外部）のアドレスについて照会が行われます。
- 発信側のスポークでは、ターゲット スポークのピア アドレスを「学習」すると、ターゲット スポークへのダイナミック IPsec トンネルを起動できるようになります。
- スポーク間のトンネルは、マルチポイント GRE インターフェイス経由で構築されます。
- スポーク間のリンクは、スポーク間にトラフィックが発生するたびにオンデマンドで確立されます。その後、パケットはハブを迂回し、スポーク間トンネルを使用できます。

（注） スポークツースポーク トンネルに対して不稼働度が事前に設定されている場合、ルータでは、それに基づいてトンネルが切断されリソースが確保されます（IPsec セキュリティ アソシエーション（SA））。

IPsec プロファイル

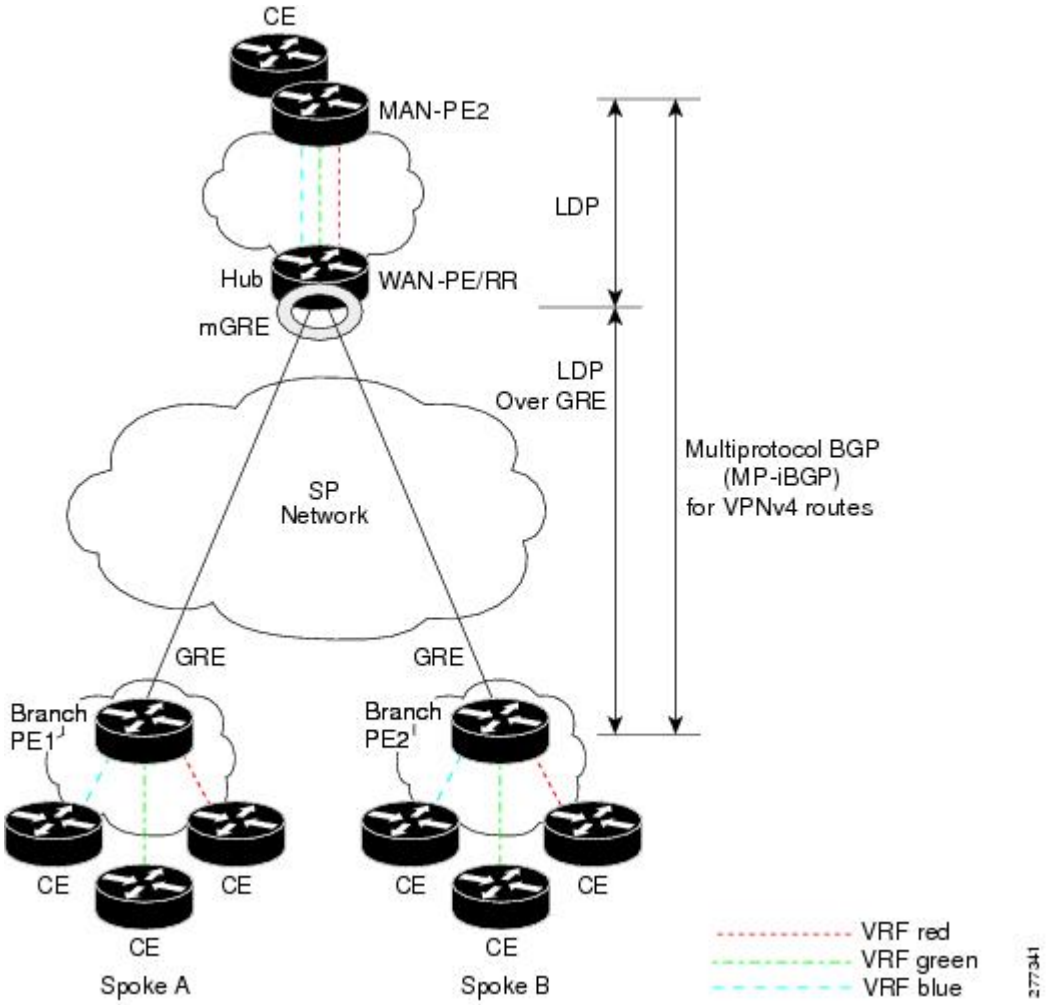
IPsec プロファイルを使用すると、主要な IPsec ポリシー情報を 1 つの設定エンティティにまとめることができます。この設定エンティティは、他の設定項目から名前を指定して参照することが可能です。これによりユーザは、ただ 1 つの設定行で、GRE トンネル保護などの機能を設定できます。IPsecプロファイルを参照すれば、ユーザがクリプトマップの設定をすべて行う必要はなくなります。IPsec プロファイルに含まれているのは IPsec 情報だけで、アクセス リスト情報やピアリング情報は含まれていません。

DMVPN 内のトラフィック セグメンテーションのイネーブル化

Cisco IOS XE Release 2.5 は、PE-PE mGRE トンネルを使用することで DMVPN トンネル内の VPN トラフィックをセグメント化できるように機能拡張されています。この保護された mGRE トンネルを使用して、すべて（または一連）の VPN トラフィックを転送できます。

次の図とそれに続く箇条書きは、DMVPN 内でのトラフィック セグメンテーションのしくみを説明したものです。

図 *2*：*DMVPN* 内のトラフィック セグメンテーション



- この図では、WAN-PE/ルート リフレクタがハブであり、クライアントがスポーク（PE ルータ）になっています。
- VRF は 3 つあり、それぞれ「赤」、「緑」、「青」で表してあります。
- 各スポークは、ハブとネイバー関係にある（マルチプロトコル内部ボーダー ゲートウェイ プロトコル（MP-iBGP）ピアリング）と同時に、ハブへの GRE トンネルを持っています。
- 各スポークからは、そのルートおよびVPN-IPv4（VPNv4）プレフィックスがハブにアドバタイズされます。
- ハブでは、アドバタイズされたルートをスポークに再アドバタイズする際、スポークから「学習」したすべての VPNv4 アドレスに対するネクストホップ ルートとして自身の IP を設

定し、VPN ごとにローカルの MPLS ラベルを割り当てます。結果として、スポーク A からスポーク B へのトラフィックは、ハブを介してルーティングされることになります。

このプロセスを具体例で説明すると次のようになります。

1. スポーク A により、VPNv4 ルートがハブにアドバタイズされ、VPN にラベル *x* が割り当てられます。
2. ハブは、スポーク B にルートをアドバタイズする際にラベルを *y* に変更します。
3. スポーク B では、スポーク A に送信するトラフィックにラベル *y* が適用され、そのトラフィックがハブに送信されます。
4. ハブはラベル y を削除してラベル x を適用することで VPN ラベルを付け替え、トラフィックをスポーク A に送信します。

NAT 透過性対応 DMVPN

多くの場合、DMVPN スポークは NAT ルータの背後に配置されます。この NAT ルータは通常、スポーク サイトのインターネット サービス プロバイダー（ISP）により制御され、スポーク ルータの外部インターフェイス アドレスが、プライベート IP アドレスに基づき ISP によって動的に割り当てられています（インターネット技術特別調査委員会（IETF）の RFC 1918 で規定）。

NAT 透過性対応 DMVPN の拡張機能により、NHRP では、IPsec トランスポート モード（DMVPN ネットワークで推奨される IPsec モード）が使用されている場合に限り、マッピングに対して NAT パブリック アドレスを学習および使用できます。NAT の背後に配置されていないスポーク ルータについては本来、アップグレードする必要はありませんが、NAT 透過性対応 DMVPN 機能を使用する場合は、事前にすべての DMVPN ルータを新しいコードにアップグレードすることを推奨します。NAT の後に配置されているスポーク ルータは、アップグレードされた後でも、ハブ ルータがアップグレードされるまでは、新しい設定（IPsec トランスポート モード）に切り替えることはできません。

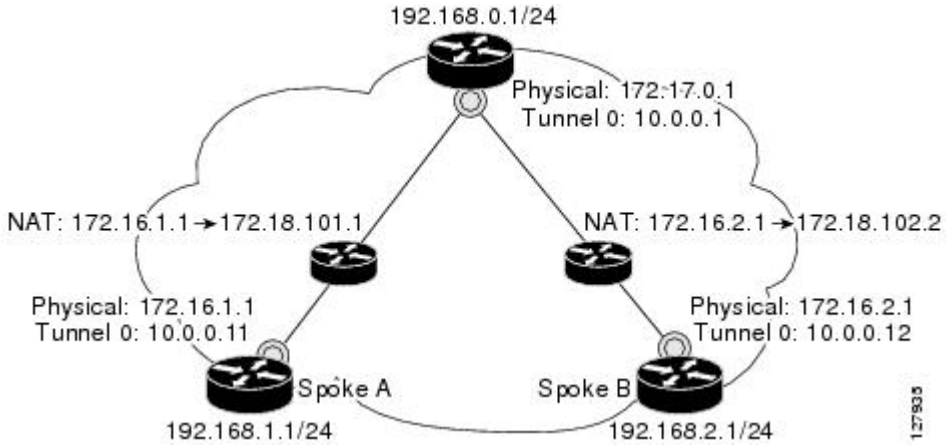
この NAT 透過性の拡張機能を使用すれば、ハブ DMVPN ルータをスタティック NAT の背後に配置できます。この機能を使用するためには、DMVPN のスポーク ルータおよびハブ ルータすべてをアップグレードする必要があります。また IPsec ではトランスポート モードを使用する必要があります。

NAT 透過性対応の拡張機能を有効にするには、トランスフォーム セットに対して IPsec トランスポート モードを使用する必要があります。また、NAT 透過性（IKE および IPsec）が有効であれば、（UDP ポートを使用して 2 つの IP アドレスを区別することにより）2 つのピア（IKE および IPsec）を同一の IP アドレスに変換できますが、DMVPN に対しては、この機能はサポートされません。DMVPN スポークの IP アドレスは、NAT 変換後、各 DMVPN スポークごとに一意であることが必要です。ただし、NAT 変換前の IP アドレスであれば、DMVPN スポーク間で重複していてもかまいません。

次の図に、NAT 透過性対応 DMVPN のシナリオを示します。

（注） NAT の背後にある DMVPN スポークは、ダイナミック ダイレクト スポークツースポーク トンネルに関与します。これらのスポークは、PAT ではなく NAT を実行する NAT 機器の後に配置する必要があります。この NAT 機器では、スポークツースポーク接続の場合でも、スポークがスポークツーハブ接続と同じ外部 NAT IP アドレスに変換されます。1 つの NAT 機器の背後に DMVPN スポークが複数配置されている場合、その NAT 機器では、それらの各 DMVPN スポークを別々の外部 NAT IP アドレスに変換する必要があります。また、それらのスポーク間には、ダイレクト スポークツースポーク トンネルを構築できない場合があります。スポークツースポーク トンネルを形成できない場合、スポークツースポーク パケットは、引き続きスポークツーハブ/スポーク パスを介して転送されます。

図 *3*：*NAT* 透過性対応 *DMVPN*



DMVPN でのコール アドミッション制御

DMVPN ネットワークでは、確立しようとするトンネル数の増加に伴って、DMVPN ルータが「過負荷」状態になることも少なくありません。コール アドミッション制御を使用すると、一度に確立できるトンネルの数を制限できます。これにより、ルータのメモリやCPU リソースのオーバーフローを回避できます。

コール アドミッション制御は、DMVPN スポークにおいて、スポーク ルータが開始または受信しようとする ISAKMAP セッション（DMVPN トンネル）の数を制限する場合に有効です。このような制限を課す場合は、コールアドミッション制御の IKE SA 制限を設定します。これによりルータでは、現在の ISAKMP SA 数が制限数を超過すると、新たな ISAKMP セッション要求（着信および発信）が廃棄されます。

またコール アドミッション制御は、DMVPN ハブにおいて、同時に確立される DMVPN トンネル数のレートを制限する場合にも有効です。このようなレート制限を課す場合は、コール アドミッション制御のシステム リソース制限を設定します。これによりルータでは、システムの使用率が指定値を超過すると、新たな ISAKMP セッション要求（新たな DMVPN トンネル）が廃棄されます。新たなセッション要求が廃棄されることにより、DMVPN ハブ ルータでは現在の ISAKMP

セッション要求の処理を完了できます。また、一度廃棄されたセッション要求でも、システムの使用率が低下した時点で再試行されれば、DMVPN ハブ ルータにより処理されます。

DMVPN でのコール アドミッション制御を使用するうえで、特別な設定は必要ありません。コール アドミッション制御の設定については、『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Call Admission Control for IKE」の章を参照してください。

NHRP のレート制限メカニズム

NHRP は、特定のインターフェイスから送信される NHRP パケットの総数を制限するためのレート制限メカニズムを備えています。**ipnhrpmax-send** コマンドを使用して設定されるデフォルト値は、インターフェイスあたり 10 秒ごとに 10,000 パケットです。制限数を超過した場合には、次のようなシステム メッセージが表示されます。

```
%NHRP-4-QUOTA: Max-send quota of [int]pkts/[int]Sec. exceeded on [chars]
```

このシステム メッセージの詳細については、『System Messages for Cisco IOS XE Software』を参照してください。

Dynamic Multipoint VPN の設定方法

ハブ ルータおよびスポーク ルータに対して mGRE/IPsec トンネルリングをイネーブルにするには、グローバル IPsec ポリシー テンプレートを使用して IPsec プロファイルを設定すること、および IPsec 暗号化に使用する mGRE トンネルを設定することが必要です。ここでは、次の手順について説明します。

IPsec プロファイルの設定

IPsec プロファイルには、クリプトマップの設定に使用するものと同じコマンドが多く使用されます。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 プロファイルでは、IPsec ポリシーに対応するコマンドだけを発行できます。IPsec ピア アドレスや、暗号化するパケットを照合するためのアクセス コントロール リスト（ACL）を指定することはできません。

（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。

はじめる前に

IPsec プロファイルを設定する前に、**cryptoipsectransform-set** コマンドを使用してトランスフォーム セットを定義する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **cryptoipsecprofile***name*
4. **settransform-set***transform-set-name*
5. **setidentity**
6. **setsecurityassociationlifetime** {**seconds***seconds* | **kilobytes***kilobytes*}
7. **setpfs** [**group1** | **group2**]

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： `Router> 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： `Router# 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	**cryptoipsecprofile***name*
	
	例：
	
	`Router(config)#`
	`crypto ipsec profile vpnprof`
		「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。
		• このコマンドを実行すると、クリプト マップ コンフィギュレーション モードが開始されます。
		• *name* 引数には、IPsec プロファイルの名前を指定します。

ステップ 4	**settransform-set***transform-set-name*
	
	例：
	
	`Router(config-crypto-map)# set`
	`transform-set trans2`
		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。
		• *transform-set-name* 引数には、トランスフォーム セットの名前を指定します。

ステップ 5	**setidentity**
	
	例：
	
	`Router(config-crypto-map)# set`
	`identity`
		（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。

	コマンドまたはアクション	目的
ステップ 6	**setsecurityassociationlifetime** {**seconds***seconds* | **kilobytes***kilobytes*} 例： `Router(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。 • **seconds***seconds* オプションには、セキュリティ アソシエーションの有効期間を秒数で指定します。また、**kilobytes***kilobytes* オプションには、特定のセキュリティ アソシエーションを使用してその有効期間内に IPsec ピア間で受け渡しできるトラフィックの量を指定します（単位は KB）。 • *seconds* 引数のデフォルト値は 3600 秒です。
ステップ 7	**setpfs** [**group1** | **group2**] 例： `Router(config-crypto-map)# set pfs group2`	（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（**group1**）が有効になります。 • **group1** キーワードの場合、新たに Diffie-Hellman（DH）交換を実行する際に、IPsec で 768 ビット DH 素数モジュラス グループが使用されます。**group2** キーワードの場合は、1024 ビット DH 素数モジュラス グループが使用されます。

DMVPN 用のハブの設定

mGRE/IPsec 統合用にハブ ルータを設定する（つまり、トンネルと、上記手順で設定した IPsec プロファイルとを関連付ける）場合は、次のコマンドを使用します。

（注） NHRP ネットワーク ID は、ローカルに限って意味を持つため、それぞれ異なっていてもかまいません。導入やメンテナンスの点から見れば、（**ipnhrpnetwork-id** コマンドを使用して）1 つの DMVPN ネットワーク内にある全ルータに対して一意の**ネットワーク ID** 番号を使用した方が合理的ですが、ここでは必ずしも同一である必要はありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipaddress***ip-addressmasksecondary*
5. **ipmtu***bytes*
6. **ipnhrpauthentication***string*
7. **ipnhrpmapmulticastdynamic**
8. **ipnhrpnetwork-id***number*
9. **tunnelsource**{*ip-address* | *typenumber*}
10. **tunnelkey***key-number*
11. **tunnelmodegremultipoint**
12. 次のいずれかを実行します。
    - **tunnelprotectionipsecprofile***name*
    - **tunnelprotectionpsk***key*
13. **bandwidth***kbps*
14. **iptcpadjust-mss***max-segment-size*
15. **ipnhrpholdtime***seconds*
16. **delay***number*

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： `Router> 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： `Router# 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： `Router(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。

	コマンドまたはアクション	目的
ステップ 4	**ipaddress***ip-addressmasksecondary* 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	トンネル インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 （注） 同一の DMVPN ネットワーク内に存在するすべてのハブおよびスポークには、同じ IP サブネットに属するアドレスを指定する必要があります。
ステップ 5	**ipmtu***bytes* 例： `Router(config-if)# ip mtu 1400`	各インターフェイスにおいて送信される IP パケットの最大伝送単位（MTU）のサイズをバイト単位で設定します。
ステップ 6	**ipnhrpauthentication***string* 例： `Router(config-if)# ip nhrp authentication donttell`	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 7	**ipnhrpmapmulticastdynamic** 例： `Router(config-if)# ip nhrp map multicast dynamic`	NHRP において、スポーク 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、**ipnhrpmapmulticastdynamic** がデフォルトでイネーブルになっています。
ステップ 8	**ipnhrpnetwork-id***number* 例： `Router(config-if)# ip 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。 • *number* 引数には、非ブロードキャスト マルチアクセス（NBMA）ネットワークの、グローバルに一意である 32 ビット ネットワーク識別子を指定します。範囲は 1 ～ 4294967295 です。 （注） Cisco IOS XE Denali 16.3 では、**ipnhrpnetwork-id** がデフォルトでイネーブルになっています。
ステップ 9	**tunnelsource**{*ip-address* | *typenumber*} 例： `Router(config-if)# tunnel source Gigabitethernet 0/0/0`	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 10	**tunnelkey***key-number* 例： `Router(config-if)# tunnel key 100000`	（任意）トンネル インターフェイスの ID キーをイネーブルにします。 • *key-number* 引数には、トンネル キーを識別するための数値を 0 ～ 4,294,967,295 の範囲で指定します。

	コマンドまたはアクション	目的
		（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、すべて同じキー値を設定する必要があります。
ステップ 11	**tunnelmodegremultipoint** 例： `Router(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*
	• **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 13	**bandwidth***kbps* 例： `Router(config-if)# bandwidth 1000`	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。 • *kbps* 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。 • 特にトンネル インターフェイス上で EIGRP を使用する場合は、帯域幅の値を必ず 1000 以上に設定してください。1 つのハブがサポートするスポークの数によっては、帯域幅の値をさらに大きくすることが必要となる場合もあります。
ステップ 14	**iptcpadjust-mss***max-segment-size* 例： `Router(config-if)# ip tcp adjust-mss 1360`	ルータを通過する TCP パケットの最大セグメント サイズ（MSS）の値を調整します。 • *max-segment-size* 引数には、最大セグメント サイズをバイト単位で指定します。範囲は 500 ～ 1460 です。 • IP MTU のバイト数が 1400 に設定されている場合、MSS の推奨値は 1360 です。これらの推奨値を使用した場合、IP パケットのサイズは、トンネルに「適合」するように、TCP セッションによって瞬時に 1400 バイトまで縮小されます。

	コマンドまたはアクション	目的
ステップ 15	**ipnhrpholdtime***seconds* 例： `Router(config-if)# ip nhrp holdtime 450`	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。 • *seconds* 引数には、信頼できる NHRP 応答により NBMA アドレスが有効としてアドバタイズされる時間を秒単位で指定します。推奨値の範囲は、300 ～ 600 秒です。
ステップ 16	**delay***number* 例： `Router(config-if)# delay 1000`	（任意）トンネル インターフェイスを介して学習したルートの EIGRP ルーティング メトリックを変更します。 • *number* 引数には、遅延時間を秒単位で指定します。推奨値は 1000 です。

DMVPN 用のスポークの設定

mGRE/IPsec 統合用にスポーク ルータを設定する場合は、次のコマンドを使用します。

（注） NHRP ネットワーク ID は、ローカルに限って意味を持つため、それぞれ異なっていてもかまいません。導入やメンテナンスの点から見れば、（**ipnhrpnetwork-id** コマンドを使用して）1 つの DMVPN ネットワーク内にある全ルータに対して一意の**ネットワーク ID** 番号を使用した方が合理的ですが、ここでは必ずしも同一である必要はありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipaddress***ip-addressmasksecondary*
5. **ipmtu***bytes*
6. **ipnhrpauthentication***string*
7. **ipnhrpmap***hub-tunnel-ip-addresshub-physical-ip-address*
8. **ipnhrpmapmulticast***hub-physical-ip-address*
9. **ipnhrpnhs***hub-tunnel-ip-address*
10. **ipnhrpnetwork-id***number*
11. **tunnelsource**{*ip-address* | *typenumber*}
12. **tunnelkey***key-number*
13. 次のいずれかを実行します。
    - **tunnelmodegremultipoint**
    - **tunneldestination***hub-physical-ip-address*
14. 次のいずれかを実行します。
    - **tunnelprotectionipsecprofile***name*
    - **tunnelprotectionpsk***key*
15. **bandwidth***kbps*
16. **iptcpadjust-mss***max-segment-size*
17. **ipnhrpholdtime***seconds*
18. **delay***number*

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： `Router> 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： `Router# 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： `Router(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	**ipaddress***ip-addressmasksecondary* 例： `Router(config-if)# ip address 10.0.0.2 255.255.255.0`	トンネルインターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 （注） 同一の DMVPN ネットワーク内に存在するすべてのハブおよびスポークには、同じ IP サブネットに属するアドレスを指定する必要があります。
ステップ 5	**ipmtu***bytes* 例： `Router(config-if)# ip mtu 1400`	各インターフェイスにおいて送信される IP パケットの MTU サイズをバイト単位で設定します。
ステップ 6	**ipnhrpauthentication***string* 例： `Router(config-if)# ip nhrp authentication donttell`	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 7	**ipnhrpmap***hub-tunnel-ip-addresshub-physical-ip-address* 例： `Router(config-if)# ip nhrp map 10.0.0.1 172.17.0.1`	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。 • *hub-tunnel-ip-address*：ハブで NHRP サーバを定義します。これはハブのスタティック パブリック IP アドレスに、永続的にマッピングされます。 • *hub-physical-ip-address*：ハブのスタティック パブリック IP アドレスを定義します。
ステップ 8	**ipnhrpmapmulticast***hub-physical-ip-address* 例： `Router(config-if)# ip nhrp map multicast 172.17.0.1`	スポークとハブの間でダイナミック ルーティング プロトコルを使用可能にし、マルチキャスト パケットをハブ ルータへ送信します。

	コマンドまたはアクション	目的
ステップ 9	**ipnhrpnhs***hub-tunnel-ip-address* 例： `Router(config-if)# ip nhrp nhs 10.0.0.1`	ハブ ルータを NHRP ネクストホップ サーバとして設定します。
ステップ 10	**ipnhrpnetwork-id***number* 例： `Router(config-if)# ip 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。 • *number* 引数には、NBMA ネットワークのグローバルに一意である 32 ビット ネットワーク識別子を指定します。範囲は 1 ～ 4294967295 です。 （注） Cisco IOS XE Denali 16.3 では、**ipnhrpnetwork-id** がデフォルトでイネーブルになっています。
ステップ 11	**tunnelsource**{*ip-address* | *typenumber*} 例： `Router(config-if)# tunnel source Gigabitethernet 0/0/0`	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 12	**tunnelkey***key-number* 例： `Router(config-if)# tunnel key 100000`	（任意）トンネル インターフェイスの ID キーをイネーブルにします。 • *key-number* 引数には、トンネル キーを識別するための数値を 0 ～ 4,294,967,295 の範囲で指定します。 • 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、すべて同じキー値を設定する必要があります。
ステップ 13	次のいずれかを実行します。 • **tunnelmodegremultipoint** • **tunneldestination***hub-physical-ip-address* 例： `Router(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。 • この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。 トンネル インターフェイスの宛先を指定します。 • この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 トラフィックを使用できる場合です。

	コマンドまたはアクション	目的
	例： `Router(config-if)# tunnel destination 172.17.0.1`	

ステップ 14	次のいずれかを実行します。
	• **tunnelprotectionipsecprofile***name*
	• **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***kbps* 例： `Router(config-if)# bandwidth 1000`	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。 • *kbps* 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	**iptcpadjust-mss***max-segment-size* 例： `Router(config-if)# ip tcp adjust-mss 1360`	ルータを通過する TCP パケットの MSS 値を調整します。 • *max-segment-size* 引数には、最大セグメント サイズをバイト単位で指定します。範囲は 500 ～ 1460 です。 • IP MTU のバイト数が 1400 に設定されている場合、MSS の推奨数値は 1360 です。これらの推奨値を使用した場合、IP パケットのサイズは、トンネルに「適合」するように、TCP セッションによって瞬時に 1400 バイトまで縮小されます。

	コマンドまたはアクション	目的
ステップ 17	**ipnhrpholdtime***seconds* 例： `Router(config-if)# ip nhrp holdtime 450`	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。 • *seconds* 引数には、信頼できる NHRP 応答により NBMA アドレスが有効としてアドバタイズされる時間を秒単位で指定します。推奨値の範囲は、300 ～ 600 秒です。
ステップ 18	**delay***number* 例： `Router(config-if)# delay 1000`	（任意）トンネル インターフェイスを介して学習したルートの EIGRP ルーティング メトリックを変更します。 • *number* 引数には、遅延時間を秒単位で指定します。推奨値は 1000 です。

VRF へのクリアテキスト データ IP パケット転送を設定

VRF へのクリアテキスト データ IP パケット転送を設定するには、次の手順を実行します。ここで説明する設定は、「Blue」という VRF が設定済みであることが前提になっています。

（注） VRF（Blue）を設定するには、グローバル コンフィギュレーション モードで **ip vrf** *vrf-name* コマンドを使用します。

手順の概要

1. **enable**
2. configure terminal
3. **interface***typenumber*
4. **ipvrfforwarding***vrf-name*

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： `Router# 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	**interface***typenumber* 例： `Router(config)# interface tunnel 0`	インターフェイス タイプを設定し、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。
ステップ 4	**ipvrfforwarding***vrf-name* 例： `Router(config-if)# ip vrf forwarding Blue`	VRF へのクリアテキスト データ IP パケット転送を許可します。

VRF への暗号化トンネル パケット転送の設定

VRF への暗号化トンネル パケット転送に関する設定手順は、次のとおりです。ここで説明する設定は、「Red」という VRF が設定済みであることが前提になっています。

（注） VRF（Red）を設定するには、グローバル コンフィギュレーション モードで **ip vrf** *vrf-name* コマンドを使用します。

手順の概要

1. **enable**
2. configure terminal
3. **interface***typenumber*
4. **tunnelvrf***vrf-name*

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： `Router> 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	configure terminal 例： `Router# 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	**interface***typenumber* 例： `Router(config)# interface tunnel 0`	インターフェイス タイプを設定し、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。
ステップ 4	**tunnelvrf***vrf-name* 例： `Router(config-if)# tunnel vrf RED`	VPN VRF インスタンスを特定のトンネル宛先、インターフェイス、またはサブインターフェイスに関連付けて、VRF への暗号化トンネル パケット転送を許可します。

DMVPN 内のトラフィック セグメンテーションの設定

Cisco IOS XE Release 2.5 では、トラフィック セグメンテーションの設定時に使用する新しいコマンドは導入されていません。ただし、DMVPN トンネル内のトラフィックをセグメント化するには、以降の項で説明する作業を完了する必要があります。

前提条件

次の作業では、DMVPN トンネル、および「Red」と「Blue」の 2 つの VRF が設定済みであることを前提としています。

Red または Blue の VRF を設定するには、グローバル コンフィギュレーション モードで **ip vrf** *vrf-name* コマンドを使用します。

DMVPN トンネルの設定については、DMVPN 用のハブの設定，（13 ページ）およびDMVPN 用のスポークの設定，（17 ページ）を参照してください。VRF 設定の詳細については、VRF へのクリアテキスト データ IP パケット転送を設定，（22 ページ）およびVRF への暗号化トンネル パケット転送の設定，（23 ページ）を参照してください。

VPN トンネルでの MPLS のイネーブル化

DMVPN トンネル内のトラフィック セグメンテーションは MPLS に依存するため、トラフィックをセグメント化する VRF インスタンスごとに MPLS を設定する必要があります。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、分散スイッチングのみがサポートされます。分散スイッチング用の **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]、**debug ip bgp vpnv4 unicast**、および **ip cef distributed** コマンドを使用してください。

手順の概要

1. **enable**
2. configure terminal
3. **interface***typenumber*
4. **mplsip**

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： `Router> 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	configure terminal 例： `Router# 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	**interface***typenumber* 例： `Router(config)# interface tunnel 0`	インターフェイス タイプを設定し、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。
ステップ 4	**mplsip** 例： `Router(config-if)# mpls ip`	指定したトンネル インターフェイスに対してパケットの MPLS タギングをイネーブルにします。

ハブ ルータでマルチプロトコル BGP を設定

VPN トラフィックに適用する VPNv4 プレフィックスおよびラベルのアドバタイズをイネーブルにするためには、MP-iBGP を設定する必要があります。BGP を使用して、ハブをルート リフレクタとして設定します。すべてのトラフィックが強制的にハブ経由でルーティングされるようにするには、BGP ルート リフレクタがルート リフレクタ クライアント（スポーク）に VPNv4 プレフィックスをアドバタイズする際に、自身をネクスト ホップとして指定するように設定します。

BGP ルーティング プロトコルの詳細については、『*Cisco IOS XE IP Routing: BGP Configuration Guide*』の「Cisco BGP Overview」の章を参照してください。

手順の概要

1. **enable**
2. configure terminal
3. **routerbgp***autonomous-system-number*
4. **neighbor***ipaddress***remote-as***as-number*
5. **neighbor***ipaddress***update-source***interface*
6. **address-familyvpnv4**
7. **neighbor***ipaddress***activate**
8. **neighbor***ipaddress***send-communityextended**
9. **neighbor***ipaddress***route-reflector-client**
10. **neighbor***ipaddress***route-mapnexthopout**
11. **exit**
12. **address-familyipv4***vrf-name*
13. **redistributeconnected**
14. **route-map***map-tag* [**permit**| **deny**] [*sequence-number*]
15. **setipnext-hop***ipaddress*

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： `Router> 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	configure terminal 例： `Router# 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	**router bgp** *autonomous-system-number* 例： `Router(config)# router bgp 1`	BGP ルーティング プロセスの設定をイネーブルにします。
ステップ 4	**neighbor** *ipaddress* **remote-as** *as-number* 例： `Router(config-router)# neighbor 10.0.0.11 remote-as 1`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 5	**neighbor** *ipaddress* **update-source** *interface* 例： `Router(config-router)# neighbor 10.10.10.11 update-source Tunnel1`	BGP セッションで TCP 接続の動作インターフェイスが使用できるよう、Cisco IOS XE ソフトウェアを設定します。
ステップ 6	**address-family vpnv4** 例： `Router(config)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始し、VPNv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** *ipaddress* **activate** 例： `Router(config-router-af)# neighbor 10.0.0.11 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 8	**neighbor** *ipaddress* **send-community extended** 例： `Router(config-router-af)# neighbor 10.0.0.11 send-community extended`	拡張コミュニティの属性が BGP ネイバーに送信されるよう指定します。
ステップ 9	**neighbor** *ipaddress* **route-reflector-client** 例： `Router(config-router-af)# neighbor 10.0.0.11 route-reflector-client`	ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。
ステップ 10	**neighbor** *ipaddress* **route-map nexthop out** 例： `Router(config-router-af)# neighbor 10.0.0.11 route-map nexthop out`	すべてのトラフィックが強制的にハブ経由でルーティングされるようにします。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `Router(config-router-af)# exit`	VPNv4 のアドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 12	**address-familyipv4***vrf-name* 例： `Router(config)# address-family ipv4 red`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 13	**redistributeconnected** 例： `Router(config-router-af)# redistribute connected`	インターフェイス上で IP をイネーブルにしたことにより自動的に確立されたルートを、あるルーティング ドメインから別のルーティング ドメインへ再分配します。
ステップ 14	**route-map***map-tag* [**permit**| **deny**] [*sequence-number*] 例： `Router(config-router-af)# route-map cisco permit 10`	ルート マップ コンフィギュレーション モードを開始し、スポークにアドバタイズされるネクスト ホップを設定します。
ステップ 15	**setipnext-hop***ipaddress* 例： `Router(config-route-map)# set ip next-hop 10.0.0.1`	ネクスト ホップがハブになるように設定します。

スポーク ルータでのマルチプロトコル BGP の設定

DMVPN トンネル内のトラフィックをセグメント化するには、スポーク ルータとハブの両方でマルチプロトコル iBGP（MP-iBGP）を設定する必要があります。DMVPN 内のスポーク ルータごとに、次の作業を実行します。

手順の概要

1. **enable**
2. configure terminal
3. **routerbgp***autonomous-system-number*
4. **neighbor***ipaddress***remote-as***as-number*
5. **neighbor***ipaddress***update-source***interface*
6. **address-familyvpnv4**
7. **neighbor***ipaddress***activate**
8. **neighbor***ipaddress***send-communityextended**
9. **exit**
10. **address-familyipv4***vrf-name*
11. **redistributeconnected**
12. **exit**

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： `Router> 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	configure terminal 例： `Router# 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	**routerbgp***autonomous-system-number* 例： `Router(config)# router bgp 1`	BGP コンフィギュレーション モードを開始します。
ステップ 4	**neighbor***ipaddress***remote-as***as-number* 例： `Router(config-router)# neighbor 10.0.0.1 remote-as 1`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor***ipaddress***update-source***interface* 例： `Router(config-router)# neighbor 10.10.10.1 update-source Tunnel1`	BGP セッションで TCP 接続の動作インターフェイスが使用できるよう、Cisco IOS XE ソフトウェアを設定します。
ステップ 6	**address-familyvpnv4** 例： `Router(config)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始し、VPNv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor***ipaddress***activate** 例： `Router(config-router-af)# neighbor 10.0.0.1 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 8	**neighbor***ipaddress***send-communityextended** 例： `Router(config-router-af)# neighbor 10.0.0.1 send-community extended`	拡張コミュニティの属性が BGP ネイバーに送信されるよう指定します。
ステップ 9	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 10	**address-familyipv4***vrf-name* 例： `Router(config)# address-family ipv4 red`	アドレス ファミリ コンフィギュレーション モードを開始し、標準IPv4アドレスプレフィックスを使用するルーティング セッションを設定します。
ステップ 11	**redistributeconnected** 例： `Router(config-router-af)# redistribute connected`	インターフェイス上で IP をイネーブルにしたことにより自動的に確立されたルートを、あるルーティング ドメインから別のルーティング ドメインへ再分配します。
ステップ 12	**exit** 例： `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。 （注） VRF ごとにステップ 10 ～ 12 を繰り返します。

Dynamic Multipoint VPN のトラブルシューティング

DMVPN を設定した後、DMVPN が正常に動作していることを確認したり、DMVPN 統計情報またはセッションをクリアしたり、DMVPN をデバッグしたりするには、この作業の該当する手順を実行します。これらのコマンドは任意の順序で使用できます。

（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。

手順の概要

1. **cleardmvpnsession**
2. **cleardmvpnstatistics**
3. **debugdmvpn**
4. **debugdmvpncondition**
5. **debugnhrpcondition**
6. **debugnhrperror**
7. **loggingdmvpn**
8. **showcryptoipsecsa**
9. **showcryptoisakmpsa**
10. **showcryptomap**
11. **showdmvpn**
12. **showipnhrptraffic**

手順の詳細

ステップ 1 **cleardmvpnsession**

このコマンドは DMVPN セッションをクリアします。次の例では、指定したトンネルのダイナミック DMVPN セッションのみがクリアされます。

例：

```
Router# clear dmvpn session interface tunnel 5
```

次の例では、指定したトンネルのすべての DMVPN セッション（スタティック セッションとダイナミック セッションの両方）がクリアされます。

例：

```
Router# clear dmvpn session interface tunnel 5 static
```

ステップ 2 **cleardmvpnstatistics**

このコマンドは、DMVPN 関連のカウンタをクリアする場合に使用します。次の例では、指定したトンネル インターフェイスの DMVPN 関連セッション カウンタをクリアする方法を示します。

例：

```
Router#
 clear dmvpn statistics interface tunnel 5
```

ステップ 3 **debugdmvpn**

このコマンドは、DMVPN セッションをデバッグする場合に使用します。DMVPN のデバッグは、ある特定の条件に応じてイネーブル化/ディセーブル化を切り替えることができます。DMVPN のデバッグには、次のように 3 つのレベルがあります。下位のレベルほど、細部のデバッグを実行できます。

- エラー レベル
- 詳細レベル
- パケット レベル

次の例では、NHRP、ソケット、トンネル保護、および暗号情報に対するエラーデバッグをすべて表示する条件付き DMVPN デバッグをイネーブルにする方法を示します。

例：

```
Router# debug dmvpn error all
```

ステップ 4 **debugdmvpncondition**

このコマンドは、条件付きデバッグDMVPNセッションの情報を表示します。次の例では、特定のトンネル インターフェイスに対して条件付きデバッグをイネーブルにする方法を示します。

例：

```
Router# debug dmvpn condition interface tunnel 5
```

ステップ 5 **debugnhrpcondition**

このコマンドは、特定の条件に基づくデバッグをイネーブルまたはディセーブルにします。次に、条件付き NHRP デバッグをイネーブルにするためのコマンドの使用例を示します。

例：

```
Router#
debug nhrp condition
```

ステップ 6 **debugnhrperror**

このコマンドは、NHRP エラー アクティビティに関する情報を表示します。次に、NHRP のエラー メッセージに対するデバッグをイネーブルにするためのコマンドの使用例を示します。

例：

```
Router#
debug nhrp error
```

ステップ 7 **loggingdmvpn**

このコマンドは、DMVPN のシステム ロギングをイネーブルにする場合に使用します。次の例では、20 秒ごとに 1 つのメッセージが生成される DMVPN のシステム ロギングをイネーブルにする方法を示します。

例：

```
Router(config)#
logging dmvpn rate-limit 20
```

次に、DMVPN メッセージがリスト表示されたシステム ログの例を示します。

例：

```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel1 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel101 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```

ステップ 8 **showcryptoipsecsa**

このコマンドは、現在の SA によって使用されている設定を表示します。次に、アクティブなデバイスの IPsec SA ステータスだけが表示される出力例を示します。

例：

```
Router#
show crypto ipsec sa active
interface: gigabitethernet0/0/0
    Crypto map tag: to-peer-outside, local addr 209.165.201.3
   protected vrf: (none
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
     path mtu 1500, media mtu 1500
     current outbound spi: 0xD42904F0(3559458032)
     inbound esp sas:
      spi: 0xD3E9ABD0(3555306448)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: 6, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4586265/3542)
```

```
        HA last key lifetime sent(k): (4586267)
        ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```

ステップ 9 **showcryptoisakmpsa**

このコマンドは、ピアの現在の IKE SA をすべて表示します。たとえば次の例は、2 つのピア間の IKE ネゴシエーションが正常に実行された後に表示される出力です。

例：

```
Router# show crypto isakmp sa
dst             src             state          conn-id    slot
172.17.63.19    172.16.175.76   QM_IDLE              2       0
172.17.63.19    172.17.63.20    QM_IDLE              1       0
172.16.175.75   172.17.63.19    QM_IDLE              3       0
```

ステップ 10 **showcryptomap**

このコマンドは、クリプト マップの設定を表示します。次に、クリプト マップの設定が完了した後に表示される出力例を示します。

例：

```
Router# show crypto map
Crypto Map "Tunnel5-head-0" 10 ipsec-isakmp
        Profile name: vpnprof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={trans2, }
Crypto Map "Tunnel5-head-0" 20 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.175.75
        Extended IP access list
            access-list permit gre host 172.17.63.19 host 172.16.175.75
        Current peer: 172.16.175.75
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={trans2, }
Crypto Map "Tunnel5-head-0" 30 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.17.63.20
        Extended IP access list
            access-list permit gre host 172.17.63.19 host 172.17.63.20
        Current peer: 172.17.63.20
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={trans2, }
Crypto Map "Tunnel5-head-0" 40 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.16.175.76
        Extended IP access list
            access-list permit gre host 172.17.63.19 host 172.16.175.76
        Current peer: 172.16.175.76
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={trans2, }
        Interfaces using crypto map Tunnel5-head-0:
```

Tunnel5

ステップ 11 **showdmvpn**

このコマンドは、DMVPN 固有のセッション情報を表示します。次に、サマリー情報の出力例を示します。

例：

```
Router# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.
Tunnel1, Type: Spoke, NBMA Peers: 3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2      192.0.2.21     192.0.2.116   IKE     3w0d D
     1     192.0.2.102      192.0.2.11  NHRP 02:40:51 S
     1     192.0.2.225      192.0.2.10    UP     3w0d S
Tunnel2, Type: Spoke, NBMA Peers: 1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1        192.0.2.25      192.0.2.171   IKE    never S
```

ステップ 12 **showipnhrptraffic**

このコマンドは、NHRP の統計情報を表示します。次に、特定のトンネル（tunnel7）に関する出力例を示します。

例：

```
Router# s
how ip nhrp traffic interface tunnel7
Tunnel7: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 79
         18 Resolution Request  10 Resolution Reply  42 Registration Request
         0 Registration Reply    3 Purge Request      6 Purge Reply
         0 Error Indication      0 Traffic Indication
   Rcvd: Total 69
         10 Resolution Request  15 Resolution Reply  0 Registration Request
         36 Registration Reply   6 Purge Request     2 Purge Reply
         0 Error Indication      0 Traffic Indication
```

次の作業

「DMVPN 用のハブの設定」と「DMVPN 用のスポークの設定」の項に進みます。

Dynamic Multipoint VPN 機能の設定例

DMVPN 用のハブ設定例

次に、マルチポイント GRE/IPsec 統合用のハブ ルータの設定例を示します。これは、すべてのスポーク ルータが対話可能なグローバル IPsec ポリシー テンプレートを使用した設定方法で、各ス

ポークに対する個別の設定を明示的に行う必要はありません。ここでは、EIGRP が、プライベート物理インターフェイスおよびトンネル インターフェイスを介して実行されるように設定されています。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the receiving
 router would have to do the reassembly.
 ip mtu 1400
! The following line must match on all nodes that “want to use” this mGRE tunnel:
 ip nhrp authentication donttell
! Note that the next line is required only on the hub.
 ip nhrp map multicast dynamic
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not advertise
 routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
! Enables dynamic, direct spoke-to-spoke tunnels when using EIGRP.
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
! Sets IPsec peer address to Ethernet interface’s public address.
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface FastEthernet0/0/0
 ip address 172.17.0.1 255.255.255.0
!
interface FastEthernet0/0/1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
!
```

ISAKMP プロファイルの定義および設定の詳細については、『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Certificate to ISAKMP Profile Mapping」の章を参照してください。

DMVPN 用のスポーク設定例

次の例は、すべてのスポークを、トンネルとローカルインターフェイスアドレス以外は同じ内容で設定する方法で、ユーザが行うべき設定操作を軽減できます。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
```

```
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp authentication donttell
! Definition of NHRP server at the hub (10.0.0.1), which is permanently mapped to the static
 public address of the hub (172.17.0.1).
 ip nhrp map 10.0.0.1 172.17.0.1
! Sends multicast packets to the hub router, and enables the use of a dynamic routing
protocol between the spoke and the hub.
 ip nhrp map multicast 172.17.0.1
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Configures the hub router as the NHRP next-hop server.
 ip nhrp nhs 10.0.0.1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel:
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
! This is a spoke, so the public address might be dynamically assigned via DHCP.
interface FastEthernet0/0/0
 ip address dhcp hostname Spoke1
!
interface FastEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
!
! EIGRP is configured to run over the inside physical interface and the tunnel.
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
```

BGP 専用トラフィック セグメンテーションでの 2547oDMVPN の例

次に、PEデバイスとして動作する2つのスポーク間でトラフィックをセグメント化するためのトラフィック セグメンテーションの設定例を示します。

ハブの設定

```
hostname hub-pe1
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
clock timezone EST 0
ip cef
no ip domain lookup
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
```

```
mpls label protocol ldp
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t1 esp-des
 mode transport
crypto ipsec profile prof
 set transform-set t1
interface Tunnel1
 ip address 10.9.9.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
!The command below enables MPLS on the DMVPN network:
mpls ip
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
interface Ethernet0/0/0
 ip address 172.0.0.1 255.255.255.0
!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.11 remote-as 1
 neighbor 10.0.0.11 update-source Tunnel1
 neighbor 10.0.0.12 remote-as 1
 neighbor 10.0.0.12 update-source Tunnel1
 no auto-summary
 address-family vpnv4
 neighbor 10.0.0.11 activate
 neighbor 10.0.0.11 send-community extended
 neighbor 10.0.0.11 route-reflector-client
 neighbor 10.0.0.11 route-map nexthop out
 neighbor 10.0.0.12 activate
 neighbor 10.0.0.12 send-community extended
 neighbor 10.0.0.12 route-reflector-client
 neighbor 10.0.0.12 route-map nexthop out
 exit
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit
 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit
no ip http server
no ip http secure-server
!In this route map information, the hub sets the next hop to itself, and the VPN prefixes
are advertised:
route-map cisco permit 10
 set ip next-hop 10.0.0.1
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
end
```

スポークの設定

スポーク 2

```
hostname spoke-pe2
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
clock timezone EST 0
ip cef
no ip domain lookup
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
mpls label protocol ldp
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t1 esp-des
 mode transport
crypto ipsec profile prof
 set transform-set t1
interface Tunnel1
 ip address 10.0.0.11 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1
!The command below enables MPLS on the DMVPN network:
 mpls ip
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof
interface Loopback0
 ip address 10.9.9.11 255.255.255.255
interface FastEthernet0/0/0
 ip address 172.0.0.11 255.255.255.0
!
!
interface FastEthernet1/0/0
 ip vrf forwarding red
 ip address 192.168.11.2 255.255.255.0
interface FastEthernet2/0/0
 ip vrf forwarding blue
 ip address 192.168.11.2 255.255.255.0
!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 update-source Tunnel1
 no auto-summary
 address-family vpnv4
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-community extended
 exit
!
```

```
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit
 !
 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit
no ip http server
no ip http secure-server
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
end
```

スポーク 3

```
hostname spoke-PE3
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
clock timezone EST 0
ip cef
no ip domain lookup
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
mpls label protocol ldp
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t1 esp-des
 mode transport
crypto ipsec profile prof
 set transform-set t1
interface Tunnel1
 ip address 10.0.0.12 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1
!The command below enables MPLS on the DMVPN network:
 mpls ip
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof
!
interface Loopback0
 ip address 10.9.9.12 255.255.255.255
interface FastEthernet0/0/0
 ip address 172.0.0.12 255.255.255.0
interface FastEthernet1/0/0
 ip vrf forwarding red
 ip address 192.168.12.2 255.255.255.0
interface FastEthernet2/0/0
 ip vrf forwarding blue
```

```
 ip address 192.168.12.2 255.255.255.0
!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 update-source Tunnel1
 no auto-summary
 address-family vpnv4
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-community extended
 exit
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit
 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit
no ip http server
no ip http secure-server
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
end
```

エンタープライズ ブランチ トラフィック セグメンテーションでの 2547oDMVPN の例

次に、企業のブランチ オフィスに配置されている 2 つのスポーク間でトラフィックをセグメント化するための設定例を示します。この例では、DMVPN 内の BGP ネイバーに到達するルートを学習するように、EIGRP が設定されています。

ハブの設定

```
hostname HUB
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
clock timezone EST 0
ip cef
no ip domain lookup
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!This refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
mpls label protocol ldp
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t1 esp-des
```

```
 mode transport
crypto ipsec profile prof
 set transform-set t1
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
no ip split-horizon eigrp 1
!The command below enables MPLS on the DMVPN network:
 mpls ip
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof
!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.1 255.255.255.255
interface FastEthernet0/0/0
 ip address 172.0.0.1 255.255.255.0
!EIGRP is configured to learn the BGP peer addresses (10.9.9.x networks)
router eigrp 1
 network 10.9.9.1 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary
!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.1
 bgp log-neighbor-changes
 neighbor 10.9.9.11 remote-as 1
 neighbor 10.9.9.11 update-source Loopback0
 neighbor 10.9.9.12 remote-as 1
 neighbor 10.9.9.12 update-source Loopback0
 no auto-summary
 address-family vpnv4
 neighbor 10.9.9.11 activate
 neighbor 10.9.9.11 send-community extended
 neighbor 10.9.9.11 route-reflector-client
 neighbor 10.9.9.12 activate
 neighbor 10.9.9.12 send-community extended
 neighbor 10.9.9.12 route-reflector-client
 exit
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit
 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit
no ip http server
no ip http secure-server
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
end
```

スポークの設定

スポーク 2

```
hostname Spoke2
boot-start-marker
```

```
boot-end-marker
no aaa new-model
resource policy
clock timezone EST 0
ip cef
no ip domain lookup
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
mpls label protocol ldp
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t1 esp-des
 mode transport
crypto ipsec profile prof
 set transform-set t1
interface Tunnel1
 ip address 10.0.0.11 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1
!The command below enables MPLS on the DMVPN network:
 mpls ip
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof
!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.11 255.255.255.255
interface FastEthernet0/0/0
 ip address 172.0.0.11 255.255.255.0
interface FastEthernet1/0/0
 ip vrf forwarding red
 ip address 192.168.11.2 255.255.255.0
interface FastEthernet2/0/0
 ip vrf forwarding blue
 ip address 192.168.11.2 255.255.255.0
!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
router eigrp 1
 network 10.9.9.11 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary
!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.11
 bgp log-neighbor-changes
 neighbor 10.9.9.1 remote-as 1
 neighbor 10.9.9.1 update-source Loopback0
 no auto-summary
 address-family vpnv4
 neighbor 10.9.9.1 activate
 neighbor 10.9.9.1 send-community extended
 exit
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit
 address-family ipv4 vrf blue
```

```
 redistribute connected
 no synchronization
 exit
no ip http server
no ip http secure-server
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
end
```

スポーク 3

```
hostname Spoke3
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
clock timezone EST 0
ip cef
no ip domain lookup
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2
!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1
mpls label protocol ldp
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set t1 esp-des
 mode transport
crypto ipsec profile prof
 set transform-set t1
interface Tunnel1
 ip address 10.0.0.12 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1
!The command below enables MPLS on the DMVPN network:
 mpls ip
 tunnel source Gigabitethernet 0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof
!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.12 255.255.255.255
interface FastEthernet0/0/0
 ip address 172.0.0.12 255.255.255.0
interface FastEthernet1/0/0
 ip vrf forwarding red
 ip address 192.168.12.2 255.255.255.0
interface FastEthernet2/0/0
 ip vrf forwarding blue
 ip address 192.168.12.2 255.255.255.0
!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
router eigrp 1
 network 10.9.9.12 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary
```

```
!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.12
 bgp log-neighbor-changes
 neighbor 10.9.9.1 remote-as 1
 neighbor 10.9.9.1 update-source Loopback0
 no auto-summary
 address-family vpnv4
 neighbor 10.9.9.1 activate
 neighbor 10.9.9.1 send-community extended
 exit
 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit
 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit
no ip http server
no ip http secure-server
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login
end
```

コマンドの出力例：**show mpls ldp bindings**

```
Spoke2# show mpls ldp bindings
  tib entry: 10.9.9.1/32, rev 8
        local binding:  tag: 16
        remote binding: tsr: 10.9.9.1:0, tag: imp-null
  tib entry: 10.9.9.11/32, rev 4
        local binding:  tag: imp-null
        remote binding: tsr: 10.9.9.1:0, tag: 16
  tib entry: 10.9.9.12/32, rev 10
        local binding:  tag: 17
        remote binding: tsr: 10.9.9.1:0, tag: 17
  tib entry: 10.0.0.0/24, rev 6
        local binding:  tag: imp-null
        remote binding: tsr: 10.9.9.1:0, tag: imp-null
  tib entry: 172.0.0.0/24, rev 3
        local binding:  tag: imp-null
        remote binding: tsr: 10.9.9.1:0, tag: imp-null
Spoke2#
```

コマンドの出力例：**show mpls forwarding-table**

```
Spoke2# show mpls forwarding-table

Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     10.9.9.1/32        0          Tu1        10.0.0.1
17     17          10.9.9.12/32       0          Tu1        10.0.0.1
18     Aggregate   192.168.11.0/24[V]   \
                                      0
19     Aggregate   192.168.11.0/24[V]   \
                                      0
Spoke2#
```

コマンドの出力例：show ip route vrf red

```
Spoke2# show ip route vrf red
Routing Table: red
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
B    192.168.12.0/24 [200/0] via 10.9.9.12, 00:00:02
C    192.168.11.0/24 is directly connected, FastEthernet1/0/0
Spoke2#
```

コマンドの出力例：show ip route vrf blue

```
Spoke2# show ip route vrf blue
Routing Table: blue
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
B    192.168.12.0/24 [200/0] via 10.9.9.12, 00:00:08
C    192.168.11.0/24 is directly connected, FastEthernet2/0/0
Spoke2#
Spoke2# show ip cef vrf red 192.168.12.0
192.168.12.0/24, version 5, epoch 0
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Tu1, 10.0.0.1, tags imposed: {17 18}
  via 10.9.9.12, 0 dependencies, recursive
    next hop 10.0.0.1, Tunnel1 via 10.9.9.12/32
    valid adjacency
    tag rewrite with Tu1, 10.0.0.1, tags imposed: {17 18}
Spoke2#
```

コマンドの出力例：show ip bgp neighbors

```
Spoke2# show ip bgp neighbors

BGP neighbor is 10.9.9.1,  remote AS 1, internal link
  BGP version 4, remote router ID 10.9.9.1
  BGP state = Established, up for 00:02:09
  Last read 00:00:08, last write 00:00:08, hold time is 180, keepalive interval is 60 seconds

  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                4          4
    Keepalives:             4          4
    Route Refresh:          0          0
    Total:                  9          9
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast
```

```
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0
 For address family: VPNv4 Unicast
  BGP table version 9, neighbor version 9/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              2          2 (Consumes 136 bytes)
    Prefixes Total:                4          2
    Implicit Withdraw:             2          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          2
    Used as multipath:           n/a          0
                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    ORIGINATOR loop:                   n/a          2
    Bestpath from this peer:             4        n/a
    Total:                               4          2
  Number of NLRIs in the update sent: max 1, min 1
  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.9.9.11, Local port: 179
Foreign host: 10.9.9.1, Foreign port: 12365
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x2D0F0):
Timer          Starts    Wakeups            Next
Retrans             6          0             0x0
TimeWait            0          0             0x0
AckHold             7          3             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 3328307266  snduna: 3328307756  sndnxt: 3328307756     sndwnd:  15895
irs: 4023050141  rcvnxt: 4023050687  rcvwnd:      16384  delrcvwnd:      0
SRTT: 165 ms, RTTO: 1457 ms, RTV: 1292 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 536 bytes):
Rcvd: 13 (out of order: 0), with data: 7, total data bytes: 545
Sent: 11 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data:
 6, total data bytes: 489
Spoke2#
```

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
コール アドミッション制御	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Call Admission Control for IKE」の章
IKE の設定作業（IKE ポリシーの定義など）	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPSec VPNs」の章
IPsec の設定作業	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」の章
VRF 対応 IPsec の設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「VRF-Aware IPsec」の章
MPLS の設定	『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*』の「Multiprotocol Label Switching (MPLS) on Cisco Routers」の章
BGP の設定	『*Cisco IOS XE IP Routing: BGP Configuration Guide*』の「Cisco BGP Overview」の章
システム メッセージ	『System Messages for Cisco IOS XE Software』
ISAKMP プロファイルの定義と設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Certificate to ISAKMP Profile Mapping」の章
セキュリティ コマンド	『Cisco IOS Security Command Reference』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2547	『BGP/MPLS VPNs』

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

Dynamic Multipoint VPN 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*：*Dynamic Multipoint VPN* の機能情報

機能名	リリース	機能情報
DMVPN フェーズ 1	Cisco IOS XE Release 2.1	DMVPN 機能を使用すると、GRE トンネル、IPsec 暗号化、およびNHRP を組み合わせることにより、目的に合せて大小さまざまな規模の IPsec VPN を構築できます。
DMVPN フェーズ 2	Cisco IOS XE Release 2.1	DMVPN スポークツースポーク機能は、実稼働環境での使用にも十分対応できるようになりました。
NAT 透過性対応 DMVPN	Cisco IOS XE Release 2.1	ネットワーク アドレス変換透過性（NAT-T）対応 DMVPN の拡張機能が追加されました。また、DMVPN ハブツースポーク機能は、実稼働環境での使用にも十分対応できるようになりました。

機能名	リリース	機能情報
DMVPN の管理を容易にするための拡張機能	Cisco IOS XE Release 2.5	DMVPN セッションは、デバッグ、表示出力、セッションとカウンタの制御、およびシステムログ情報に関する DMVPN 専用コマンドを使用することで、より容易に管理できるようになりました。 この機能に関する詳細については、次の項を参照してください。 • Dynamic Multipoint VPN のトラブルシューティング この機能により、次のコマンドが導入または変更されました。**cleardmvpnsession**、**cleardmvpnstatistics**、**debugdmvpn**、**debugdmvpncondition**、**debugnhrpcondition**、**debugnhrperror**、**loggingdmvpn**、**showdmvpn**、**showipnhrptraffic**
DMVPN：DMVPN 内のトラフィック セグメンテーションのイネーブル化	Cisco IOS XE Release 2.5	2547oDMVPN 機能を使用すると、各 VRF の送信元および宛先を示す MPLS ラベルを VRF インスタンスに適用することにより、DMVPN トンネル内の VPN トラフィックをセグメント化できます。

用語集

AM：アグレッシブ モード。IKE ネゴシエーション実行中のモードです。MM と比較すると、AM はいくつかのプロセスが省略されているため動作は速くなりますが、セキュリティ性能は低くなります。Cisco IOS XE ソフトウェアでは、アグレッシブ モードを開始した IKE ピアにアグレッシブ モードで応答します。

GRE：総称ルーティング カプセル化。トンネルを構成することにより、共有 WAN 全体に特定の経路を確保するとともに、特定の宛先へトラフィックを確実に送り届けるため新たなパケット

ヘッダーでトラフィックをカプセル化します。トラフィックにとってトンネルの入口となるのはエンドポイントに限られるため、プライベートなネットワークを実現できます。トンネルそのものは、暗号化のように高い機密性を確保する手段にはなりませんが、暗号化されたトラフィックをトンネル経由で送信することは可能です。

GRE トンネリングを使用すると、非 IP トラフィックを IP にカプセル化して、インターネットや IP ネットワーク上に送信することもできます。非 IP トラフィックに該当するのは、インターネット パケット交換（IPX）プロトコルや AppleTalk プロトコルなどのトラフィックです。

IKE：インターネット キー交換。Oakley キー交換や Skeme キー交換を ISAKMP フレームワーク内部に実装したハイブリッド プロトコルです。IKE は、他のプロトコルでも使用できますが、初期実装されるのは IPsec です。IKE は、IPsec ピアを認証し、IPsec キーをネゴシエーションし、IPsec セキュリティ アソシエーションを実行します。

IPSec：IP セキュリティ。インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

ISAKMP：Internet Security Association Key Management Protocol。ペイロード形式、キー交換プロトコル実装の方法、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワークです。

MM：メイン モード。MM では、IKE ピアに対してより多くのセキュリティ プロポーザルが提供されます。そのため MM は、アグレッシブ モードに比べると動作速度は劣りますが、セキュリティ性能や柔軟性の面では優れたモードです。IKE 認証（RSA シグニチャ、RSA 暗号、または事前共有キー）では、MM がデフォルトで開始されます。

NHRP：Next Hop Resolution Protocol。ルータ、アクセス サーバ、およびホストは、NHRP を使用して、NBMA ネットワークに接続された他のルータおよびホストのアドレスを検出できます。

シスコによる NHRP の実装では、IETF ドラフト バージョン 11 の NBMA Next Hop Resolution Protocol（NHRP）をサポートしています。

また、IP バージョン 4 およびインターネット パケット交換（IPX）ネットワーク層をサポートしているほか、リンク層では、ATM、FastEthernet、SMDS、およびマルチポイント トンネル ネットワークもサポートしています。NHRP は FastEthernet 上で使用できますが、FastEthernet ではブロードキャストが可能であるため、NHRP を FastEthernet メディアに実装する必要はありません。IPX に対して FastEthernet のサポートは不要です（サポートはありません）。

PFS：Perfect Forward Secrecy。これは、導き出される共有秘密値に関連する暗号特性です。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。

SA：セキュリティ アソシエーション。2 つ以上のエンティティ間で、安全な通信を行うためのセキュリティ サービスをどのように使用するかを規定したものです。たとえば IPsec の SA では、IPsec 接続の際に使用される暗号化アルゴリズム（使用される場合）、認証アルゴリズム、および共有セッション キーが定義されます。

IPsec および IKE では、接続パラメータの識別に必ず SA が使用されます。IKE では、独自に SA をネゴシエーションして確立できます。IPsec の SA は、IKE により確立することも、ユーザ設定により確立することもできます。

トランスフォーム：データフローに対し、データ認証、データの機密性の確保、およびデータ圧縮を目的として行われる一連の処理。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

VPN：バーチャルプライベートネットワーク。複数のピアで構成されるフレームワークで、各ピア間では、他のパブリック インフラストラクチャを介して機密データがセキュアに転送されます。このフレームワークでは、すべてのデータをトンネルして暗号化するプロトコルによって、着信ネットワーク トラフィックおよび発信ネットワーク トラフィックが保護されます。また、ネットワークをローカル トポロジの外部にまで拡張できるほか、リモート ユーザがダイレクトネットワーク接続の状況を確認したり、その機能を利用したりすることも可能です。

第 3 章

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。

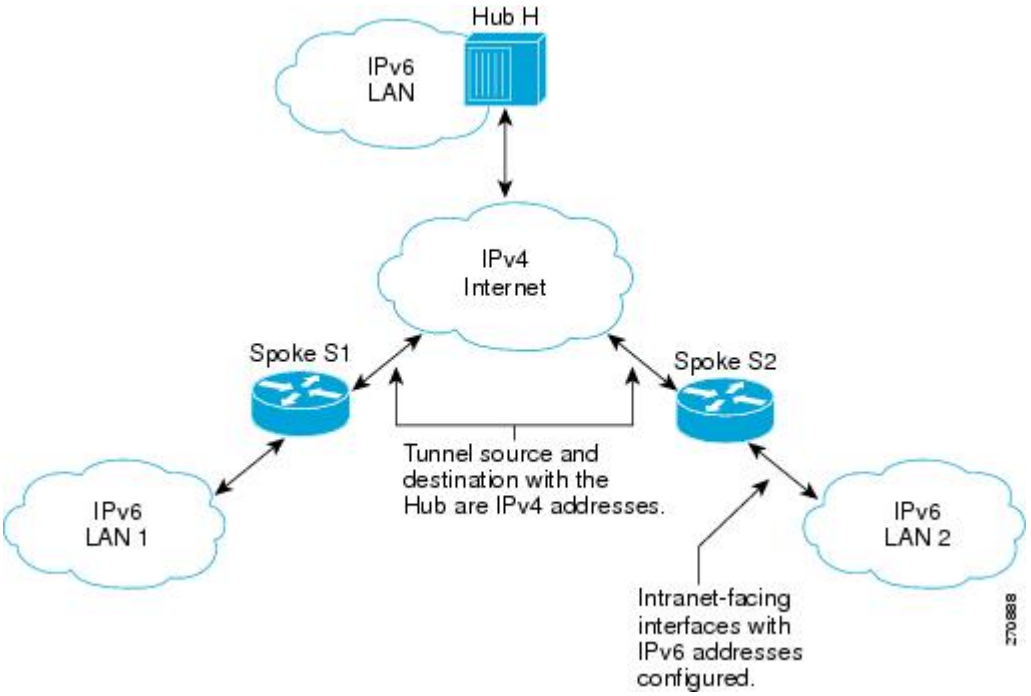
NHRP ルーティング

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 *4* : ***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。
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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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。

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。

	コマンドまたはアクション	目的

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。 （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 *2* : *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。

第 4 章

FQDN を使用した DMVPN 設定

FQDN を使用した DMVPN 設定機能により、ネクスト ホップ クライアント（NHC）をネクスト ホップ サーバ（NHS）に登録できます。

この機能を使用すると、スポーク（NHC）でハブ（NHS）の非ブロードキャスト マルチプル アクセス ネットワーク（NBMA）アドレスに完全修飾ドメイン名（FQDN）を設定することができます。スポークは DNS サービスを使用して FQDN を IP アドレスに解決し、新たに解決されたアドレスでハブに登録します。これにより、スポークは FQDN を使用してハブの IP アドレスをダイナミックに特定することができます。

この機能を使用すれば、スポークでハブのプロトコル アドレスを設定する必要はありません。スポークはハブの NHRP 登録応答からハブのプロトコル アドレスをダイナミックに学習します。RFC 2332 に従い、NHRP 登録を受信したハブは NHRP 登録応答に独自のプロトコル アドレスを含めて応答します。そのため、スポークは NHRP 登録応答パケットからハブのプロトコル アドレスを学習します。

Cisco IOS Release 15.1(2)T 以前のリリースでは、Dynamic Multipoint VPN（DMVPN）で NHS NBMA アドレスは IPv4 または IPv6 アドレスで設定されていました。NHS はダイナミック NBMA アドレスを受信するように設定されていたため、更新された NBMA アドレスを NHC が取得し、NHS に登録することは困難でした。FQDN を使用した DMVPN 設定機能により、この制限が解消されます。この機能を使用すると、NHC は IP アドレスではなく FQDN を使用してダイナミックに NBMA を設定し、NHS に登録することができます。

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。

FQDN を使用した DMVPN 設定の前提条件

Cisco IOS ドメイン ネーム システム（DNS）クライアントがスポークで使用可能である必要があります。

FQDN を使用した DMVPN 設定の制約事項

FQDN から解決された NBMA IP アドレスが、プロトコル アドレスを設定した NHS にマッピングされない場合、スポークをハブに登録することはできません。

FQDN を使用した DMVPN 設定について

DNS 機能

ドメイン ネーム システム（DNS）クライアントは DNS サーバと通信し、ホスト名を IP アドレスに変換します。

ルート上の中継 DNS サーバまたは DNS クライアントは、キャッシュに DNS サーバからの FQDN DNS応答をライフタイムにわたって格納します。DNS クライアントは、ライフタイムが期限切れになる前に別のクエリを受信した場合、キャッシュのエントリ情報を使用します。キャッシュが期限切れになると、DNS クライアントは DNS サーバにクエリーを送信します。NHS の NBMA アドレスが頻繁に変更される場合は、DNS エントリのライフタイムを短く設定する必要があります。ライフタイムが長いと、スポークが NHS の新しい NBMA アドレスを使い始めるまでに時間がかかる可能性があります。

DNS サーバの導入シナリオ

DNS サーバは、ハブ ネットワーク内またはハブ アンド スポーク ネットワークの外部に設置できます。

次に、DNS サーバのロード バランシング モデルを 4 つ示します。

- ラウンド ロビン：各 DNS 要求には、FQDN に設定されている IP アドレスのリストから IP アドレスが順番に割り当てられます。
- 重み付けラウンド ロビン：ラウンドロビン ロード バランシングに似ていますが、IP アドレスに重みとノードが割り当てられます。重み値が大きいほど、より多くの負荷やトラフィックを受け取ることができます。
- 地理またはネットワーク：地理別のロード バランシングでは、要求元に地理的に最も近いか、または最も効率のよい最適なノードに要求を転送できます。
- フェールオーバー：フェールオーバー ロード バランシングでは、ロード バランサが特定のノードを使用不可と判断するまで、すべての要求が単一のホストに送信されます。使用不可と判断された場合、トラフィックはリスト内の使用可能な次のノードに転送されます。

FQDN を使用した DMVPN 設定の設定方法

スポークでの DNS サーバの設定

スポークで DNS サーバを設定するには、次の作業を実行します。この作業は、外部 DNS サーバを使用して FQDN を解決する必要がある場合にのみ実行してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipname-server***ip-address*
4. **exit**

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**ipname-server***ip-address* 例： `Router(config)# ip name-server 192.0.2.1`	スポークで DNS サーバを設定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバルコンフィギュレーションモードを終了します。

DNS サーバの設定

DNSサーバを設定するには、次の作業を実行します。DNSサーバで設定を行う必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipdnsserver**
4. **iphost***hostnameip-address*
5. **exit**

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**ipdnsserver** 例： `Router(config)# ip dns server`	DNS サーバをイネーブルにします。
ステップ 4	**iphost***hostnameip-address* 例： `Router(config)# ip host host1.example.com 192.0.2.2`	DNS ビューの DNS ホスト名キャッシュで IP アドレスと FQDN（ホスト名）をマッピングします。 （注） スポークに DNS サーバが設定されている場合は、DNS サーバで **iphost** コマンドを設定します。スポークに DNS サーバが設定されていない場合は、このコマンドをスポークで設定します。「スポークでの DNS サーバの設定」を参照してください。
ステップ 5	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

プロトコル アドレスを使用した FQDN の設定

プロトコル アドレスを使用して FQDN を設定するには、次の作業を実行します。FQDN を設定する際は、NHS のプロトコル アドレスを把握しておく必要があります。この設定では、NBMA を使用してスポークをハブに登録します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipnhrpnhs***nhs-address* [**nbma** {*nbma-address* | *FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *number*]
5. **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： `Router> 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： `Router# 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： `Router(config)# interface tunnel 1`	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。
ステップ 4	**ipnhrpnhs***nhs-address* [**nbma** {*nbma-address* | *FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *number*] 例： `Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com multicast`	スポークをハブに登録します。 • 次の 2 つの方法でコマンドを設定できます。 • **ip nhrp nhs** *protocol-ipaddress* **nbma** *FQDN-string*：FQDN 文字列を使用してスポークをハブに登録する場合はこのコマンドを使用します。 • **ip nhrp nhs** *protocol-ipaddress* **nbma** *nbma-ipaddress*：NHS NBMA IP アドレスを使用してスポークをハブに登録する場合はこのコマンドを使用します。 （注） IPv6 アドレスを登録する場合は、**ipv6 nhrp nhs** *protocol-ipaddress* [**nbma** {*nhs-ipaddress* | *FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *number*] コマンドを使用できます。
ステップ 5	**end** 例： `Router(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。

NHS プロトコル アドレスを使用しない FQDN の設定

NHS プロトコル アドレスを使用せずに FQDN 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. **ipnhrpnhsdynamicnbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*]
5. **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： `Router> 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： `Router# 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： `Router(config)# interface tunnel 1`	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。
ステップ 4	**ipnhrpnhsdynamicnbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] 例： `Router(config-if)# ip nhrp nhs dynamic nbma examplehub.example1.com`	スポークをハブに登録します。 • NHS プロトコル アドレスはスポークによってダイナミックに取得されます。次の 2 つの方法でコマンドを設定できます。 • **ip nhrp nhs dynamic nbma** *FQDN-string*：FQDN 文字列を使用してスポークをハブに登録する場合はこのコマンドを使用します。 • **ip nhrp nhs dynamic nbma** *nbma-address*：NHS NBMA IP アドレスを使用してスポークをハブに登録する場合はこのコマンドを使用します。

	コマンドまたはアクション	目的
		（注） IPv6 アドレスを登録する場合は、**ipv6 nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] コマンドを使用できます。
ステップ 5	**end** 例： `Router(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 FQDN 設定の確認

ここでは、DMVPN FQDN 設定を確認するための情報を表示する方法を示します。次の **show** コマンドは任意の順序で実行できます。

手順の概要

1. **enable**
2. **showdmvpn**
3. **showipnhrpnhs**
4. **showrunning-configinterfacetunnel***tunnel-number*
5. **showipnhrpmulticast**

手順の詳細

ステップ 1 **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）。

例：

```
Router# enable
```

ステップ 2 **showdmvpn**
DMVPN 固有のセッション情報を表示します。

例：

```
Router# show dmvpn
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, W --> Waiting
```

```
        UpDn Time --> Up or Down Time for a Tunnel
================================================================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1       192.0.2.1         192.0.2.2 UP 00:00:12     S
               (h1.cisco.com)
```

ステップ 3 **showipnhrpnhs**

NHS のステータスを表示します。

例：

```
Router# show ip nhrp nhs
IPv4 Registration Timer: 10 seconds
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel1:
192.0.2.1 RE NBMA Address: 192.0.2.2 (h1.cisco.com) priority = 0 cluster = 0
```

ステップ 4 **showrunning-configinterfacetunnel***tunnel-number*

現在の実行コンフィギュレーションファイルまたはトンネルインターフェイス設定の内容を表示します。

例：

```
Router# show running-config interface tunnel 1
Building configuration...
Current configuration : 462 bytes
!
interface Tunnel1
 ip address 192.0.2.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication testing
 ip nhrp group spoke_group2
 ip nhrp network-id 123
 ip nhrp holdtime 150
 ip nhrp nhs dynamic nbma h1.cisco.com multicast
 ip nhrp registration unique
 ip nhrp registration timeout 10
 ip nhrp shortcut
 no ip route-cache cef
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 1001
 tunnel protection ipsec profile DMVPN
end
```

ステップ 5 **showipnhrpmulticast**

NHRP マルチキャスト マッピング情報を表示します。

例：

```
Route# show ip nhrp multicast
I/F     NBMA address
Tunnel1   192.0.2.1   Flags: nhs
```

FQDN を使用した DMVPN 設定の例

ローカル DNS サーバの設定例

次の例では、ローカル DNS サーバを設定する方法を示します。

```
enable
 configure terminal
  ip host host1.example.com 192.0.2.2
```

外部 DNS サーバの設定例

次の例では、外部 DNS サーバを設定する方法を示します。

スポーク

```
enable
 configure terminal
  ip name-server 192.0.2.1
```

DNS サーバ

```
enable
 configure terminal
  ip dns server
  ip host host1.example.com 192.0.2.2
```

プロトコル アドレスと NBMA アドレスを使用した NHS の設定例

次の例では、プロトコル アドレスと NBMA アドレスを使用して NHS を設定する方法を示します。

```
enable
 configure terminal
  interface tunnel 1
   ip nhrp nhs 192.0.2.1 nbma 209.165.200.225
```

プロトコル アドレスと FQDN を使用した NHS の設定例

次の例では、プロトコル アドレスと FQDN を使用して NHS を設定する方法を示します。

```
enable
 configure terminal
  interface tunnel 1
   ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

プロトコル アドレスを指定せずに NBMA アドレスを使用した NHS の設定例

次の例では、プロトコル アドレスを指定せずに NBMA アドレスを使用して NHS を設定する方法を示します。

```
enable
 configure terminal
  interface tunnel 1
   ip nhrp nhs dynamic nbma 192.0.2.1
```

プロトコル アドレスを指定せずに FQDN を使用した NHS の設定例

次の例では、プロトコル アドレスを指定せずに FQDN を使用して NHS を設定する方法を示します。

```
enable
 configure terminal
  interface tunnel 1
   ip nhrp nhs dynamic nbma examplehub.example1.com
```

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
DMVPN のコマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
この機能では、新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』

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

FQDN を使用した DMVPN 設定の機能情報

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 *3* : *FQDN* を使用した *DMVPN* 設定の機能情報

機能名	リリース	機能情報
FQDN を使用した DMVPN 設定	Cisco IOS XE Release 3.9S	FQDN を使用した DMVPN 設定機能により、NHC を NHS に登録できます。この機能では、NHS のプロトコル アドレスを使用せずに NHRP を使用します。 次のコマンドが導入または変更されました。 **cleardmvpnsession**、**debugnhrpcondition**、**ipnhrpnhs**、**ipv6nhrpnhs**

第 5 章

DMVPN トンネル ヘルス モニタリングと回復バックアップ NHS

DMVPN トンネル ヘルス モニタリングと回復（バックアップ NHS）機能を使用すると、Dynamic Multipoint Virtual Private Network（DMVPN）ハブへの接続数を制御できます。また、プライマリ ハブに接続できないときは代替ハブへの切り替えが可能です。

DMVPN トンネル ヘルス モニタリングと回復（バックアップ NHS）機能が提供する回復メカニズムでは、障害が発生したスポークツーハブ トンネルを別のアクティブなスポークツーハブ トンネルで置き換えることにより、スポークをそのトンネルパスから回復させます。スポークは、スポーク自体に設定されているネクスト ホップ サーバ（NHS）のリストから NHS（ハブ）を選択できます。NHS にプライオリティ値を設定して、スポークが NHS を選択する順序を制御できます。

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 トンネル ヘルス モニタリングと回復バックアップ NHS について

NHS の状態

NHSは、スポークツーハブ トンネルを形成するためにハブに関連付けられると同時に状態が変わります。次の表では、NHS の各種状態について説明します。

表 *4*：*NHS* の状態

状態	説明
DOWN	NHS はスケジューリングを待機しています。
PROBE	NHSは「DOWN」として宣言されていますが、「UP」にするためにスポークによるアクティブなプローブが継続されます。
UP	NHSはトンネルを確立するためにスポークに関連付けられています。

NHS のプライオリティ

NHS のプライオリティはハブに割り当てられる数値です。これによって、スポークがスポークツーハブ トンネルを確立する際にハブを選択する順序を制御します。プライオリティ値の範囲は 0 ～ 255 で、プライオリティは 0 が最も高く、255 が最も低くなります。

ハブのプライオリティは、次の方法で割り当てることができます。

- すべての NHS に一意のプライオリティを割り当てる。
- 一連の NHS に同じプライオリティ レベルを割り当てる。
- 1 台の NHS、一連の NHS、またはすべての NHS にプライオリティを指定しない（値 0）。

NHS 非クラスタ モデル

NHS 非クラスタ モデルとは、NHS にプライオリティ値を割り当て、NHS をグループに分類しないモデルです。NHS 非クラスタ モデルでは、すべての NHS を 1 つのデフォルト グループにまとめ、設定された最大 NHS 接続数に基づいて冗長接続を維持します。最大 NHS 接続数とは、クラスタ内で常時アクティブである必要がある NHS 接続の数です。最大 NHS 接続数の有効範囲は、0 ～ 255 です。

プライオリティ値をハブに割り当てて、スポークがスポークツーハブ トンネルを確立する際にハブを選択する順序を制御します。ただし、非クラスタ モデルでこれらのプライオリティを割り当てる場合は特定の制限があります。

次の表に、非クラスタ モデルでプライオリティを割り当てる際の制限の例を示します。

表 *5*：非クラスタ モデルの制限

最大接続数：3			
NHS	**NHS のプライオリティ**	**シナリオ 1**	**シナリオ 2**
NHS A1	1	UP	UP
NHS B1	1	UP	PROBE
NHS C1	1	UP	UP
NHS A2	2	DOWN	UP
NHS B2	2	DOWN	DOWN
NHS C2	2	DOWN	DOWN

A、B、および C の 3 つのデータセンターを使ったシナリオを想定します。各データセンターはそれぞれ 2 台の NHS で構成されています（NHS A1 と A2、NHS B1 と B2、および NHS C1 と C3）。

データセンターごとに 2 台の NHS が使用可能ですが、スポークが常時接続する NHS は各データセンターで 1 台のみです。したがって最大接続値は 3 に設定されています。つまり、3 つのスポークツーハブ トンネルが確立されます。たとえば、NHS B1 が非アクティブになった場合、NHS B1 に関連付けられたスポークツーハブ トンネルがダウンします。プライオリティ モデルに従い、次のプライオリティ値を持ち、キュー内の次に使用可能な NHS である NHS A2 が、スポークツーハブ トンネルを形成してアップ状態になります。ただし、この場合はトンネルを形成するスポークにデータセンター B のハブが関連付けられていないため、要件が満たされません。したがって、データセンター B への接続は確立されません。

この問題は、NHS を異なるグループに分類することで解決できます。各グループにグループ固有の最大接続値を設定できます。いずれのグループにも割り当てられていない NHS はデフォルト グループに属します。

NHS クラスタ

次の表にクラスタ機能の例を示します。さまざまなデータセンターに対応するNHSをグループ化してクラスタを形成します。NHS A1（プライオリティ 1）と NHS A2（プライオリティ 2）がクラスタ 1、NHS B1（プライオリティ 1）と NHS B2（プライオリティ 2）がクラスタ 2、NHS C1（プライオリティ 1）と NHS C2（プライオリティ 2）がクラスタ 3 としてそれぞれグループ化されています。NHS 7、NHS 8、および NHS 9 はデフォルト クラスタに属します。各クラスタの最大クラスタ値が 1 に設定されているため、4 つのクラスタのすべてで少なくとも 1 つのスポークツーハブ トンネルが常に確立されます。

シナリオ 1 では、それぞれのクラスタでプライオリティが最も高い NHS A1、NHS B1、および NHS C1 が UP 状態です。シナリオ 2 では、スポークと NHS A1 間の接続が切断され、スポークと NHS A2（同じクラスタのハブ）との間に接続が確立されます。プライオリティが最も高い NHS A1 は PROBE 状態になります。このように、常に 3 つのデータセンターへの接続がすべて確立されます。

表 *6*：クラスタの機能

NHS	NHS のプライオリティ	クラスタ	最大接続数	シナリオ 1	シナリオ 2
NHS A1	1	1	1	UP	PROBE
NHS A2	2			DOWN	UP
NHS B1	1	2	1	UP	UP
NHS B2	2			DOWN	DOWN
NHS C1	1	3	1	UP	UP
NHS C2	2			DOWN	DOWN
NHS 7	1	デフォルト	2	UP	DOWN
NHS 8	2			UP	UP
NHS 9	0			PROBE	UP

NHS Fallback Time

フォールバック時間とは、NHS がアクティブになるまでスポークが待機する時間です。この時間が経過した後、スポークはプライオリティの低いNHSとの接続を解除し、プライオリティが最も高い NHS に接続してスポークツーハブ トンネルを形成します。フォールバック時間を設定すると、過剰なフラップを回避できます。

次の表は、フォールバック時間がスポークで設定されていない場合に、スポークによってNHS間の過剰なフラップが発生する状態を示しています。スポークに接続してスポークツーハブ トンネルを形成できる NHS が 5 台あり、プライオリティはそれぞれ異なっています。これらの NHS はすべてデフォルト クラスタに属しています。最大接続数は 1 です。

表 *7*：フォールバック時間を設定しない場合の *NHS* の動作

NHS	NHS のプライオリティ	クラスタ	シナリオ 1	シナリオ 2	シナリオ 3	シナリオ 4	シナリオ 5
NHS 1	1	デフォルト	PROBE	PROBE	PROBE	PROBE	UP
NHS 2	2	デフォルト	PROBE	PROBE	PROBE	UP	DOWN
NHS 3	3	デフォルト	PROBE	PROBE	UP	DOWN	DOWN
NHS 4	4	デフォルト	PROBE	UP	DOWN	DOWN	DOWN
NHS 5	5	デフォルト	UP	DOWN	DOWN	DOWN	DOWN

シナリオ 1 では、プライオリティ値が最も低い NHS 5 がスポークに接続され、トンネルが確立されます。NHS 5 よりもプライオリティが高い他のすべての NHS は PROBE 状態です。

シナリオ 2 で NHS 4 がアクティブになると、スポークは既存のトンネルとの接続を解除して、NHS 4 との新しい接続を確立します。シナリオ 3 およびシナリオ 4 では、よりプライオリティが高いNHSがアクティブになると、スポークはただちに既存の接続を解除して新しいトンネルを確立します。シナリオ 5 では、プライオリティが最も高い NHS（NHS 1）がアクティブになっているため、スポークはこれに接続してトンネルを形成し、このNHSが非アクティブになるまで維持します。NHS 1 のプライオリティが最も高いので、他の NHS は PROBE 状態になりません。

次の表では、フォールバック時間の設定によって過剰なフラッピングを回避する方法を示します。最大接続数は 1 です。30 秒のフォールバック時間がスポークで設定されています。シナリオ 2 でスポークに関連付けられた NHS よりもプライオリティが高い NHS がアクティブになっても、フォールバック時間が経過するまでスポークは既存のトンネル接続を解除しません。したがってNHS 4 はアクティブになっていても、トンネルを形成せず、UP 状態にはなりません。NHS 4 はアクティブなままですが、フォールバック時間が経過するまでトンネルは形成されません。フォールバック時間が経過すると、スポークはアクティブなNHSの中でプライオリティが最も高いNHSに接続します。

これによって、より高いプライオリティのNHSがアクティブになるとすぐに発生するフラップを回避できます。

表 *8*：フォールバック時間を設定した場合の *NHS* の動作

NHS	NHS のプライオリティ	クラスタ	シナリオ 1	シナリオ 2	シナリオ 3	シナリオ 4	シナリオ 5
NHS 1	1	デフォルト	PROBE	PROBE	PROBE	UP（保持）	UP
NHS 2	2	デフォルト	PROBE	PROBE	UP（保持）	UP（保持）	DOWN
NHS 3	3	デフォルト	PROBE	UP（保持）	UP（保持）	UP（保持）	DOWN
NHS 4	4	デフォルト	UP（保持）	UP（保持）	UP（保持）	UP（保持）	DOWN
NHS 5	5	デフォルト	UP	UP	UP	UP	DOWN

NHS 回復プロセス

NHS回復とは、既存のトンネルが非アクティブになったときに代替スポークツーハブ トンネルを確立し、回復時に最適なハブに接続するプロセスのことです。

以降の項で NHS 回復について説明します。

代替スポークツーハブ NHS トンネル

スポークツーハブ トンネルに障害が発生した場合は、新しいスポークツーハブ トンネルでバックアップする必要があります。新しいNHSは、障害が発生したハブが属する同じクラスタから選択されます。これにより、1 つ以上のトンネル パスが使用できなくなっても、必要な数のスポークツーハブ トンネルが常に確保されます。

次の表に、NHS バックアップ機能の例を示します。

表 *9* : *NHS* バックアップ機能

NHS	NHSのプライオリティ	クラスタ	最大接続数	シナリオ 1	シナリオ 2	シナリオ 3
NHS A1	1	1	1	UP	PROBE	PROBE
NHS A2	2			DOWN	UP	DOWN
NHS A3	2			DOWN	DOWN	UP
NHS A4	2			DOWN	DOWN	DOWN
NHS B1	1	3	1	UP	PROBE	PROBE
NHS B2	2			DOWN	UP	DOWN
NHS B3	2			DOWN	DOWN	UP
NHS B4	2			DOWN	DOWN	DOWN
NHS 9	デフォルト	デフォルト	1	UP	UP	DOWN
NHS 10				DOWN	DOWN	UP

スポークツーハブ トンネルのセットアップに、クラスタ 1 およびクラスタ 3 に属する 4 台の NHS とデフォルト クラスタに属する 2 台の NHS を使用できます。すべての NHS にそれぞれのプライオリティが設定されています。最大接続数は 3 つのクラスタですべて 1 に設定されています。つまり、各クラスタの少なくとも 1 台の NHS が常にスポークに接続され、トンネルを形成する必要があります。

シナリオ 1 では、クラスタ 1 の NHS A1、クラスタ 3 の NHS B1、およびデフォルト クラスタの NHS 9 が UP です。これらはスポークとの通信を確立し、異なるスポークツーハブ トンネルを形成します。シナリオ 2 では、それぞれのクラスタでプライオリティが最も高い NHS A1 および NHS B1 が非アクティブになっています。そのため、次にプライオリティ値が高い NHS A2 および NHS B2 とスポークの間にトンネルが確立されます。ただしプライオリティが最も高いのは NHS A1 と NHS B1 であるため、スポークはこれらのプローブを継続します。したがって、NHS A1 と NHS B1 は PROBE 状態のままです。

シナリオ 3 では、NHS A2、NHS B2、および NHS 9 が非アクティブになっています。スポークは、PROBE 状態の NHS がアクティブになったかどうかを確認します。アクティブになっている場合、スポークはその NHS への接続を確立します。またはシナリオ 3 で示すように、PROBE 状態の NHS がどれもアクティブになっていない場合、スポークはクラスタ 1 の NHS A3 およびクラスタ 3 の NHS B3 に接続します。NHS A1 と NHS B1 は、スポークと接続してトンネルを形成し、UP 状態になるまで PROBE 状態のままです。

回復時に最適な NHS トンネルに戻る

スポークツーハブ トンネルに障害が発生すると、プライオリティ値が次に高い NHS を使用してバックアップ トンネルが確立されます。プライオリティ値が低い NHS でトンネルが確立された場合も、スポークはプライオリティ値が最も高いNHSのプローブを継続します。プライオリティ値が最も高い NHS がアクティブになると、スポークはその NHS とのトンネルを確立します。この結果、その NHS は UP 状態になります。

次の表に、NHS 回復機能を示します。スポークツーハブ トンネルのセットアップに、クラスタ 1 およびクラスタ 3 に属する 4 台の NHS とデフォルト クラスタに属する 2 台の NHS を使用できます。すべての NHS に異なるプライオリティが設定されています。最大接続値は 1 に設定されています。シナリオ 1 では、それぞれのクラスタでプライオリティが最も低い NHS A4、NHS B4、および NHS 10 が、トンネルを確立するスポークと関連付けられます。スポークは、プライオリティ値が最も高い NHS との接続を確立するために、より高いプライオリティを持つ NHS のプローブを継続します。したがってシナリオ 1 では、各クラスタでプライオリティ値が最も高い NHS の状態は PROBE です。シナリオ 2 では、アクティブな NHS A1 がスポークとのトンネルを形成して UP 状態になります。NHS A1 のプライオリティが最も高いので、スポークはクラスタ内の他の NHS をプローブしません。したがって、クラスタ 1 の他の NHS はすべて DOWN 状態です。

NHS B4 との接続が切断された場合、クラスタ 3 の NHS B1 がアクティブではないため、スポークはプライオリティ値が次に高い NHS B3 に接続します。シナリオ 3 では NHS A1 が引き続き UP 状態です。さらにクラスタ 3 でプライオリティが最も高い NHS B1 がアクティブになり、トンネルを形成して UP 状態になります。したがって、クラスタ 3 の他の NHS は PROBE 状態ではありません。ただし、デフォルト クラスタでプライオリティ値が最も低い NHS 10 が UP 状態であるため、スポークはクラスタ内で最も高いプライオリティを持つ NHS 9 のプローブを継続します。

シナリオ 4 では、NHS A1 と NHS B1 が引き続き UP 状態で、デフォルト クラスタで最も高いプライオリティを持つ NHS 9 が UP 状態になっています。これにより、各クラスタでそれぞれ最も高いプライオリティを持つ NHS とスポークが関連付けられるので、PROBE 状態の NHS はありません。

表 *10*：*NHS* 回復機能

NHS	NHS のプライオリティ	クラスタ	最大接続数	シナリオ 1	シナリオ 2	シナリオ 3	シナリオ 4
NHS A1	1	1	1	PROBE	UP	UP	UP
NHS A2	2			DOWN	DOWN	DOWN	DOWN
NHS A3	2			DOWN	DOWN	DOWN	DOWN
NHS A4	2			UP	DOWN	DOWN	DOWN

NHS	NHSのプライオリティ	クラスタ	最大接続数	シナリオ 1	シナリオ 2	シナリオ 3	シナリオ 4
NHS B1	1	3	1	PROBE	PROBE	UP	UP
NHS B2	10			PROBE	DOWN	DOWN	DOWN
NHS B3	10			PROBE	UP	DOWN	DOWN
NHS B4	30			UP	DOWN	DOWN	DOWN
NHS 9	デフォルト	デフォルト	1	PROBE	PROBE	PROBE	UP
NHS 10	100			UP	UP	UP	DOWN

DMVPN トンネル ヘルス モニタリングと回復バックアップ NHS の設定方法

NHS クラスタの最大接続数の設定

NHS クラスタの必要な最大接続数を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipnhrpnhscluster***cluster-number***max-connections***value*

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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： `Router(config)# interface tunnel 1`	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。
ステップ 4	**ipnhrpnhscluster***cluster-number***max-connections***value* 例： `Router(config-if)# ip nhrp nhs cluster 5 max-connections 100`	必要な最大接続数を設定します。 （注） IPv6 設定の場合は、**ipv6 nhrp nhs cluster** *cluster-number* **max-connections** *value* コマンドを使用します。

NHS フォールバック時間の設定

NHS フォールバック時間を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipnhrpnhsfallback***fallback-time*

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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： `Router(config)# interface tunnel 1`	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。
ステップ 4	**ipnhrpnhsfallback***fallback-time* 例： `Router(config-if)# ip nhrp nhs fallback 25`	NHS フォールバック時間を設定します。 （注） IPv6 設定の場合は、**ipv6 nhrp nhs fallback** *fallback-time* コマンドを使用します。

NHS のプライオリティ値とグループ値の設定

NHS のプライオリティ値とグループ値を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipnhrpnhs***nhs-address***priority***nhs-priority***cluster***cluster-number***

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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： `Router(config)# interface tunnel 1`	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。
ステップ 4	**ipnhrpnhs***nhs-address***priority***nhs-priority***cluster***cluster-number* 例： `Router(config-if)# ip nhrp nhs 172.0.2.1 priority 1 cluster 2`	必要なプライオリティ値とクラスタ値を設定します。 （注） IPv6 設定の場合は、**ipv6 nhrp nhs** *nhs-address* **priority** *nhs-priority* **cluster** *cluster-number* コマンドを使用します。

DMVPN トンネル ヘルス モニタリングと回復バックアップ NHS 機能の確認

DMVPN トンネル ヘルス モニタリングと回復（バックアップ NHS）機能の設定に関する情報を表示および確認するには、次の作業を実行します。次の **show** コマンドを任意の順序で実行できます

手順の概要

1. **enable**
2. **showipnhrpnhs**
3. **showipnhrpnhsredundancy**
4. **showipv6nhrpnhs**
5. **showipv6nhrpnhsredundancy**

手順の詳細

ステップ 1 **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）。

例：

```
Router# enable
```

ステップ 2 **showipnhrpnhs**

NHRP NHS 情報を表示します。

例：

```
Router# show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.0.0.1 RE priority = 0 cluster = 0
```

ステップ 3 **showipnhrpnhsredundancy**

NHRP NHS 回復情報を表示します。

例：

```
Router# show ip nhrp nhs redundancy
Legend: E=Expecting replies, R=Responding, W=Waiting
No.  Interface  Cluster  NHS          Priority  Cur-State  Cur-Queue  Prev-State Prev-Queue
1    Tunnel0    0        10.0.0.253   3         RE         Running    E          Running
2    Tunnel0    0        10.0.0.252   2         RE         Running    E          Running
3    Tunnel0    0        10.0.0.251   1         RE         Running    E          Running
No.  Interface  Cluster  Status   Max-Con Total-NHS Responding Expecting Waiting Fallback
1    Tunnel0    0        Enable   3       3         3          0         0       0
```

ステップ 4 **showipv6nhrpnhs**

IPv6 固有の NHRP NHS 情報を表示します。

例：

```
Router# show ipv6 nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
2001::101 RE priority = 1 cluster = 5
```

ステップ 5 **showipv6nhrpnhsredundancy**

IPv6 固有の NHRP NHS 回復情報を表示します。

例：

```
Router# show ipv6 nhrp nhs redundancy
Legend: E=Expecting replies, R=Responding, W=Waiting
No.  Interface  Cluster  NHS          Priority  Cur-State  Cur-Queue  Prev-State Prev-Queue
1    Tunnel0    5        2001::101    1         E          Running     RE         Running
No.  Interface  Cluster  Status  Max-Con  Total-NHS Responding Expecting Waiting Fallback
1    Tunnel0    5        Disable Not Set  1         0          1         0       0
```

DMVPN トンネル ヘルス モニタリングと回復バックアップ NHS の設定例

NHS クラスタの最大接続数の設定例

次の例では、クラスタ 0 に属する 3 台の NHS について「max-connections」値を 3 に設定する方法を示します。

```
interface tunnel 0
 bandwidth 1000
 ip address 10.0.0.1 255.0.0.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.0.2.1
 ip nhrp map 10.0.0.253 172.0.2.1
 ip nhrp map multicast 172.0.2.2
 ip nhrp map 10.0.0.251 172.0.2.2
 ip nhrp map multicast 172.0.2.3
 ip nhrp map 10.0.0.252 172.0.2.3
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.252 priority 2
 ip nhrp nhs 10.0.0.251 priority 1
 ip nhrp nhs 10.0.0.253 priority 3
 ip nhrp nhs cluster 0 max-connections 3

 ip nhrp shortcut
 delay 100
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
 !
!
```

NHS フォールバック時間の設定例

次の例では、NHS フォールバック時間を 25 秒に設定する方法を示します。

```
configure terminal
 interface tunnel 1
  ip nhrp nhs fallback 25
```

NHS のプライオリティ値とグループ値の設定例

次の例では、NHS を複数のクラスタにグループ化し、各クラスタに異なる最大接続値を指定する方法を示します。

```
Configure terminal
 interface tunnel 0
  ip nhrp nhs 10.0.0.251 priority 1 cluster  1
  ip nhrp map 10.0.0.251 192.0.2.4
```

```
  ip nhrp map multicast 192.0.2.4
  end
configure terminal
 interface tunnel 0
  ip nhrp nhs 10.0.0.252 priority 2 cluster  2
  ip nhrp map 10.0.0.252 192.0.2.5
  ip nhrp map multicast 192.0.2.5
  end
configure terminal
 interface tunnel 0
  ip nhrp nhs 10.0.0.253 priority 3 cluster  3
  ip nhrp map 10.0.0.253 192.0.2.6
  ip nhrp map multicast 192.0.2.6
  end
configure terminal
 interface tunnel 0
  ip nhrp nhs cluster 1 max 1
  ip nhrp nhs cluster 2 max 1
  ip nhrp nhs cluster 3 max 1
  end
```

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
DMVPNのコマンド構文、コマンドモード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
この機能では、新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能では、新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次のURLにある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。	--

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 トンネル ヘルス モニタリングと回復バックアップ NHS 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 *11* : *DMVPN* トンネル ヘルス モニタリングと回復バックアップ *NHS* の機能情報

機能名	リリース	機能情報
DMVPN トンネル ヘルス モニタリングと回復（バックアップ NHS）	Cisco IOS XE Release 3.9S	DMVPN トンネル ヘルス モニタリングと回復（バックアップ NHS）機能を使用すると、DMVPN ハブへの接続数を制御できます。また、プライマリ ハブに接続できないときは代替ハブへの切り替えが可能です。 次のコマンドが導入または変更されました。**ipnhrpnhs**、**ipv6nhrpnhs**、**showipnhrpnhs**、**showipv6nhrpnhs**

第 6 章

DHCP トンネル サポート

DHCP トンネル サポート機能では、DHCP を使用して総称ルーティング カプセル化（GRE）トンネル インターフェイスのノード（またはスポーク）をダイナミックに設定できます。

Dynamic Multipoint VPN（DMVPN）ネットワークに参加している各スポークには、同じ IP サブネットに属している一意の IP アドレスが必要です。大規模な DMVPN ネットワークでは、ネットワーク管理者がスポーク アドレスを手動で設定することは困難です。したがって、DHCP を使用して DMVPN ネットワークでスポーク アドレスをダイナミックに設定します。

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。

DHCP トンネル サポートの制約事項

- DHCP サーバは DMVPN ハブに導入できません。DMVPN ハブがリレー エージェントとして機能し、DHCP サーバは DMVPN ハブに隣接して導入される必要があります。
- アドレス検証の DHCP 機能は DMVPN ではサポートされていません。

DHCP トンネル サポートについて

DHCP の概要

DHCP はブートストラップ プロトコル（BOOTP）に基づいており、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。DHCP により、再利用可能なネットワーク アドレスおよび設定オプションをインターネット ホストに自動的に割り当てられるようになります。DHCP は 2 つのコンポーネントで構成されます。1 つはホスト固有の設定パラメータを DHCP サーバからホストに配信するためのプロトコルで、もう 1 つはホストにネットワーク アドレスを割り当てるためのメカニズムです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバ ホストが、ダイナミックに設定されるホストに対して、ネットワーク アドレスを割り当て、設定パラメータを提供します。詳細については、『*Cisco IOS IP Addressing Configuration Guide*』の「DHCP」の項を参照してください。

トンネル ネットワークでの DHCP の動作

DMVPN スポーク ノードは、事前設定された DMVPN ネクスト ホップ サーバ（NHS）（ハブ ノード）とのトンネルを確立し、トンネル インターフェイスで IP アドレスが設定される前に NHS と IP パケットを交換します。これにより、スポーク上の DHCP クライアント、および NHS 上の DHCP リレー エージェントまたは DHCP サーバが DHCP メッセージを送受信できます。DHCP リレー エージェントとは、クライアントとサーバ間で DHCP パケットを転送するホストです。

スポークのトンネルが UP 状態であるか、アクティブになっている場合、スポークは事前設定されたハブ ノードとのトンネルを確立します。トンネルの形成時に、スポークとハブ間のトンネルに対して IP Security（IPsec）暗号化が設定される場合があります。スポークがハブとのトンネルを確立した後にのみ、DHCP は GRE トンネル インターフェイス UP 通知を受信します。スポークで設定された DHCP クライアントは、ハブ（DHCP リレー エージェントまたはサーバ）と DHCP IP パケットを交換して、GRE トンネル インターフェイスの IP アドレスを取得する必要があります。したがって、GRE トンネル インターフェイス UP 通知が DHCP サーバまたはリレー エージェントに送信される前に、スポーク ツーハブ トンネルがアクティブ状態になっている必要があります。

DMVPN スポークでブロードキャストされる IP パケットは DMVPN ハブに到達します。スポークは、GRE トンネル インターフェイスの IP アドレスを取得する前に、DMVPN ハブ上の DHCP リレー エージェントに DHCPDISCOVER メッセージをブロードキャストします。DHCP は、

DHCPDISCOVERメッセージを使用してクライアントにオファーをユニキャストします。ハブは、スポークから Next Hop Resolution Protocol（NHRP）登録を受信しないとスポークに IP パケットを送信できません。DMVPN ハブで設定された DHCP リレー エージェントは、DHCP クライアント パケット（DHCPDISCOVER および DHCPREQUEST）にマッピング情報を追加します。DHCP クライアントに追加されたマッピング情報は、DMVPN ハブが DHCP サーバ応答をリレーするために使用できます。

（注） DHCP が GRE トンネル インターフェイスのアドレスを取得するまで、スポークから送信される NHRP 登録は制限されます。そのため、信頼できる標準 DHCP メッセージの交換が可能になります。

DHCP リレー エージェントとしての DMVPN ハブ

リレーエージェントがなくても DHCP は動作できます。リレーエージェントは、DHCP クライアントおよびサーバが別のサブネットにある場合にのみ使用されます。リレー エージェントは、DHCP クライアントとサーバ間の通信チャネルとして機能します。DHCP トンネル サポート機能では、DMVPN ハブが DHCP サーバに DHCP メッセージをリレーするリレー エージェントとして機能する必要があります。

DHCP サーバは DMVPN ネットワークの外部にあり、DMVPN ハブ ノードから物理パスを介してアクセスできます。スポーク ノードは、ハブツースポーク トンネル（GRE トンネル）を通って DHCP サーバに到達します。DHCP サーバに DMVPN スポークから直接到達することはできません。DMVPN ハブ上の DHCP リレー エージェントは、スポーク上の DHCP クライアントと DHCP サーバ間で DHCP プロトコル メッセージを交換する際に役立ちます。

DMVPN トポロジ

デュアルハブ シングル DMVPN トポロジ

デュアルハブ シングル DMVPN トポロジでは、DMVPN 冗長性を維持するハイ アベイラビリティ（HA）サポートを備えた同じ DHCP サーバに両方のハブを接続する必要があります。ハブを異なる DHCP サーバに接続する場合は、相互に排他的な IP アドレス プールをアドレス割り当て用に設定する必要があります。

デュアルハブ デュアル DMVPN トポロジ

デュアルハブ デュアル DMVPN トポロジでは、各ハブが別々の DHCP サーバに接続されます。DMVPN ハブ（DHCP リレー エージェント）は、リレーされた DHCP 要求にクライアント側のトンネル IP アドレスを含めます。DHCP 要求は、DHCP サーバが正しいプールから IP アドレスを割り当てるために使用されます。

階層型 DMVPN トポロジ

DMVPN の階層型トポロジでは、DMVPN ハブに複数のレベルがあります。ただしトンネル インターフェイスの IP アドレスは、すべて同一の IP サブネット アドレスから割り当てられます。DHCP クライアントのブロードキャスト パケットは、直接接続されたハブにブロードキャストされます。そのため、すべてのレベルの DMVPN ハブは、DHCP サーバまたは DHCP リレー エージェントのいずれかである必要があります。DHCP サーバを使用する場合、サーバのデータベースを同期する必要があります。DMVPN ハブは、DHCP クライアント パケットを中央の DHCP サーバに転送する DHCP リレー エージェントとして設定する必要があります。DHCP サーバが中央ハブに配置されている場合、すべての DHCP ブロードキャストはリレー エージェントでリレーされて DHCP サーバに到達します。

DHCP トンネル サポートの設定方法

DHCP 応答をユニキャストするための DHCP リレー エージェントの設定

DHCP 応答をユニキャストするように DHCP リレー エージェントを設定するには、次の作業を実行します。

デフォルトでは、DHCP 応答は DMVPN ハブからスポークにブロードキャストされます。このため、帯域幅のバーストが発生します。DHCP トンネル サポート機能は、DHCP メッセージがブロードキャストされると機能しません。したがって、DHCP を DMVPN 環境で機能させるには、DHCP リレー エージェントが DHCP メッセージをユニキャストするように設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipdhcpsupporttunnelunicast**
4. **exit**

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**ipdhcpsupporttunnelunicast** 例： `Router(config)# ip dhcp support tunnel unicast`	DMVPN ネットワーク上で DHCP 応答をユニキャストするスポークツーハブ トンネルを設定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

ブロードキャスト フラグをクリアするための DMVPN スポークの設定

ブロードキャスト フラグをクリアするように DMVPN スポークを設定するには、次の作業を実行します。

DMVPN スポークは、デフォルトで DHCP の DISCOVER および REQUEST メッセージにブロードキャスト フラグを設定します。そのため DHCP リレー エージェントは、DHCP 応答をユニキャストするために必要な情報がそろっていても、DHCP 応答をスポークにブロードキャストせざるを得ません。したがって、DMVPN スポークからのブロードキャスト フラグをクリアする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipdhcpclientbroadcast-flagclear**
5. **exit**

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： `Router> 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： `Router# 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： `Router(config)# interface tunnel 1`	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。
ステップ 4	**ipdhcpclientbroadcast-flagclear** 例： `Router(config-if)# ip dhcp client broadcast-flag clear`	ブロードキャスト フラグをクリアするように DHCP クライアントを設定します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	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、グローバル コンフィギュレーション モードに戻ります。

DHCP トンネル サポートの設定例

DHCP 応答をユニキャストするための DHCP リレー エージェントの設定例

次の例では、DHCP 応答をユニキャストするように DHCP リレー エージェントを設定する方法を示します。

```
Device# configure terminal
Device(config)# ip dhcp support tunnel unicast
Device(config)# exit
```

ブロードキャスト フラグをクリアするための DMVPN スポークの設定例

次の例では、ブロードキャスト フラグをクリアするように DMVPN スポークを設定する方法を示します。

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip dhcp client broadcast-flag clear
Device(config-if)# exit
```

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Cisco IOS IP アドレッシング設定作業	『*Cisco IOS IP Addressing Configuration Guide*』
Cisco IOS IP アドレッシング サービス コマンド	『*Cisco IOS IP Addressing Services Command Reference*』

標準

規格	タイトル
--	この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2131	*Dynamic Host Configuration Protocol*

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

DHCP トンネル サポートの機能情報

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 *12* : ***DHCP*** トンネル サポートの機能情報

機能名	リリース	機能情報
DHCP トンネル サポート	Cisco IOS XE Release 3.9S	DHCP トンネル サポート機能では、DHCP を使用して GRE トンネル インターフェイスのノード（またはスポーク）をダイナミックに設定できます。 Cisco IOS XE Release 3.9S では、Cisco 4400 シリーズ サービス統合型ルータおよび Cisco CSR 1000V シリーズ クラウド サービス ルータにこの機能が実装されました。 Cisco IOS XE Release 3.13S では、Cisco 4300 シリーズ サービス統合型ルータでのサポートが追加されました。 次のコマンドが導入または変更されました。**ip address dhcp**、**ip dhcp client broadcast-flag**、**ip dhcp support tunnel unicast**

第 7 章

DMVPN トンネル ヘルス モニタリングと回復

ダイナミック マルチポイント VPN（DMVPN）トンネル ヘルス モニタリングと回復機能により、システムで DMVPN イベントをモニタおよびレポートする機能が強化されます。この機能には、重要な DMVPN イベントに対する簡易ネットワーク管理プロトコル（SNMP）Next Hop Resolution Protocol（NHRP）通知のサポートと、DMVPN Syslog メッセージのサポートが組み込まれています。また、この機能を使用することで、DMVPN トンネルの正常性に基づいて、システムでトンネル インターフェイスの状態を制御できます。

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 トンネル ヘルス モニタリングと回復の前提条件

SNMP NHRP 通知

- SNMP がシステム上でイネーブルにされている必要があります。
- Get 操作および Set 操作と通知に対する一般的な SNMP 設定をシステム上に実装する必要があります。
- 関連するすべての NHRP トラップがイネーブルにされている必要があります。

DMVPN トンネル ヘルス モニタリングと回復の制約事項

MIB SNMP

- SNMP SET UNDO はサポートされていません。
- リロード後に MIB-SNMP データが維持される、MIB の持続機能はサポートされていません。ただし MIB 通知コントロール オブジェクトについては、その情報がコンフィギュレーション コマンドライン インターフェイス（CLI）からもキャプチャされているため仮想持続が行われます。
- 通知と Syslog は仮想ルーティングおよび転送（VRF）対応ではありません。
- レート制限を超えたことを示す通知に、IPv4 と IPv6 のプロトコル タイプでの違いはありません。

インターフェイス状態の制御

- インターフェイス状態の制御は、リーフ スポーク ノードでだけ設定できます。
- インターフェイス状態の制御では、IPv4 だけがサポートされています。

DMVPN トンネル ヘルス モニタリングと回復について

NHRP 拡張 MIB

NHRP 拡張 MIB モジュールは、クライアントとサーバの両方のためのリダイレクト関連の統計情報を管理するオブジェクトと、次のような重要な DMVPN イベントのための SNMP 通知を管理するオブジェクトから構成されます。

- スポークはハブがダウンしたことを感知します。これは、スポークが以前ハブに登録されていない場合にも発生します。
- スポークが正常にハブに登録されます。
- ハブはスポークがダウンしたことを感知します。
- ハブはスポークが活動化したことを感知します。
- スポークまたはハブは、NHRP 登録によって関連付けられていない別の NHRP ピアがダウンしたことを感知します。たとえば、スポークとスポークとの間のトンネルがダウンする場合です。
- スポークまたはハブは、NHRP 登録によって関連付けられていない別の NHRP ピアが活動化したことを感知します。たとえば、スポークとスポークとの間のトンネルが活動化する場合です。
- インターフェイス上で NHRP パケットに対して設定されたレート制限を超えています。

MIB のエージェントの実装によって、特定のトラップをネットワーク管理システムまたは CLI からイネーブルまたはディセーブルにする手段が提供されます。

DMVPN Syslog メッセージ

DMVPN Syslog 機能を使用すると、次のイベントの Syslog メッセージを出力できます。

- すべてのネクスト ホップ状態イベント。たとえば、システムでネクスト ホップ サーバ（NHS）、ネクスト ホップ クライアント（NHC）、またはネクスト ホップ ピア（NHP）が活動化している、またはダウンしていることが宣言されたときです。これらのメッセージの重大度レベルは重要として設定されます。
- NHRP 解決イベント。たとえば、スポークが解決をリモート スポークに対して送信するとき、または NHRP 解決が応答を受信せずにタイムアウトしたときです。これらのメッセージの重大度レベルは情報として設定されます。
- DMVPN 暗号法イベント。たとえば、DMVPN ソケット エントリがオープンからクローズ、またはクローズからオープンに変更されたときです。これらのメッセージの重大度レベルは通知として設定されます。

- NHRP エラー通知。たとえば、NHRP 登録または解決イベントが失敗したとき、システム チェック イベントが失敗したとき、またはNHRP カプセル化エラーが発生したときにNHRP エラー通知が表示されます。これらのメッセージの重大度レベルはエラーとして設定されます。
  以下に、NHRP エラー メッセージの例を示します。

  Received Error Indication from 209.165.200.226, code: administratively prohibited(4), (trigger src: 209.165.200.228 (nbma: 209.165.200.230) dst: 209.165.202.140), offset: 0, data: 00 01 08 00 00 00 00 00 00 FE 00 68 F4 03 00 34

  エラー メッセージには、エラーが発生したノードの IP アドレス、送信元非ブロードキャスト マルチアクセス（NBMA）、および宛先アドレスが含まれています。

- DMVPN エラー通知。たとえば、NET_ID 値が設定されていないとき、または NHRP マルチキャストのレプリケーション エラーが発生したときです。重大度レベルは、NET_ID 値メッセージが設定されていない場合は通知に設定され、NHRP マルチキャストのレプリケーション エラーが発生した場合はエラーに設定されます。

- インターフェイス上でNHRPパケットに対して設定されたレート制限を超えています。このイベントは、NHRP プロセスで処理される NHRP パケットが、インターフェイス上に設定されているレート制限を超えたときに発生します。これらのメッセージの重大度レベルは警告として設定されます。

インターフェイス状態の制御

インターフェイス状態の制御機能を使用すると、インターフェイス上のトンネルが活動化しているかどうかに基づいて、NHRP でインターフェイスの状態を制御できます。インターフェイス上に設定されたすべての NHS がダウンしている状態にあることが NHRP で検出された場合、NHRP によってインターフェイスの状態がダウンに変更されます。しかし、インターフェイス上に設定されたいずれかのNHSが活動化していることがNHRPで検出された場合、状態は活動化に変更されます。

NHRP でインターフェイスの状態が変更された場合、その他のシスコ サービスは、状態の変化に応じて次のように対応できます。

- インターフェイスの状態が変更された場合、総称ルーティング カプセル化（GRE）インターフェイスで LinkUp メッセージまたは LinkDown メッセージを報告する IF-MIB 通知（トラップ）が生成されます。これらのトラップを使用し、システムで DMVPN クラウドに対する接続が監視されます。

- インターフェイスの状態がダウンに変更された場合、Cisco IOS バックアップ インターフェイス機能が開始され、エラーになったプライマリ パスの代替パスを提供するための別のインターフェイスがシステムで使用されるようにできます。

- インターフェイスの状態がダウンに変更された場合、すべてのダイナミック ルーティング プロトコルに送信されるアップデートがシステムで生成されます。インターフェイス状態の制御機能は、マルチポイント GRE（mGRE）インターフェイスがダウンした際にダイナミック ルーティングを行うフェールオーバー メカニズムを提供します。

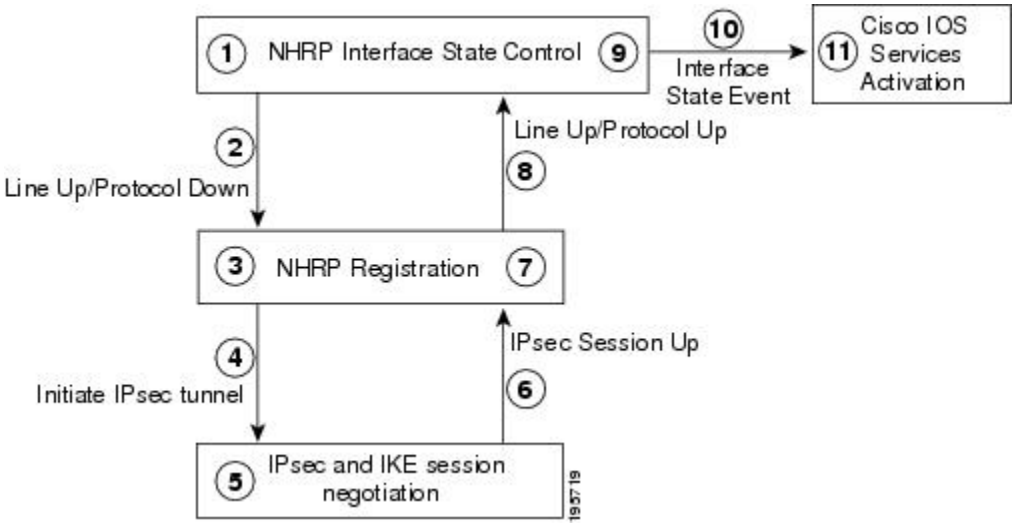
- インターフェイスの状態がダウンに変更された場合、mGREをネクストホップとして使用するすべてのスタティックルートがシステムでクリアされます。インターフェイス状態の制御機能は、mGREインターフェイスがダウンした際にルーティングを行うフェールオーバーメカニズムを提供します。

インターフェイス状態の制御機能は、ポイントツーポイントインターフェイスとmGREインターフェイスの両方で動作します。

インターフェイス状態の制御の設定ワークフロー

次の図に、インターフェイス状態の制御機能を初期化する際のシステムの動作を示します。

図 *5*：インターフェイス状態の制御設定の初期化ワークフロー



インターフェイス状態の制御の初期化は次のように動作します。

1. インターフェイス状態の制御機能は、GREインターフェイスのNHRP設定でイネーブルに設定されます。
2. システムでプロトコル状態が再評価され、設定されたNHSに応答するものがない場合に、ラインのアップとプロトコルのダウンに状態が変更されます。
3. ラインのアップ状態の変更によって、NHRP登録プロセスが開始されます。
4. NHRP登録プロセスでIPsecトンネルが開始されます。
5. IPsecトンネルの開始によって、IPsecとIKEトンネルのネゴシエーションプロセスが開始されます。
6. トンネルのネゴシエーションプロセスが正常に完了したら、システムでIPsecセッションアップ メッセージがシステムが送信されます。
7. NHRP登録プロセスでIPsecセッション アップ メッセージが受信されます。

8 NHRP 登録プロセスで、ラインのアップとプロトコルのアップ状態が GRE インターフェイスに対して報告されます。

9 GRE インターフェイス状態がラインのアップとプロトコルのアップに変更されます。

10 システムによって、GREインターフェイス状態の変更がシスコ ソフトウェアに報告されます。

11 状態の変更に伴い、インターフェイスイベント通知、Syslogイベント、DHCPの更新、IPルートのリフレッシュ、SNMP トラップなどのシスコ サービスがトリガーされます。

DMVPN トンネル ヘルス モニタリングと回復の設定方法

DMVPN トンネル ヘルス モニタリングと回復機能を使用すると、SNMP NHRP 通知とインターフェイス状態を設定できます。

SNMP NHRP 通知を生成するためのインターフェイスの設定

NHRP イベントに対して SNMP NHRP トラップが生成されるように、インターフェイスを設定できます。さらに、システムからトラップが特定のトラップ レシーバに送信されるように設定できます。SNMP NHRP 通知をインターフェイス上で設定するには、ここで説明する手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-servercommunity***string***rw**
4. **snmp-serverenabletrapsnhrpnhs**
5. **snmp-serverenabletrapsnhrpnhc**
6. **snmp-serverenabletrapsnhrpnhp**
7. **snmp-serverenabletrapsnhrpquota-exceeded**
8. **snmp-serverhost***ip-address***version***snmpversioncommunity-string*
9. **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）。

	コマンドまたはアクション	目的
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	**snmp-servercommunity***string***rw** 例： `Device(config)# snmp-server community public rw`	SNMPへのアクセスを許可するように、コミュニティ アクセス ストリングを設定します。
ステップ 4	**snmp-serverenabletrapsnhrpnhs** 例： `Device(config)# snmp-server enable traps nhrp nhc`	NHRP NHS 通知をイネーブルにします。
ステップ 5	**snmp-serverenabletrapsnhrpnhc** 例： `Device(config)# snmp-server enable traps nhrp nhc`	NHRP NHC 通知をイネーブルにします。
ステップ 6	**snmp-serverenabletrapsnhrpnhp** 例： `Device(config)# snmp-server enable traps nhrp nhc`	NHRP NHP 通知をイネーブルにします。
ステップ 7	**snmp-serverenabletrapsnhrpquota-exceeded** 例： `Device(config)# snmp-server enable traps nhrp quota-exceeded`	NHRPパケットに対して設定されたレート制限がインターフェイス上で超過した場合の通知をイネーブルにします。
ステップ 8	**snmp-serverhost***ip-address***version***snmpversioncommunity-string* 例： `Device(config)# snmp-server host 192.40.3.130 version 2c public`	SNMP 通知動作の指定 • デフォルトでは、SNMP通知はトラップとして送信されます。 • すべての NHRP トラップは、public コミュニティ ストリングを使用して IP アドレス 192.40.3.130 と一緒に通知レシーバに送信されます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config)# end`	現在の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。

トラブルシューティングのヒント

SNMP NHRP 通知のトラブルシューティングを行うには、**debugsnmpmibnhrp** コマンドを使用します。

インターフェイス上でのインターフェイス状態の制御の設定

インターフェイス状態の制御機能を使用することで、インターフェイスに接続されているDMVPNトンネルが活動中かどうかに基づき、システムでインターフェイスの状態を制御するようにできます。インターフェイス上でのインターフェイス状態の制御を設定するには、ここで説明する手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **if-statenhrp**
5. **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	**interface***typenumber* 例： `Device(config)# interface tunnel 1`	インターフェイス タイプを設定し、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。
ステップ 4	**if-statenhrp** 例： `Device(config-if)# if-state nhrp`	トンネルインターフェイスの状態を制御するためのNHRPをイネーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	現在の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 トンネル ヘルス モニタリングと回復の設定例

例：SNMP NHRP 通知の設定

次の例は、ハブまたはスポーク上の SNMP NHRP 通知の設定方法を示します。

```
Device(config)# snmp-server community public rw
Device(config)# snmp-server enable traps nhrp nhs
Device(config)# snmp-server enable traps nhrp nhc
Device(config)# snmp-server enable traps nhrp nhp
Device(config)# snmp-server enable traps nhrp quota-exceeded
Device(config)# snmp-server host 209.165.200.226 version 2c public
```

例：インターフェイス状態の制御の設定

次の例は、スポークに対するインターフェイス状態の制御機能の設定方法を示します。

```
interface Tunnel 1
 ip address 209.165.200.228 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map 209.165.201.2 209.165.201.10
 ip nhrp map 209.165.201.3 209.165.201.11
 ip nhrp map multicast 209.165.201.10
 ip nhrp map multicast 209.165.201.11
 ip nhrp network-id 1
 ip nhrp holdtime 90
 ip nhrp nhs 209.165.201.3
 ip nhrp nhs 209.165.201.2
```

```
 ip nhrp shortcut
 if-state nhrp
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 !
end
```

DMVPN トンネル ヘルス モニタリングと回復の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
ダイナミック マルチポイント VPN 情報	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Dynamic Multipoint VPN (DMVPN)」の章
IKE の設定作業（IKE ポリシーの定義など）	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」の章
IPsec の設定作業	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」の章
システム メッセージ	『*System Messages Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』
RFC 2677	『*Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)*』

MIB

MIB	MIB のリンク
• CISCO-NHRP-EXT-MIB • NHRP-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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 トンネル ヘルス モニタリングと回復の機能情報

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 *13*：トンネル ヘルス モニタリングと回復の機能情報

機能名	リリース	機能情報
DMVPN：トンネル ヘルス モニタリングと回復（インターフェイス ライン制御）	Cisco IOS XE Release 3.9S	DMVPN：トンネル ヘルス モニタリングと回復（インターフェイス ライン制御）機能では、DMVPN トンネルの正常性に基づいて、NHRP でトンネル インターフェイスの状態を制御できます。 Cisco IOS XE Release 3.9S では、この機能は Cisco CSR 1000V シリーズ クラウド サービス ルータに導入されました。 Cisco IOS XE Release 3.13S では、この機能は Cisco 4000 シリーズ サービス統合型ルータに導入されました。 Cisco IOS XE Release 3.13.1S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入されました。**if-state nhrp**

第 8 章

DMVPN イベント トレーシング

DMVPN イベント トレーシング機能は、Cisco IOS Dynamic Multipoint VPN（DMVPN）のトラブルシューティングに使用するトレース ファシリティを提供します。この機能を使用すると、DMVPN のイベント、エラー、および例外をモニタできます。実行時に、イベント トレース メカニズムによってバッファ領域にトレース情報が記録されます。表示メカニズムによりデバッグ データが抽出およびデコードされます。

DMVPN イベント トレーシング機能を使用してデバイス障害の原因を分析できます。DMVPN イベント トレーシング機能を設定すると、ルータは特定の DMVPN サブシステム コンポーネントからのメッセージをデバイスのメモリに記録します。メモリに保存されているトレース メッセージを表示したり、ファイルに保存したりすることができます。

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 イベント トレーシングについて

DMVPN イベント トレーシングの利点

- 実行時にコンソールでデバッグ情報を表示できます。
- 複数のデバッグ コールを回避できるため、デバイスのパフォーマンスが向上します。
- メモリ領域を節約できます。

DMVPN イベント トレーシング オプション

DMVPN イベント トレーシング機能は、イベント データ タイプの定義、イベントをキャプチャする機能の提供、ログにアクセスして変更するために必要なイベントと CLI 拡張の出力を行います。次の表に、DMVPN イベント トレーシング機能を使用してモニタできる各種オプションを示します。

表 *14* : *DMVPN* イベント トレース オプション

イベント タイプ	説明
NHRP イベント トレース	Next Hop Resolution Protocol（NHRP）プロトコル、NHRP メッセージ、NHRP データ構造での変更、NHRP NBMA またはプロトコル アドレスの変更、NHRP トラップなど、一般的な NHRP イベント。
NHRP エラー トレース	すべての NHRP エラー イベント。
NHRP 例外トレース	すべての NHRP 例外イベント。
トンネル イベント トレース	すべてのトンネル イベント。

DMVPN イベント トレーシングの設定方法

DMVPN イベント トレーシング機能は、必要なパラメータに基づいて特権 EXEC モードまたはグローバル コンフィギュレーション モードで設定できます。特権 EXEC モードまたはグローバル コンフィギュレーション モードで使用できるさまざまなパラメータについては、『*Cisco IOS Security Command Reference*』を参照してください。

DMVPN イベント トレーシング機能を設定するには、次のいずれかの作業を実行します。

特権 EXEC モードでの DMVPN イベント トレーシングの設定

特権 EXEC モードで DMVPN イベント トレーシングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **monitorevent-tracedmvpn** {**nhrp** {**error** | **event** | **exception**} | **tunnel**} {**clear** | **continuous** [**cancel**] | **disable** | **enable** | **one-shot**} | **tunnel**}

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： `Router> 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	**monitorevent-tracedmvpn** {**nhrp** {**error**	**event**	**exception**}	**tunnel**} {**clear**	**continuous** [**cancel**]	**disable**	**enable**	**one-shot**}	**tunnel**} 例： `Router# monitor event-trace dmvpn nhrp error enable`	DMVPM トレースをモニタおよび制御します。

グローバル コンフィギュレーション モードでの DMVPN イベント トレーシングの設定

グローバル コンフィギュレーション モードで DMVPN イベント トレーシングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **monitorevent-tracedmvpn** {**dump-file** *url* | {**nhrp** {**error** | **event** | **exception**} | **tunnel**} {**disable** | **dump-file** *url* | **enable** | **size** | **stacktrace** *value*}}
4. **exit**

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： `Router> 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： `Router# 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	**monitorevent-tracedmvpn** {**dump-file** *url* | {**nhrp** {**error** | **event** | **exception**} | **tunnel**} {**disable** | **dump-file** *url* | **enable** | **size** | **stacktrace** *value*}} 例： `Router(config)# monitor event-trace dmvpn nhrp error enable`	DMVPM トレースをモニタおよび制御します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

DMVPN イベント トレーシングの設定例

特権 EXEC モードでの DMVPN イベント トレーシングの設定例

次の例では、特権 EXEC モードで NHRP エラー トレースをモニタする方法を示します。

```
Router> enable
Router# monitor event-trace dmvpn nhrp error enable
```

グローバル コンフィギュレーション モードでの DMVPN イベント トレーシングの設定例

次の例では、グローバル コンフィギュレーション モードで NHRP エラー トレースをモニタする方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# monitor event-trace dmvpn nhrp error enable
```

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
DMVPN コマンド	『*Cisco IOS Security Command Reference*』

標準

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	--

RFC

RFC	タイトル
なし	--

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 イベント トレーシングの機能情報

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 *15* : *DMVPN* イベント トレーシングの機能情報

機能名	リリース	機能情報
DMVPNイベント トレーシング	Cisco IOS XE Release 3.9S	DMVPNイベント トレーシング機能は、Cisco IOS DMVPN のトラブルシューティングに使用するトレース ファシリティを提供します。この機能を使用すると、DMVPNのイベント、エラー、および例外をモニタできます。実行中は、イベント トレース メカニズムによってバッファ領域にトレース情報が記録されます。表示メカニズムによりデバッグ データが抽出およびデコードされます。 次のコマンドが導入または変更されました。 **monitorevent-tracedmvpn**、**showmonitorevent-tracedmvpn**

第 9 章

NHRP MIB

Cisco NHRP MIB は、簡易ネットワーク管理プロトコル（SNMP）を介して Next Hop Resolution Protocol（NHRP）の管理やモニタを行ううえで有用な NHRP MIB をサポートするための機能です。NHRP MIB に指定されたオブジェクトを照会する標準ベースの SNMP 操作（GET 操作）により、統計情報の収集やモニタを行うことが可能です。NHRP MIB は VPN ルーティングおよび転送（VRF）に対応しており、VRF 対応クエリーをサポートしています。

（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。

NHRP MIB を使用するための前提条件

- SNMP の設定方法を熟知していることが必要です。

NHRP MIB の制約事項

- RFC 2677『Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)』で規定されている MIB 変数の中には、シスコでサポートされていないものもあります。サポートされている変数のリスト、およびこの機能に関するその他の注意事項については、Agent Capabilities ファイルを参照してください。シスコでは、RFC 2677 で規定されている SET 操作はサポートしていません。

NHRP MIB について

CISCO-NHRP-MIB

CISCO-NHRP-MIB には、管理対象オブジェクトに関する NHRP MIB 情報があります。これらの情報は、クライアントだけに関連するもの、サーバだけに関連するもの、クライアントとサーバ双方に関連するものに分類されます。

NHRP MIB モジュールに含まれるオブジェクトのテーブルは次の 10 個です。

- NHRP キャッシュ テーブル
- NHRP 消去要求テーブル
- NHRP クライアント テーブル
- NHRP クライアント登録テーブル
- NHRP クライアント NHS テーブル
- NHRP クライアント統計情報テーブル
- NHRP サーバ テーブル
- NHRP サーバ キャッシュ テーブル
- NHRP サーバ NHC テーブル

- NHRP サーバ統計情報テーブル

シスコの実装では、NHRP 消去要求テーブルを除くすべてのテーブルがサポートされています。

RFC-2677

RFC-2677『Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)』には、SNMP を介して NHRP のリモート モニタを行う際に使用できる管理対象オブジェクトが規定されています。この管理対象オブジェクトにより、NHRP のパフォーマンスに関する管理情報を取得できます。

NHRP MIB の使用方法

NHRP MIB 機能を実装する際に特別な設定は必要ありません。NHRP MIB は、SNMP フレームワークを使用して管理できます。VRF 対応 NHRP MIB の管理方法の例については、「NHRP MIB の設定例」を参照してください。

ここでは、次のタスクについて説明します。

NHRP MIB ステータスの確認

NHRP MIB ステータスを確認する作業は次のとおりです。

手順の概要

1. **enable**
2. **showsnmpmibnhrpstatus**

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： `Router> enable`	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	**showsnmpmibnhrpstatus** 例： `Router# show snmp mib nhrp status`	NHRP MIB のステータスを表示します。

NHRP MIB の設定例

NHRP MIB ステータスの確認例

show snmp mib nhrp status コマンドを実行すると、次のような内容が出力されます。

```
Router# show snmp mib nhrp status
NHRP-SNMP Agent Feature: Enabled
NHRP-SNMP Tree State: Good
ListEnqueue Count = 0 Node Malloc Counts = 1
Spoke_103#
```

「NHRP-SNMP Agent Feature:」の「Enabled」ステータスは、NHRP MIB がイネーブルになっていることを示しています。NHRP MIB がディセーブルであれば、この部分には「Disabled」と表示されます。「ListEnqueue Count」および「Node Malloc Counts」の右側に表示されている数字は、内部的な数値です。「ListEnqueue Count」は、解放を待機しているノードの数を表します。「Node Malloc Counts」は、割り当てられているノードの数を表します。

VRF 対応 NHRP MIB 設定例

ここでは具体例として、SNMP によるモニタを実行するために、Vrf1 という名前の VRF テーブルを設定する方法を紹介します。

```
ip vrf Vrf1
 rd 198102
! Name of the SNMP VPN context
 context Vrf1-context
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
! DMVPN tunnel for Vrf1 VPN
 ip vrf forwarding Vrf1
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication sample
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
```

```
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
address-family ipv4 vrf Vrf1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
 autonomous-system 1
exit-address-family
!
! V2C Community ABC for VRF Vrf1
snmp-server group abc v2c context V3red_context read view_V3
snmp-server view view_V3 iso included
snmp-server community abc RO
snmp-server community public RO
snmp-server context Vrf1_context
!
!
snmp mib community-map abc context Vrf1-context
Spoke Configuration for DMVPN Example
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication sample
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
```

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
SNMP の説明、SNMP MIB の説明、およびシスコの各種デバイスにおける SNMP の設定方法の説明	『*Cisco IOS Network Management Configuration Guide*』の「Configuring SNMP Support」の章
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

標準

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
CISCO-NHRP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2677	『Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)』

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

NHRP MIB 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 *16*：*NHRP MIB* の機能情報

機能名	リリース	機能情報
DMVPN ネットワークの NHRP MIB	Cisco IOS XE Release 2.5	Cisco NHRP MIB は、簡易ネットワーク管理プロトコル（SNMP）を介して NHRP の管理やモニタを行ううえで有用な NHRP MIB をサポートするための機能です。NHRP MIB に指定されたオブジェクトを照会する標準ベースの SNMP 操作（GET 操作）により、統計情報の収集やモニタを行うことが可能です。 次のコマンドが導入または変更されました。debug snmp mib nhrp、**showsnmpmibnhrpstatus**

第 10 章

NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネル

NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネル機能により、1 つまたは複数のスポークがネットワーク アドレス変換（NAT）デバイスの背後に配置されていても、Next Hop Resolution Protocol（NHRP）スポークツースポーク トンネルを Dynamic Multipoint Virtual Private Network（DMVPN）に構築できます。

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。

NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネルに関する制約事項

スポーク間にトンネルを構築するには、2 つのスポークでそれぞれの NAT 後のアドレスが認識されている必要があります。

NAT 環境でスポークツースポーク トンネリングを使用する際には、次の制約事項を考慮してください。

- **複数の NAT 変換**：パケットは、非ブロードキャスト マルチアクセス（NBMA）DMVPN クラウドの複数の NAT デバイスを通過でき、宛先に到達するまでに、いくつかの（重要でない）変換を行います。最後のものが重要な変換になります。それを使用して、最後の NAT デバイスを介してスポークに到達するすべてのデバイスに、NAT 変換を作成するからです。
- **NAT 前のアドレスを使用して到達できるハブまたはスポーク**：複数のスポークを同じ NAT デバイスの背後に配置でき、NAT 前の IP アドレスを使用して到達することができます。トンネルが望ましくないパスをたどることがあっても、NAT 後の IP アドレスだけが信頼されます。両方のスポークが同じデバイスを介して NAT を使用する場合、パケットが NAT デバイスの想定どおりに移動（内側から外側に、あるいは外側から内側に）しないことがあり、変換が適切に行われないことがあります。
- **NAT 対応のデバイスと NAT 非対応のデバイスとの相互運用性**：DMVPN を使用して展開されるネットワークでは、NHRP NAT 機能を使用するデバイスが NAT 非対応のデバイスと連動することが重要です。NHRP パケット ヘッダーの機能ビットは、送信元デバイスが NAT 拡張部を認識するかどうか、任意の受信者に示します。
- **同一の NAT 変換**：スポークの NAT 後の IP アドレスは、スポークが自身のハブと通信する場合も他のスポークと通信する場合も同一である必要があります。たとえば、スポークが DMVPN ネットワーク内でトンネル パケットをいずれの場所に送信しても、スポークの NAT 後の IP アドレスは同じである必要があります。
- NAT のタイプが共に PAT である 2 つの NAT デバイスのそれぞれの後にスポークが配置されている場合、その 2 つのスポーク間でセッションが開始されても、そのセッションは確立できません。

次に、NAT インターフェイスにおける PAT の 1 つの設定例を示します。

```
ip nat inside source list nat_acl interface FastEthernet0/1 overload
```

NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネルについて

以降の項では、1 つまたは両方のスポーク デバイスが NAT デバイスの背後に配置されていても、NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネル機能により、スポークツースポーク トンネルの構築を可能にする方法について説明します。

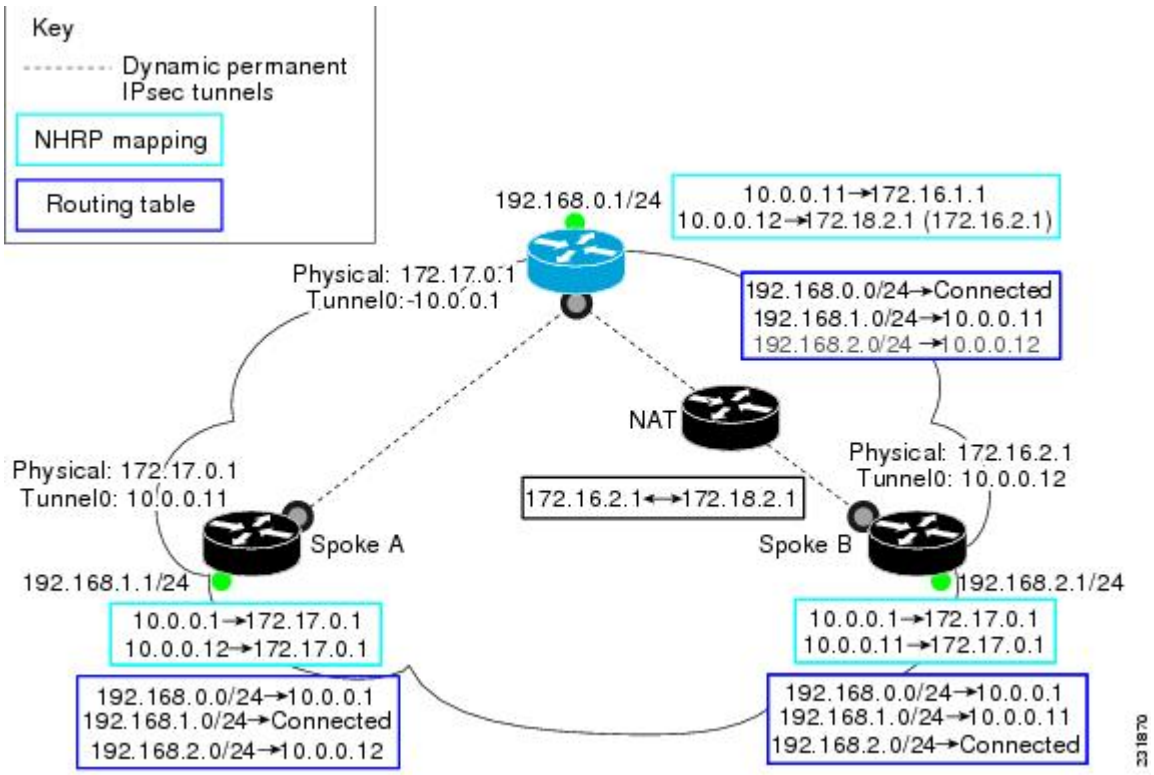
NATデバイスの背後に配置されていないスポークに制限されるDMVPN スポークツースポーク トンネリング

NAT を使用すると、ルータなどの単一のデバイスが、インターネット（または「パブリック ネットワーク」）とローカル（または「プライベート」）ネットワークの間でエージェントとして動作できます。NAT が主に使用されるのは、利用可能な IP アドレスが不足している場合です。NAT デバイスの外部に対してデバイス グループ全体を表す一意の IP アドレスが 1 つ必要です。また、NAT はセキュリティおよび管理上の目的でも展開されます。

DMVPN ネットワークでは、スポークツースポーク トンネリングを構築できる場所は、NAT デバイスの背後に配置されていないスポークに制限されます。1 つまたは両方のスポークが NAT デバイスの背後に配置されている場合、スポークツースポーク トンネルを NAT デバイスに対して、または NAT デバイスから構築できません。これは、スポークツースポーク トンネル トラフィックに障害が発生したり、トラフィックが長時間失われる（「ブラックホール化」される）可能性があるためです。

以下の図および以降の項では、スポークツースポーク トンネリングが NAT デバイスの背後に配置されていないスポークに限定されている場合に、DMVPN がどのように機能するかを示します。

図 *6*：*NAT* デバイスの背後に配置されていないスポークに限定される *DMVPN* スポークツースポーク トンネリングの実装



NHRP 登録

NHRP 登録を受信するとハブは、NHRP パケットのカプセル化 GRE/IP ヘッダーの送信元 IP アドレスと、NHRP 登録パケットに含まれている送信元 NBMA IP アドレスを照合します。これらの IP アドレスが異なる場合、NHRP は、NAT によって外部 IP ヘッダー送信元アドレスが変更されていると認識します。ハブは、登録されたスポークの NAT 前のアドレスと NAT 後のアドレスの両方を保持します。

（注） 暗号化を使用する場合は、IPsec トランスポート モードを使用して NHRP をイネーブルにする必要があります。

次の **showipnhrp** コマンド出力例は、上の図のスポーク B に関する NHRP パケットの送信元 IP アドレスおよびトンネル情報を示しています。

（注） スポーク B の NBMA（NAT 後の）アドレスは、172.18.2.1 です（要求された NBMA（NAT 前の）送信元アドレスは 172.16.2.1 です）。

```
Router# show ip nhrp
10.0.0.11/32 via 10.0.0.11, Tunnel0 created 00:00:21, expire 00:05:38
  Type: dynamic, Flags: authoritative unique registered used
NBMA address: 172.18.2.1
   (Claimed NBMA address: 172.16.2.1)
```

NHRP 解決

次に、上の図に示したスポーク A とスポーク B 間の NHRP 解決プロセスを説明します。スポーク B は NAT デバイスの背後に配置されており、NAT 前のアドレスは 172.16.2.1、NAT 後のアドレスは 172.18.2.1 です。

- ハブ上のスポーク B の NHRP テーブル エントリには、NAT 後のアドレスと NAT 前のアドレスが含まれています。ハブは、スポーク B の VPN アドレス（トンネル アドレス）に対する NHRP 解決要求を受け取ると、スポーク B の NBMA アドレスの代わりに、ハブ自身の NBMA アドレスで応答します。
- ハブは、スポーク B から送信された他のスポークに対する NHRP 解決要求受け取ると、ハブ自身の NBMA アドレスで応答します。これにより、スポーク B とのスポークツースポーク トンネルを構築しようと試みた場合、データ パケットがスポークツースポーク トンネルではなく、ハブを介して確実に送信されるようになります。

次に例を示します。

- - 送信元 IP アドレス 192.168.1.1（スポーク A の背後）から宛先 IP アドレス 192.168.2.1（スポーク B の背後）へのデータ トラフィックにより、スポーク A がトリガーされて、スポーク B（10.0.0.12）に対する解決要求をネクストホップ ルータ（ハブ）に送信されます。
  - ハブは解決要求を受信し、スポーク B（10.0.0.12）のマッピング エントリを検索します。スポーク B は、NAT デバイスの背後に配置されているため、プロキシとして機能し、自身の NBMA アドレス（172.17.0.1）で応答します。
  - ハブは、スポーク A（10.0.0.11）に対する解決要求もスポーク B から受信します。スポーク B は、NAT デバイスの背後に配置されているため、プロキシとして機能し、自身の NBMA アドレス（172.17.0.1）で応答します。これにより、スポーク間にトンネルを確立せずに、ハブ ルータを通過するスポーク B に出入りするすべてのスポークツースポーク トラフィックが制限されます。

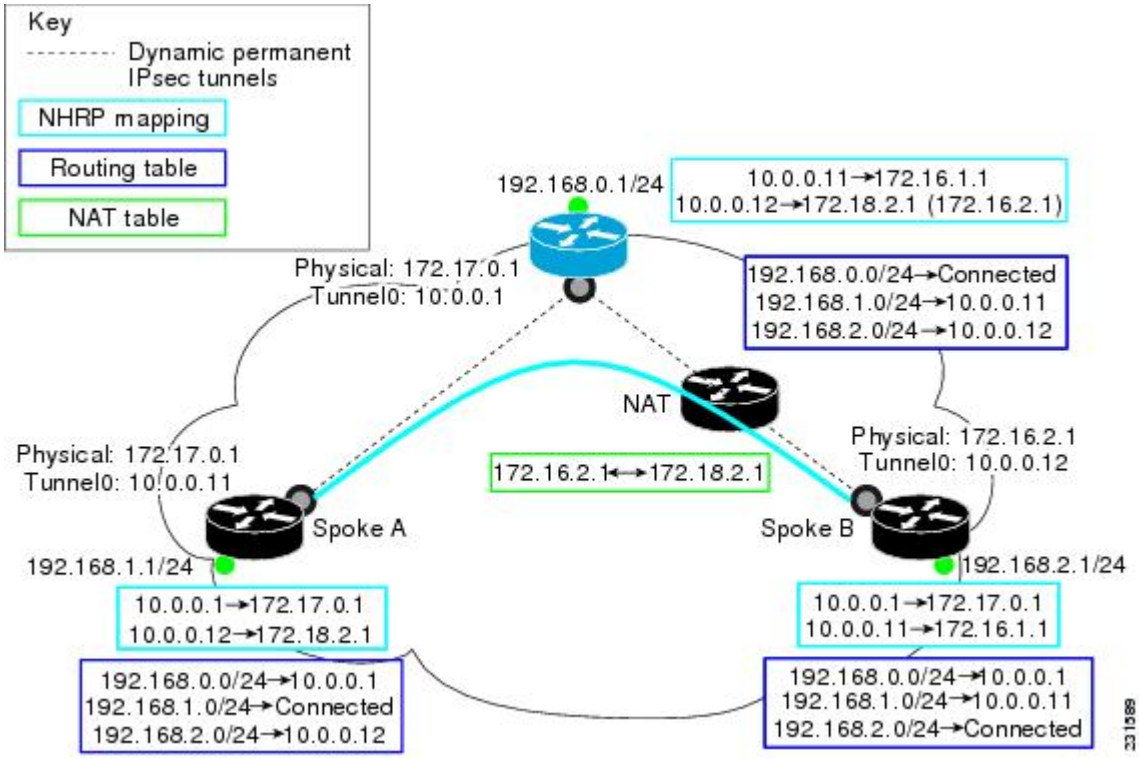
NAT デバイスを使用した NHRP スポークツースポーク トンネル

NAT を使用した NHRP スポークツースポーク トンネル機能では、NHRP プロトコルに NAT 拡張部が導入され、これは自動的にイネーブルになります。NHRP NAT 拡張部は、プロトコルおよび NAT 後の NBMA アドレスに関する情報が含まれるクライアント情報エントリ（CIE）エントリです。1 つのスポークまたは両方のスポークが NAT デバイスの背後に配置されている場合、この追加情報により、スポーク間でスポークツースポーク トンネルをサポートできます。トラフィックが長期間喪失（ブラックホール化）する問題が発生することはありません。

（注） スポークツースポーク トンネルがアップ状態にならないことがありますが、これは検出されるので、データ トラフィックは、失われずに（ブラックホール化されずに）ハブを通過します。

下の図に、NHRP スポークツースポーク トンネルがどのように NAT と連動するかを示します。

図 7：スポークツースポーク トンネル間の ***NHRP***



NHRP 登録プロセス

次のステップでは、NHRP 登録プロセスについて説明します。

1 スポークが、スポーク上の設定に従って、登録要求とともにNAT-Capability=1パラメータおよびハブの NBMA アドレスの NAT NHRP 拡張部を送信します。

2 ハブは、NHRP（NAT）拡張部をその設定済みの NBMA アドレスと比較し、スポークが NAT デバイスの背後にあるかどうか判別します。またハブは、着信GRE/IP送信元アドレスをNHRPパケット内のスポークの NBMA アドレスと比較して、スポークが NAT デバイスの背後に配置されているかどうかを記録します。

3 ハブが、スポークが NAT デバイスの背後にあると検出した場合、ハブからスポークへの登録応答には、NAT NHRP 拡張部とスポークの NAT 後のアドレスが含まれています。

4 スポークは NHRP 登録応答の NAT NHRP 拡張部を取得すると、後で使用できるように NAT 後の IP アドレスを記録します。

NHRP 解決および消去プロセス

次のステップでは、NHRP 解決および消去プロセスについて説明します。

1 スポークが NAT デバイスの背後に配置されている場合に NHRP 解決要求を送信するとき、スポークには NAT NHRP 拡張部が含まれています。

2 ハブが解決要求を受信します。スポークが NAT デバイスの背後に配置されていて、かつ NAT 拡張部がない場合、ハブは、NAT拡張部を追加してから、この拡張部をパスに沿って次のノード（スポークまたはネクスト ホップ サーバ）に転送します。ただし、ハブが要求を非 NAT 拡張部対応ノードに転送する場合、ハブはその NAT 前の IP アドレスではなく、パケット内部の送信元 NBMA を書き換えて要求元スポークの NAT 後の IP アドレスとします。

3 受信側（スポーク）は、NAT NHRP 拡張部レコード（NAT 対応）または送信元 NBMA アドレス（NAT 非対応情報）を使用して、トンネルを構築します。このスポークが NAT デバイスの背後に配置されている場合、このスポークの応答には、自身のNAT拡張部が含まれています。

（注） ハブは、スポークにかわってNHRP解決要求に応答しません。ハブは常にNHRP解決要求を、要求されたトンネルIPアドレスを持つエンドスポークか、またはホストのIPアドレスから要求されたデータを処理するエンドスポークに転送します。

次に、上の図に示すスポーク A とスポーク B 間の NHRP 解決プロセスを説明します。スポーク B は NAT デバイスの背後に配置されており、NAT 前のアドレスは 172.16.2.1、NAT 後のアドレスは 172.18.2.1 です。

- スポーク A の背後にあるホストから 192.168.2.0/24 ネットワークへのデータ トラフィックにより、スポーク B のトンネル IP アドレス（10.0.0.12）の NHRP 解決要求がトリガーされ、ハブを介して送信されます。ハブは解決要求を受信し、スポーク B に転送します。スポーク B は NHRP 解決要求に含まれるスポーク A の送信元 NBMA IP アドレスを使用してダイナミック スポークツースポーク トンネルを作成し、スポーク A に NHRP 解決応答を直接送信します。この NAT NHRP 拡張ヘッダーにはスポーク B の NAT 後のアドレスが含まれます。

- また、スポーク B 上の NAT デバイスの背後に配置されているホストから 192.168.1.0/24 ネットワークへのトラフィックにより、スポーク A のトンネル IP アドレス（10.0.0.11）に対する NHRP 解決要求がトリガーされます。スポーク B は、自身の NAT 後の IP アドレスを解決要求の NHRP NAT 拡張部に追加します。ハブは解決要求を受信し、スポーク A に転送します。スポーク A は NHRP NAT 拡張部を解析し、スポーク B の NAT 後のアドレスを使用してトンネルを構築し、スポーク B に直接応答します。

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
NHRP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Addressing Services Command Reference*』
ダイナミック マルチポイント VPN	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Dynamic Multipoint VPN (DMVPN)」の章

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC	タイトル
このリリースによってサポートされる新しい RFC や変更された RFC はありません。	--

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

NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネルの機能情報

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 *17* : ***NAT*** デバイスの背後に配置されたスポーク間の ***DMVPN*** ダイナミック トンネルの機能情報

機能名	リリース	機能情報
NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネル	Cisco IOS XE Release 2.5	NAT デバイスの背後に配置されたスポーク間の DMVPN ダイナミック トンネル機能により、1 つまたは複数のスポークがネットワーク アドレス変換（NAT）デバイスの背後に配置されていても、NHRP スポーク ツースポーク トンネルを DMVPN ネットワークに構築できます。 Cisco IOS XE Release 2.5 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション ルータに導入されました。

第 11 章

トンネル保護による IPsec 共有

トンネル保護による IPsec 共有機能を使用すると、トンネルが保護された状態で、IP Security（IPsec）セキュリティ アソシエーション データベース（SADB）を 2 つ以上の総称ルーティング カプセル化（GRE）トンネル インターフェイス間で共有できます。これらのトンネル インターフェイスでは、Dynamic Multipoint Virtual Private Network（DMVPN）設定に含まれる、単一の基本的な暗号化 SADB、暗号化マップ、および IPsec プロファイルが共有されます。

1 つの IPsec SADB 内で IPsec セキュリティ アソシエーション（SA）セッションが共有されていない場合、IPsec SA が、不適切な IPsec SADB、ひいては誤ったトンネル インターフェイスに関連付けられて、IPsec SA の重複やトンネル インターフェイスのフラッピングが発生する可能性があります。トンネル インターフェイスがフラップする（オンライン状態とオフライン状態が短時間で何度も切り替わる）と、ネットワーク接続に問題が発生します。

（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。

トンネル保護による IPsec 共有の前提条件

- マルチポイント GRE（mGRE）および IPsec トンネルを確立するには、**crypto isakmp policy** コマンドを使用して、インターネット キー交換（IKE）ポリシーを定義しておく必要があります。

トンネル保護による IPsec 共有に関する制約事項

- トンネル送信元が同じであるすべてのトンネル インターフェイスに対して、**tunnelsource** コマンドを設定する必要があります。設定には、トンネルの IP アドレスではなく、インターフェイスのタイプおよび番号を使用します。
- トンネル送信元インターフェイスが同じであるすべてのトンネルで同一の IPsec プロファイルを使用し、**tunnelprotection shared** コマンドを設定する必要があります。唯一の例外は、トンネル送信元が同じで、トンネル宛先の IP アドレスはそれぞれ一意であるピアツーピア（P2P）GRE トンネル インターフェイスのみがシステムで設定されている場合です。
- 共有トンネルと非共有トンネルには、別々の IPsec プロファイル名を使用する必要があります。
  たとえば、「トンネル 1」に **tunnelsourceloopback0** コマンドを設定し、「トンネル 2」および「トンネル 3」は **tunnelsourceloopback1** コマンドを使用して共有する場合は、「トンネル 1」に対しては ipsec-profile-1、「トンネル 2」および「トンネル 3」に対しては ipsec-profile-2 をそれぞれ使用します。
- 共有トンネルの 1 つのまとまりごとに、個別の IPsec プロファイルを使用することが必要です。
  たとえば、トンネル 1 ～ 5 のトンネル送信元として **loopback0** が使用され、トンネル 6 ～ 10 のトンネル送信元として loopback1 が使用されている場合、トンネル 1 ～ 5 に対しては ipsec-profile-1、トンネル 6 ～ 10 に対しては ipsec-profile-2 をそれぞれ定義します。

- 同じトンネル送信元を使用する複数のトンネル インターフェイス間では、IPsec セッションを共有しないことを推奨します。
  たとえば、各 DMVPN クラウドに対して異なるカスタマーが対応するようなサービス プロバイダー環境では、特定のカスタマーからトンネル インターフェイスへの接続を固定し、それ以外のカスタマーからの IPsec セッションを共有したり許可しないのが望ましいです。このような場合、Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを使用して、カスタマー接続の識別と ISAKMP プロファイルへのバインドを行い、その ISAKMP プロファイルを使用して IPsec プロファイルに接続できます。この ISAKMP プロファイルにより、IPsec プロファイルで許可される接続は、対応する ISAKMP プロファイルに適合したものだけに制限されます。ISAKMP プロファイルおよび IPsec プロファイルは、同一の IPsec SADB を共有していない DMVPN クラウド（トンネル インターフェイス）ごとに、個別に取得できます。

- 仮想トンネル インターフェイス（VTI）に対しては、IPsec の共有は適しておらず、サポートもされていません。VTI により、ルーティング可能なインターフェイス タイプを使って IPsec トンネルを終端できるほか、サイト間に保護機能を定義してオーバーレイ ネットワークを構成できます。

トンネル保護による IPsec 共有について

単一の IPsec SA と GRE トンネル セッション

デュアル ハブ デュアル DMVPN トポロジでは、同じタイプの 2 つのエンドポイント間で複数の GRE トンネル セッション（トンネルの送信元および宛先は同じだが、トンネル キーは異なる）を確立できます。この場合は、共通の IPsec SA を使用して両方の GRE トンネル セッションを確保してください。2 つのトンネル インターフェイスのトンネル送信元が同じである場合に、IPsec クイック モード（QM）要求をどちらのトンネル インターフェイスで処理およびバインドするかは指定できません。

同一のプロファイルおよびトンネル送信元インターフェイスを使用するすべてのトンネル インターフェイスに対して、共通の IPsec SADB を作成する場合は、**tunnelprotectionipsecprofileshared** コマンドを使用します。この設定により、同じタイプの 2 つのエンドポイント間にあるすべての GRE トンネル（トンネルの送信元および宛先は同じだが、トンネル キーは異なる）に対して、共通の IPsec SA を使用できます。また、**tunnelprotectionipsecprofileshared** コマンドを使用すると、IPsec QM の処理が明確になります。これは、SADB が共有されずに複数の SADB（トンネル インターフェイスごとに 1 つ）が使用される場合とは異なり、すべての共有トンネル インターフェイスに対して、着信 IPsec QM 要求が 1 つの SADB で処理されるためです。

トンネル インターフェイスに対する QM プロポーザルの SA は、共有 SADB および暗号化マップ パラメータを使用して処理されます。クリプト データ プレーンでは、復号化されたパケットおよび GRE カプセル化を解除されたパケットは、ローカル アドレス、リモート アドレス、およびオプションのトンネル キー情報に基づいて、GRE モジュールにより逆多重化されたうえで、適切なトンネル インターフェイスへ送信されます。

IPsec パスの最大伝送ユニット（MTU）が変わると、Quantum Flow Processor（QFP）およびハードウェア暗号化エンジンの SA MTU 値が更新され、IPsec MTU と一致します。MTU の変化に伴い、システムで一部のパケットがドロップされ、一時的な %ATTN-3-SYNC_TIMEOUT エラーがコンソールに表示されることがあります。

（注） トンネル送信元、トンネル宛先、およびトンネル キー（3 ビット バイト）は、ルータ上のすべてのトンネル インターフェイスに対して一意である必要があります。トンネル宛先が設定されていないマルチポイント GRE（mGRE）インターフェイスの場合は、トンネル送信元とトンネル キーのペアが一意である必要があります。また、着信 GRE パケットは最初に P2P GRE トンネルと照合され、一致がない場合は mGRE トンネルと照合されます。

トンネル保護による IPsec 共有の設定方法

DMVPN の複数トンネル インターフェイスによる IPsec SADB の共有

DMVPN の複数トンネル インターフェイス間で IPsec SADB が共有されるように Cisco IOS ルータを設定するには、次の作業を実行します。

デュアル ハブ デュアル DMVPN トポロジで、さらにスポーク ルータを設定する必要がある場合は、この作業の手順を繰り返して追加のスポークを設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **tunnel source** {*ip-address* | *interface-type interface-number*}
5. **tunnelprotectionipsecprofile***name* [**shared]**
6. **exit**
7. **exit**

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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： `Router(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	**tunnel source** {*ip-address* | *interface-type interface-number*} 例： `Router(config-if)# tunnel source GigabitEthernet 0`	トンネル インターフェイスの送信元 IP アドレスまたは送信元インターフェイス タイプ番号を設定します。 • **tunnelprotectionipsecprofile** コマンドを使用する場合は、トンネル送信元の IP アドレスではなくインターフェイスを指定する必要があります。
ステップ 5	**tunnelprotectionipsecprofile***name* [**shared]** 例： `Router(config-if)# tunnel protection ipsec profile vpnprof shared`	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。 • **shared** キーワードを指定すると、同じトンネル送信元 IP を設定した複数のトンネル インターフェイス間で IPsec セッションを共有できるようになります。
ステップ 6	**exit** 例： `Router(config-if)# exit`	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、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

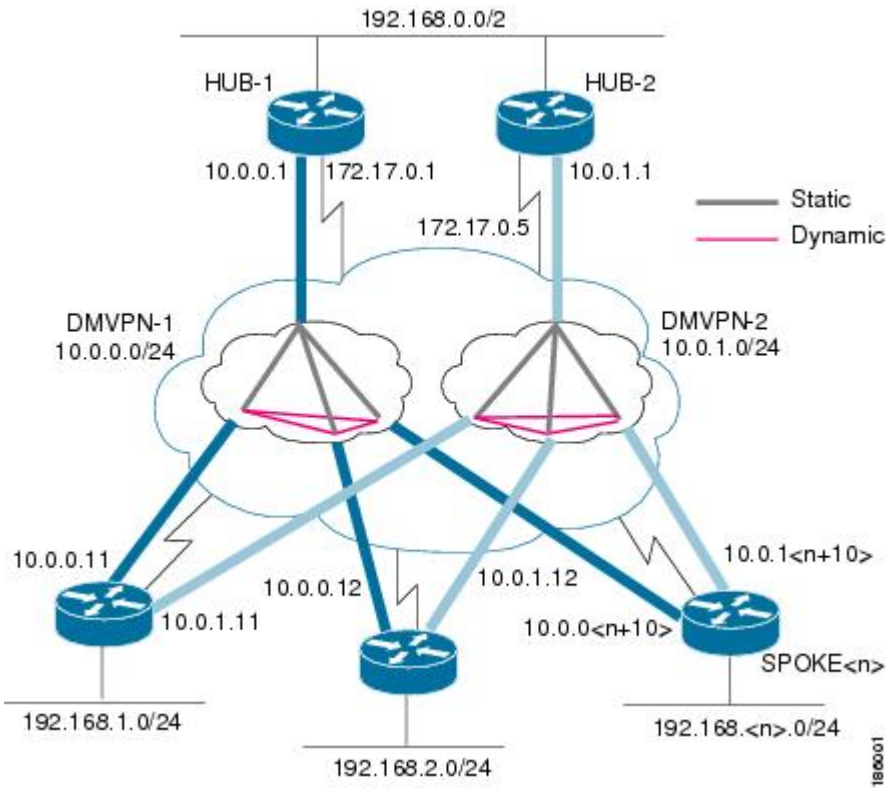
トンネル保護による IPsec 共有の設定例

例：デュアルハブ ルータ デュアル DMVPN トポロジ

以下の図に示したデュアルハブ ルータ デュアル DMVPN トポロジには、次の特性があります。

- 各ハブ ルータには、mGRE トンネル インターフェイスが 1 つ設定されます。
- 各ハブ ルータは、1 つの DMVPN サブネット（クラウド）に接続され、スポークは DMVPN-1 と DMVPN-2 の双方に接続されます。
- 各スポーク ルータには、mGRE トンネル インターフェイスが 2 つ設定されます。
- 一方の mGRE トンネル インターフェイスは DMVPN-1 に属し、もう一方の mGRE トンネル インターフェイスは DMVPN-2 に属します。
- 各 mGRE トンネル インターフェイスに同一のトンネル送信元 IP アドレスが設定され、両者の間でトンネル保護が共有されます。

図 *8*：デュアルハブ ルータ デュアル *DMVPN* トポロジ



例：DMVPN の複数トンネル インターフェイス間での IPsec SADB の設定

例：ハブ 1 の設定

ハブ 1 とハブ 2 は、属する DMVPN が異なることを除けば、その設定内容は同じです。

ハブ 1 の DMVPN 設定は次のとおりです。

- IP サブネット：10.0.0.0/24
- Next Hop Address Resolution Protocol（NHRP）ネットワーク ID：100000
- トンネル キー：100000
- ダイナミック ルーティング プロトコル：Enhanced IGRP（EIGRP）

```
!
hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto IPsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto IPsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel 5
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  no ip next-hop-self eigrp 1
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
no ip split-horizon eigrp 1
ip tcp adjust-mss 1360
  delay 1000
  tunnel source GigabitEthernet 0/0/0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection IPsec profile vpnprof
 !
 interface GigabitEthernet 0/0/0
  ip address 172.17.0.1 255.255.255.252
 !
 interface GigabitEthernet 0/0/1
  ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
```

例：ハブ 2 の設定

ハブ 2 の DMVPN 設定は次のとおりです。

- IP サブネット：10.0.1.0/24
- NHRP ネットワーク ID：100001
- トンネル キー：100001
- ダイナミック ルーティング プロトコル：EIGRP

```
!
hostname Hub2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel 5
  bandwidth 1000
  ip address 10.0.1.1 255.255.255.0
  ip mtu 1400
  no ip next-hop-self eigrp 1
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100001
  ip nhrp holdtime 600
no ip split-horizon eigrp 1
ip tcp adjust-mss 1360
  delay 1000
  tunnel source GigabitEthernet 0/0/0
  tunnel mode gre multipoint
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
 interface GigabitEthernet 0/0/0
  ip address 172.17.0.5 255.255.255.252
 !
 interface GigabitEthernet 0/0/1
  ip address 192.168.0.2 255.255.255.0
 !
 router eigrp 1
  network 10.0.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
```

例：スポーク 1 の設定

スポーク 1 に対する DMVPN 設定は次のとおりです。

```
!
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
```

```
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
interface Tunnel 5
 bandwidth 1000
.
.
.
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300|
 ip nhrp nhs 10.0.0.1
 ip tcp adjust-mss 1360
 delay 1000
.
.
.
 tunnel protection ipsec profile vpnprof shared
!
interface Tunnel 5
 bandwidth 1000
.
.
.
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp map multicast 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 ip tcp adjust-mss 1360
 delay 1000
.
.
.
 tunnel protection ipsec profile vpnprof shared
!
 interface GigabitEthernet 0/0/0
  ip address dhcp hostname Spoke1
 !
 interface GigabitEthernet 0/0/1
  ip address 192.168.1.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  no auto-summary
 !
```

例：スポーク 2 の設定

スポーク 2 に対する DMVPN 設定は次のとおりです。

```
!
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
```

```
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
interface Tunnel 5
 bandwidth 1000
.
.
.
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300|
 ip nhrp nhs 10.0.0.1
 ip tcp adjust-mss 1360
 delay 1000
.
.
.
 tunnel protection ipsec profile vpnprof shared
!
interface Tunnel 5
 bandwidth 1000
.
.
.
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp map multicast 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 ip tcp adjust-mss 1360
 delay 1000
.
.
.
 tunnel protection ipsec profile vpnprof shared
 !
 interface GigabitEthernet 0/0/0
  ip address dhcp hostname Spoke2
 !
 interface GigabitEthernet 0/0/1
  ip address 192.168.2.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  no auto-summary
 !
```

例：スポーク 1 の結果

スポーク 1 に対する DMVPN 設定の結果は次のとおりです。

```
Spoke1# show ip nhrp

10.0.0.1/32 via 10.0.0.1, Tunnel 0 created 00:06:52, never expire
  Type: static, Flags: used
  NBMA address: 172.17.0.1
10.0.0.12/32 via 10.0.0.12, Tunnel 0 created 00:03:17, expire 00:01:52
  Type: dynamic, Flags: router
  NBMA address: 172.17.0.12
10.0.1.1/32 via 10.0.1.1, Tunnel 1 created 00:13:45, never expire
  Type: static, Flags: used
  NBMA address: 172.17.0.5
10.0.1.12/32 via 10.0.1.12, Tunnel 1 created 00:00:02, expire 00:04:57
```

```
  Type: dynamic, Flags: router
  NBMA address: 172.17.0.12
Spoke1# show crypto socket
```

（注） クリプト接続は、172.17.0.12、172.17.0.5、および172.17.0.1 の 3 つのみです。2 つの NHRP セッション（10.0.0.12, Tunnel0 と 10.0.1.12, Tunnel1）は、非ブロードキャスト マルチアクセス（NBMA）の IPsec ピア アドレスが同じであるため、どちらも同じ IPsec セッションです。

```
Number of Crypto Socket connections 3
   Shd Peers (local/remote): 172.17.0.11
/172.17.0.12
       Local Ident  (addr/mask/port/prot): (172.17.0.11/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (172.17.0.12/255.255.255.255/0/47)
       Flags: shared
       ipsec Profile: "vpnprof"
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
   Shd Peers (local/remote): 172.17.0.11
/172.17.0.5
       Local Ident  (addr/mask/port/prot): (172.17.0.11/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (172.17.0.5/255.255.255.255/0/47)
       Flags: shared
       ipsec Profile: "vpnprof"
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
   Shd Peers (local/remote): 172.17.0.11
/172.17.0.1
       Local Ident  (addr/mask/port/prot): (172.17.0.11/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (172.17.0.1/255.255.255.255/0/47)
       Flags: shared
       ipsec Profile: "vpnprof"
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "vpnprof" Map-name: "vpnprof-head-1"
Spoke1# show crypto map

Crypto Map: "vpnprof-head-1" idb: FastEthernet0/0/0 local address: 172.17.0.11
Crypto Map "vpnprof-head-1" 65536 ipsec-isakmp
        Profile name: vpnprof
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trans2,
        }
Crypto Map "vpnprof-head-1" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.17.0.5
        Extended IP access list
            access-list  permit gre host 172.17.0.11 host 172.17.0.5
        Current peer: 172.17.0.5
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trans2,
        }
Crypto Map "vpnprof-head-1" 65538 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.17.0.1
        Extended IP access list
            access-list  permit gre host 172.17.0.11 host 172.17.0.1
        Current peer: 172.17.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trans2,
        }
```

```
Crypto Map "vpnprof-head-1" 65539 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 172.17.0.12
        Extended IP access list
            access-list  permit gre host 172.17.0.11 host 172.17.0.12
        Current peer: 172.17.0.12
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                trans2,
        }
        Interfaces using crypto map vpnprof-head-1:
                Tunnel1
                Tunnel0
```

（注） **showcryptoipsecsa** の出力結果には、3 つのクリプトセッションが両方のトンネル インターフェイスに対して表示されています（3 つのエントリが 2 回ずつ）。これは、どちらのインターフェイスも、3 つのエントリを持つ同じ IPsec SADB にマッピングされているためです。この場合、このように、結果が重複して出力されます。

```
Spoke1# show crypto ipsec sa

interface: Tunnel 0
   Crypto map tag: vpnprof-head-1, local addr 172.17.0.11
   protected vrf: (none)
           local  ident (addr/mask/prot/port): (172.17.0.11/255.255.255.255/47/0)
           remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
           current_peer 172.17.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 134, #pkts encrypt: 134, #pkts digest: 134
    #pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 22, #recv errors 0
     local crypto endpt.: 172.17.0.11, remote crypto endpt.: 172.17.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
     current outbound spi: 0xA75421B1(2807308721)
     inbound esp sas:
      spi: 0x96185188(2518176136)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 3, flow_id: SW:3, crypto map: vpnprof-head-1
        sa timing: remaining key lifetime (k/sec): (4569747/3242)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xA75421B1(2807308721)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 4, flow_id: SW:4, crypto map: vpnprof-head-1
        sa timing: remaining key lifetime (k/sec): (4569745/3242)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     outbound ah sas:
     outbound pcp sas:
   protected vrf: (none)
           local  ident (addr/mask/prot/port): (172.17.0.11/255.255.255.255/47/0)
           remote ident (addr/mask/prot/port): (172.17.0.5/255.255.255.255/47/0)
           current_peer 172.17.0.5 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 244, #pkts encrypt: 244, #pkts digest: 244
    #pkts decaps: 253, #pkts decrypt: 253, #pkts verify: 253
```

```
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0
  local crypto endpt.: 172.17.0.11, remote crypto endpt.: 172.17.0.5
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
  current outbound spi: 0x3C50B3AB(1011921835)
  inbound esp sas:
   spi: 0x3EBE84EF(1052673263)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 1, flow_id: SW:1, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4549326/2779)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x3C50B3AB(1011921835)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 2, flow_id: SW:2, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4549327/2779)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  outbound ah sas:
  outbound pcp sas:
protected vrf: (none)
        local  ident (addr/mask/prot/port): (172.17.0.11/255.255.255.255/47/0)
        remote ident (addr/mask/prot/port): (172.17.0.12/255.255.255.255/47/0)
        current_peer 172.17.0.12 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0
  local crypto endpt.: 172.17.0.11, remote crypto endpt.: 172.17.0.12
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
  current outbound spi: 0x38C04B36(952126262)
  inbound esp sas:
   spi: 0xA2EC557(170837335)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 5, flow_id: SW:5, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4515510/3395)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x38C04B36(952126262)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 6, flow_id: SW:6, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4515511/3395)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  outbound ah sas:
  outbound pcp sas:
     interface: Tunnel 1
     Crypto map tag: vpnprof-head-1, local addr 172.17.0.11
protected vrf: (none)
        local  ident (addr/mask/prot/port): (172.17.0.11/255.255.255.255/47/0)
        remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
        current_peer 172.17.0.1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 134, #pkts encrypt: 134, #pkts digest: 134
```

```
 #pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 22, #recv errors 0
  local crypto endpt.: 172.17.0.11, remote crypto endpt.: 172.17.0.1
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
  current outbound spi: 0xA75421B1(2807308721)
  inbound esp sas:
   spi: 0x96185188(2518176136)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 3, flow_id: SW:3, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4569747/3242)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0xA75421B1(2807308721)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 4, flow_id: SW:4, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4569745/3242)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  outbound ah sas:
  outbound pcp sas:
protected vrf: (none)
        local  ident (addr/mask/prot/port): (172.17.0.11/255.255.255.255/47/0)
        remote ident (addr/mask/prot/port): (172.17.0.5/255.255.255.255/47/0)
        current_peer 172.17.0.5 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 244, #pkts encrypt: 244, #pkts digest: 244
 #pkts decaps: 253, #pkts decrypt: 253, #pkts verify: 253
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 1, #recv errors 0
  local crypto endpt.: 172.17.0.11, remote crypto endpt.: 172.17.0.5
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
  current outbound spi: 0x3C50B3AB(1011921835)
  inbound esp sas:
   spi: 0x3EBE84EF(1052673263)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 1, flow_id: SW:1, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4549326/2779)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x3C50B3AB(1011921835)
     transform: esp-des esp-md5-hmac ,
     in use settings ={Transport, }
     conn id: 2, flow_id: SW:2, crypto map: vpnprof-head-1
     sa timing: remaining key lifetime (k/sec): (4549327/2779)
     IV size: 8 bytes
     replay detection support: Y
     Status: ACTIVE
  outbound ah sas:
  outbound pcp sas:
protected vrf: (none)
        local  ident (addr/mask/prot/port): (172.17.0.11/255.255.255.255/47/0)
        remote ident (addr/mask/prot/port): (172.17.0.12/255.255.255.255/47/0)
        current_peer 172.17.0.12 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
 local crypto endpt.: 172.17.0.11, remote crypto endpt.: 172.17.0.12
 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
 current outbound spi: 0x38C04B36(952126262)
 inbound esp sas:
  spi: 0xA2EC557(170837335)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Transport, }
    conn id: 5, flow_id: SW:5, crypto map: vpnprof-head-1
    sa timing: remaining key lifetime (k/sec): (4515510/3395)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
 inbound ah sas:
 inbound pcp sas:
 outbound esp sas:
  spi: 0x38C04B36(952126262)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Transport, }
    conn id: 6, flow_id: SW:6, crypto map: vpnprof-head-1
    sa timing: remaining key lifetime (k/sec): (4515511/3395)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
 outbound ah sas:
 outbound pcp sas:
```

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

トンネル保護による IPsec 共有の機能情報

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 *18*：トンネル保護による *IPsec* 共有の機能情報

機能名	リリース	機能情報
トンネル保護による IPSec 共有	Cisco IOS XE Release 2.5	トンネル保護による IPsec 共有機能を使用すると、IPsec セッションを 2 つ以上の GRE トンネル インターフェイス間で共有できます。 Cisco IOS XE Release 2.5 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 この機能により、次のコマンドが変更されました。**tunnelprotectionipsecprofileshared**

用語集

GRE：総称ルーティング カプセル化。トンネルを構成することにより、共有 WAN 全体に特定の経路を確保するとともに、特定の宛先へトラフィックを確実に送り届けるため新たなパケット ヘッダーでトラフィックをカプセル化します。トラフィックにとってトンネルの入口となるのはエンドポイントに限られるため、プライベートなネットワークを実現できます。トンネルそのものは、暗号化のように高い機密性を確保する手段にはなりませんが、暗号化されたトラフィックをトンネル経由で送信することは可能です。

GRE トンネリングを使用すると、非 IP トラフィックを IP にカプセル化して、インターネットや IP ネットワーク上に送信することもできます。非IP トラフィックに該当するのは、インターネット パケット交換（IPX）プロトコルや AppleTalk プロトコルなどのトラフィックです。

IKE：インターネット キー交換。Oakley キー交換や Skeme キー交換を ISAKMP フレームワーク内部に実装したハイブリッド プロトコルです。IKE は、他のプロトコルでも使用できますが、初期実装されるのは IPsec です。IKE は、IPsec ピアを認証し、IPsec キーをネゴシエーションし、IPsec セキュリティ アソシエーションを実行します。

IPsec：IP Security。IETF によって開発されたオープン規格のフレームワークです。IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で実装され、Cisco ルータなどの参加している IPsec デバイス（ピア）の間の IP パケットを保護および認証します。

ISAKMP：Internet Security Association Key Management Protocol。ペイロード形式、キー交換プロトコル実装の方法、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワークです。

NHRP：Next Hop Resolution Protocol。ルータ、アクセス サーバ、およびホストにおいて、非ブロードキャスト マルチアクセス（NBMA）ネットワークに接続された他のルータおよびホストのアドレスを検出する際に使用されるプロトコルです。

シスコによる NHRP の実装では、IETF ドラフト バージョン 11 の NBMA NHRP をサポートしています。

また、IP バージョン 4 および IPX ネットワーク層をサポートしているほか、リンク層では、ATM、イーサネット、SMDS、およびマルチポイント トンネル ネットワークもサポートしています。NHRP はイーサネット上で使用できますが、イーサネットではブロードキャストが可能であるため、NHRP をイーサネット メディアに実装する必要はありません。IPX に対してイーサネットのサポートは不要です（サポートはありません）。

SA：セキュリティ アソシエーション。2 つ以上のエンティティ間で、安全な通信を行うためのセキュリティ サービスをどのように使用するかを規定したものです。たとえば IPsec の SA では、IPsec 接続の際に使用される暗号化アルゴリズム（使用される場合）、認証アルゴリズム、および共有セッション キーが定義されます。

IPsec および IKE では、接続パラメータの識別に必ず SA が使用されます。IKE では、独自に SA をネゴシエーションして確立できます。IPsec の SA は、IKE により確立することも、ユーザ設定により確立することもできます。

トランスフォーム：データフローに対し、データ認証、データの機密性の確保、およびデータ圧縮を目的として行われる一連の処理。トランスフォームには、Hash-based Message Authentication Code（HMAC）-Message Digest Algorithm（MD5）認証アルゴリズムを使用する Encapsulating Security Payload（ESP）プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する Authentication Header（AH）プロトコル、および HMAC-Secure Hash Algorithm（SHA）認証アルゴリズムを使用する ESP プロトコルなどがあります。

トンネル：2 つのピア間（2 台のルータ間など）のセキュアな通信パス。トンネル モードで IPsec を使用することではありません。

VPN：バーチャル プライベート ネットワーク。複数のピアで構成されるフレームワークで、各ピア間では、他のパブリック インフラストラクチャを介して機密データがセキュアに転送されます。このフレームワークでは、すべてのデータをトンネルして暗号化するプロトコルによって、着信ネットワーク トラフィックおよび発信ネットワーク トラフィックが保護されます。また、ネットワークをローカル トポロジの外部にまで拡張できるほか、リモート ユーザがダイレクト ネットワーク接続の状況を確認したり、その機能を利用したりすることも可能です。

第 12 章

DMVPN の Per-Tunnel QoS

DMVPN の Per-Tunnel QoS 機能は、DMVPN のトンネルごとの QoS サポートを提供し、IPSec トンネル インターフェイスのトンネルごとの QoS パフォーマンスを向上させます。

（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 の Per-Tunnel QoS の前提条件

- DMVPN の Per-Tunnel QoS 機能を設定する前に、シスコ エクスプレス フォワーディング スイッチングを設定する必要があります。
- スポークで Next Hop Resolution Protocol（NHRP）グループを設定し、ハブの QoS ポリシーに NHRP グループをマッピングするには、トンネルごとの QoS を使用しない DMVPN 用にスポークおよびハブを設定しておく必要があります。

DMVPN の Per-Tunnel QoS の制約事項

- DMVPN の Per-Tunnel QoS 機能では、次のカプセル化およびトランスポート プロトコルの組み合わせのみがサポートされます。
  - DMVPN 経由の IPv4 の Per-Tunnel QoS と IPv4 トランスポート（Cisco IOS XE Release 3.6S 以降で有効）。
  - DMVPN 経由の IPv6 の Per-Tunnel QoS と IPv4 トランスポート（Cisco IOS XE Release 3.8S 以降で有効）。
  - DMVPN 経由の IPv4 の Per-Tunnel QoS と IPv6 トランスポート（Cisco IOS XE Release 3.11S 以降で有効）。
  - DMVPN 経由の IPv6 の Per-Tunnel QoS と IPv6 トランスポート（Cisco IOS XE Release 3.11S 以降で有効）。
  - DMVPN 経由の MPLS VPN の Per-Tunnel QoS と IPv4 トランスポート（2547oDMVPN）（Cisco IOS XE Release 3.15S 以降で有効）。
  - DMVPN 経由の MPLS VPN の Per-Tunnel QoS と IPv6 トランスポート（2547oDMVPN）（Cisco IOS XE Release 3.15S 以降で有効）。
- ある特定の DMPVN トンネル インターフェイスの場合、1 つのトランスポート プロトコルとして、IPv4 または IPv6 のみを使用できます。ただし、同じデバイスでも別の DMVPN トンネル インターフェイスでは IPv4 または IPv6 トランスポート プロトコルを同時に使用できます。Per-Tunnel QoS を IPv4 および IPv6 DMVPN パッセンジャのトラフィック パケット用に設定して、アウトバウンド物理インターフェイス（IPv4 か IPv6、またはその両方）に関連付けることができます。独自の制限付き QoS ポリシーが設定されたアウトバウンド物理インターフェイスでは、この DMVPN トンネル トラフィックで DMVPN 以外の IPv4 または IPv6 トラフィック、もしくは両方を混在させることができます。
- DMVPN の Per-Tunnel QoS 機能は、次をサポートしません。

- DMVPN 経由の IPv4、IPv6、または MPLS（マルチプロトコル ラベル スイッチング）VPN の Per-Tunnel QoS とレイヤ 2 トンネル プロトコル（L2TP）トランスポート。
- ポートチャネル インターフェイスまたは集約ポートチャネル インターフェイスでの DMVPN 経由の IPv4、IPv6、または MPLS VPN の Per-Tunnel QoS。

- Per-Tunnel QoS サービス ポリシーは出力方向でのみサポートされます。
- この機能では、クリプトエンジンの前にユーザがキューイングおよびスケジューリングを設定できる機能の追加はサポートされません。
- IP アドレスが変わらない外部ヘッダーが個々のフローキューの選択に使用されるため、均等化キューイングは DMVPN の Per-Tunnel QoS ポリシー マップでは使用しないでください。均等化キューイングを使用すると、そのクラスを通過するすべてのトラフィックに対して同じキューが選択されることになります。
- QoS サービス ポリシーは、DMVPN トンネル インターフェイスで Per-Tunnel QoS サービス ポリシーとともにトンネルが発信される、メイン インターフェイスまたはサブインターフェイスでサポートされます。ただし、メインまたはサブインターフェイスのサービス ポリシーについては、次のような一定の制限があります。
  - サービス ポリシーは、Per-Tunnel QoS サービス ポリシーとともにメイン インターフェイスまたはサブインターフェイスのいずれかでサポートされますが、両方ではサポートされません。
  - メイン インターフェイスまたはサブインターフェイスの QoS サービス ポリシーは、クラスデフォルトのシェーパーのみに制限されます（含めることができるのは **class class-default** コマンドと **shape** コマンドのみです）。2 つの異なる QoS サービス ポリシーがメイン インターフェイスまたはサブインターフェイスとトンネル インターフェイスに同時に適用されている場合、QoS 設定をメイン インターフェイスまたはサブインターフェイスに追加できません。
  - メイン インターフェイスまたはサブインターフェイスの QoS サービス ポリシーは、トンネル インターフェイスのサービス ポリシーより先に適用する必要があります。
  - メインインターフェイスまたはサブインターフェイスの QoS サービス ポリシーは、QoS サービス ポリシーをトンネル インターフェイスに適用したときにのみ有効性が確認されます。メインインターフェイスまたはサブインターフェイスのサービス ポリシーは、トンネルの移動または変更時にはチェックされません。
  - メイン インターフェイスまたはサブインターフェイスのポリシー マップに新しいクラスまたは機能を追加する操作はサポートされていません。新しいクラスまたは機能が CLI でブロックされることはありませんが、予期しない動作を引き起こす可能性があります。
  - メイン インターフェイスまたはサブインターフェイスのサービス ポリシーに対する policy-map カウンタ（**show policy-map interface** コマンドで出力される）では、すべてのパケットが計上されない場合があるため、使用または参照しないでください。ただし、これによって QoS 機能が影響を受けることはありません。この場合も、メインインター

フェイスまたはサブインターフェイス上のトラフィック（そのインターフェイス上のすべてのDMVPNトンネル トラフィックを含む）は、シェーパーによって制限されます。

DMVPN の Per-Tunnel QoS について

DMVPN の Per-Tunnel QoS の概要

Dynamic Multipoint VPN（DMVPN）の Per-Tunnel QoS 機能を使用すると、トンネル別インスタンス（スポーク別ベース）で DMVPN ハブからスポークへのトンネルの出力方向で、DMVPN ハブに Quality of Service（QoS）ポリシーを適用できます。トンネル別インスタンスの DMVPN ハブに対する QoS ポリシーにより、各スポークにトンネル トラフィックをシェーピングし（親ポリシー）、ポリシングのためにトンネルを通る個別のデータ フローを区別（子ポリシー）できます。特定のスポークにハブが使用する QoS ポリシーは、そのスポークが設定されている特定の NHRP（Next Hop Resolution Protocol）グループに基づいて選択されます。同じ NHRP グループに複数のスポークを設定できますが、各スポークのトンネル トラフィックは個別に測定されてシェーピングおよびポリシングされます。

この機能は、インターネット プロトコル セキュリティ（IPSec）を使用するかどうかにかかわらず、DMVPN で使用できます。

DMVPN の Per-Tunnel QoS 機能をイネーブルにすると、総称ルーティング カプセル化（GRE）/IPsec トンネル パケットのアウトバウンド物理インターフェイスでキューイングとシェーピングが実行されます。DMVPN の Per-Tunnel QoS 機能を使用すると、QoS でのパケットのシェーピングと帯域幅キューイングに関するパケットサイズの計算に GRE ヘッダー、IPsec ヘッダー、レイヤ 2（物理インターフェイス用）ヘッダーが含まれるようになります。

DMVPN の Per-Tunnel QoS の利点

DMVPN の Per-Tunnel QoS 機能を導入する前に、すべてのスポークの集約された発信トラフィックまたはスポーク別（手動による各種の設定が必要）の発信トラフィックのいずれかのみを測定するように、Dynamic Multipoint VPN（DMVPN）ハブの Quality of Service（QoS）を設定することができます。

DMVPN の Per-Tunnel QoS 機能には次の利点があります。

- QoS ポリシーが DMVPN ハブにアタッチされ、トンネル トラフィックをマッチングする基準が各スポーク レジスタとして自動的にハブで設定される（手動による各種の設定が不要）。
- ハブからスポークへのトラフィックをスポーク別に制限できる。
- ハブは過剰なトラフィックを小さなスポークに送信（およびオーバーラン）できない。
- 「使用量の多い」スポークが使うアウトバウンド ハブ帯域幅の量を制限できるため、トラフィックによってハブのリソースが独占されて他のスポークがリソースを使えなくなる事態を回避できる。

DMVPN の NHRP QoS プロビジョニング

Next Hop Resolution Protocol（NHRP）は、NHRP グループを使用して DMVPN の Per-Tunnel QoS 機能をプロビジョニングします。

NHRP グループはこの機能で導入された新機能で、Dynamic Multipoint VPN（DMVPN）ノード（スポーク）によって DMVPN ハブに伝送されるグループ ID 情報です。ハブはこの情報を使って、ローカルで定義されている、リモート ノードの Quality of Service（QoS）ポリシー インスタンスを選択します。

DMVPN 総称ルーティング カプセル化（GRE）トンネル インターフェイス上のスポーク ルータで NHRP グループを設定できます。NHRP グループ名は、スポークからハブに定期的に送信される NHRP 登録要求ごとにハブに送信されます。

NHRP グループと QoS ポリシーのマッピングは、ハブ DMVPN GRE トンネル インターフェイスで設定されます。スポークから受信された NHRP グループ ストリングは、ハブツースポーク トンネルに出力方向で適用される QoS ポリシーにマッピングされます。

スポークに NHRP グループを設定しても、ハブにはすぐに送信されません。次の定期登録要求時に送信されます。スポークは、GRE トンネル インターフェイスごとに 1 つの NHRP グループのみに属することができます。スポークを複数の DMVPN ネットワーク（複数の GRE トンネル インターフェイス）の一部として設定する場合は、GRE トンネルインターフェイスごとに異なる NHRP グループ名をスポークに設定できます。

スポークから NHRP グループが受信されない場合は QoS ポリシーが適用されず、そのスポークにすでに適用されている QoS ポリシーはすべて削除されます。前の NHRP 登録で NHRP グループが受信されていない場合にスポークから NHRP グループが受信されると、対応する QoS ポリシーが適用されます。以前の NHRP 登録要求と同じ NHRP グループをスポークから受信した場合、そのスポークにはすでに QoS ポリシーが適用されていることになるため、何も実行されません。前の NHRP 登録要求時とは異なった NHRP グループをスポークから受信すると、適用されている QoS ポリシーはすべて削除され、新しい NHRP グループに対応した QoS ポリシーが適用されます。

スポーク間接続のトンネルごとの QoS

QoS：DMVPN のスポーク間 Per-Tunnel QoS 機能により、DMVPN クライアントは Next Hop Resolution Protocol（NHRP）を使用してスポークツースポーク接続を構築し、トンネル別 QoS ポリシーを使用している別の DMVPN クライアントとのダイレクト クリプト トンネルを確立できます。

この機能によって適応型 QoS over DMVPN 機能が拡張され、使用可能な帯域幅に基づく動的シェーパーを使って効率的に帯域幅を管理できるようになります。

スポークツースポーク接続は、**nhrp attribute group** コマンドを使用してスポークで設定されたグループ ID 情報が、NHRP ベンダー プライベート拡張（VPE）によってスポーク間で交換されるときに確立されます。NHRP ベンダー プライベート拡張は、NHRP 制御パケット（NHRP 解決要求および応答のパケット）にカプセル化されています。

ネットワークの 2 つのスポーク（スポーク A とスポーク B）がハブに接続されているとします。スポーク A に **nhrp attribute group** コマンドが設定され、スポーク A とスポーク B の間にトラ

フィックが存在する場合、スポーク A からの解決要求にベンダープライベート拡張（VPE）の一部としてグループ ID 情報が含まれます。スポーク B は解決要求を受信すると、VPE ヘッダーを抽出し、解決要求パケットの一部として受信した拡張タイプを確認します。VPE 拡張にグループタイプが含まれている場合、NHRP VPE パーサーでグループ情報が抽出され、一致するマップが存在するかどうかが確認されます。一致するマップが見つかると、QoS は対象のインターフェイスでポリシーを適用します。

DMVPN の Per-Tunnel QoS の設定方法

DMVPN の Per-Tunnel QoS 機能を設定するには、スポークに Next Hop Resolution Protocol（NHRP）グループを定義し、その NHRP グループをハブの Quality of Service（QoS）ポリシーにマッピングします。

スポークでの NHRP グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interfacetunnel***number*
4. 次のいずれか 1 つを入力します。
   - **ipnhrpgroup***group-name*
   - **nhrpgroup***group-name*
5. **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	**configure terminal** 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 1`	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。

ステップ 4	次のいずれか 1 つを入力します。
	• **ipnhrpgroup***group-name*
	• **nhrpgroup***group-name*
	
	例：
	`Device(config-if)# ip nhrp group spoke_group1`
	
	例：
	`Device(config-if)# nhrp group spoke_group1`
		スポークに Next Hop Resolution Protocol（NHRP）グループを設定します。

ステップ 5	**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。

スポークでの NHRP グループ属性の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interfacetunnel***number*
4. **nhrpgroup***group-name*
5. **nhrpattributegroup***group-name*
6. **nhrpmapgroup***group-name***service-policyoutput***qos-policy-map-name*
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	**configure terminal** 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 1`	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。
ステップ 4	**nhrpgroup***group-name* 例： `Device(config-if)# nhrp group spoke_group1`	スポークに Next Hop Resolution Protocol（NHRP）グループを設定します。
ステップ 5	**nhrpattributegroup***group-name* 例： `Device(config-if)# nhrp group attribute spoke1`	スポークに QoS グループ ID 情報を設定します。
ステップ 6	**nhrpmapgroup***group-name***service-policyoutput***qos-policy-map-name* 例： `Device(config-if)# nhrp map group spoke_group1 service-policy output group1_parent`	Quality of Service（QoS）ポリシーマッピングに Next Hop Resolution Protocol（NHRP）グループを追加します。
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。

ハブの QoS ポリシーへの NHRP グループのマッピング

手順の概要

1. **enable**
2. **configure terminal**
3. **interfacetunnel***number*
4. 次のいずれかを実行します。
   - **ipnhrpmapgroup***group-name***service-policyoutput***qos-policy-map-name*
   - **nhrpmapgroup***group-name***service-policyoutput***qos-policy-map-name*
5. **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	**configure terminal** 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 1`	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。
ステップ 4	次のいずれかを実行します。 • **ipnhrpmapgroup***group-name***service-policyoutput***qos-policy-map-name* • **nhrpmapgroup***group-name***service-policyoutput***qos-policy-map-name* 例： `Device(config-if)# ip nhrp map group spoke_group1 service-policy output group1_parent`	ハブの Quality of Service（QoS）ポリシー マッピングに Next Hop Resolution Protocol（NHRP）グループを追加します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# nhrp map group spoke_group1 service-policy output group1_parent`	
ステップ 5	**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 の Per-Tunnel QoS の確認

手順の概要

1. **enable**
2. **showdmvpndetail**
3. **show ip nhrp**
4. **showipnhrpgroup** [*group-name*]
5. 次のいずれかを実行します。
   - **showipnhrpgroup-map** [*group-name*]
   - **shownhrpgroup-map** [*group-name*]
6. **showpolicy-mapmultipoint** [**tunnel***tunnel-interface-number*]
7. **showtunnelendpoints**

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	**showdmvpndetail** 例： `Device# show dmvpn detail`	各セッションの Dynamic Multipoint VPN（DMVPN）詳細情報（ネクスト ホップ サーバ（NHS）および NHS のステータス、暗号セッション情報、ソケットの詳細など）を表示します。

	コマンドまたはアクション	目的
		• 出力には、スポークから受信した Next Hop Resolution Protocol（NHRP）グループ、およびスポーク トンネルに適用されている Quality of Service（QoS）ポリシーが含まれます。
ステップ 3	**show ip nhrp** 例： `Device# show ip nhrp`	NHRP キャッシュと、スポークから受信した NHRP グループを表示します。
ステップ 4	**showipnhrpgroup** [*group-name*] 例： `Device# show ip nhrp group`	NHRP グループ マッピングを表示します。 • 出力には、関連付けられた QoS ポリシーの名前とその QoS ポリシーを使用しているトンネル エンドポイントのリストが含まれます。

ステップ 5	次のいずれかを実行します。
	• **showipnhrpgroup-map** [*group-name*]
	• **shownhrpgroup-map** [*group-name*]
	例：
	`Device# show ip nhrp group-map group1-parent`
	例：
	`Device# show nhrp group-map group1-parent`
		ハブで設定されているグループとポリシーのマップ、および QoS ポリシーが適用されているトンネルを表示します。

ステップ 6	**showpolicy-mapmultipoint** [**tunnel***tunnel-interface-number*] 例： `Device# show policy-map multipoint tunnel 1`	マルチポイント トンネルに適用されている QoS ポリシーの詳細を表示します。
ステップ 7	**showtunnelendpoints** 例： `Device# show tunnel endpoints`	マルチポイント トンネルの送信元および宛先エンドポイントに関する情報、およびスポーク トンネルで適用されている QoS ポリシーを表示します。

DMVPN の Per-Tunnel QoS の設定例

例：スポークでの NHRP グループの設定

次の例では、3 つのスポークに 2 つの Next Hop Resolution Protocol（NHRP）グループを設定する方法を示します。

1 番目のスポークの設定

```
interface tunnel 1
 ip address 209.165.200.225 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp group spoke_group1
 ip nhrp map 209.165.200.226 203.0.113.1
 ip nhrp map multicast 203.0.113.1
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
 ip tcp adjust-mss 1360
 ip nhrp nhs 209.165.200.226
 tunnel source fastethernet 2/1/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
 ip address 203.0.113.2 255.255.255.0
```

2 番目のスポークの設定

```
interface tunnel 1
 ip address 209.165.200.227 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp group spoke_group1
 ip nhrp map 209.165.200.226 203.0.113.1
 ip nhrp map multicast 203.0.113.1
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
 ip tcp adjust-mss 1360
 ip nhrp nhs 209.165.200.226
 tunnel source fastethernet 2/1/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
 ip address 203.0.113.3 255.255.255.0
```

3 番目のスポークの設定

```
interface tunnel 1
 ip address 209.165.200.228 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp group spoke_group2
 ip nhrp map 209.165.200.226 203.0.113.1
 ip nhrp map multicast 203.0.113.1
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
```

```
 ip tcp adjust-mss 1360
 ip nhrp nhs 209.165.200.226
 tunnel source fastethernet 2/1/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
 ip address 203.0.113.4 255.255.255.0
```

例：スポークでの NHRP グループ属性の設定

次の例では、2 つのスポークに 2 つの Next Hop Resolution Protocol（NHRP）グループ属性を設定する方法を示します。

1 番目のスポークの設定

```
class-map match-any class2
match ip precedence 5
end
!
policy-map p2
class class2
priority percent 60
end
!
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip mtu 1436
 ip nhrp authentication h1there
 ip nhrp attribute group1
 ip nhrp map group group1 service-policy output p2
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 253
 ip nhrp nhs 10.0.0.1
 ip nhrp registration timeout 600
 ip nhrp cache non-authoritative
 no ip mroute-cache
 tunnel source 172.17.0.2
 tunnel mode gre multipoint
 tunnel key 253
 tunnel protection ipsec profile dmvpn-profile
end
```

2 番目のスポークの設定

```
class-map match-any class1
 match ip precedence 5

policy-map policy p1
 class class1
  priority 70

interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1436
 ip nhrp authentication h1there
 ip nhrp attribute group1
 ip nhrp map group group1 service-policy output p1
 ip nhrp map multicast 172.17.0.2
 ip nhrp map 10.0.0.2 172.17.0.2
 ip nhrp network-id 253
 ip nhrp nhs 10.0.0.2
 ip nhrp registration timeout 600
 ip nhrp cache non-authoritative
 no ip mroute-cache
```

```
 tunnel source 172.17.0.1
 tunnel mode gre multipoint
 tunnel key 253
 tunnel protection ipsec profile dmvpn-profile
end
```

例：ハブの QoS ポリシーへの NHRP グループのマッピング

次の例では、ハブの Quality of Service（QoS）ポリシーに Next Hop Resolution Protocol（NHRP）グループをマッピングする方法を示します。この例に示す階層型 QoS ポリシー（親：group1_parent/group2_parent、子：group1/group2）は、Dynamic Multipoint VPN（DMVPN）の Per-Tunnel QoS 機能の設定に使用されます。またこの例では、ハブで、NHRP グループ spoke_group1 を QoS ポリシー group1_parent に、NHRP グループ spoke_group2 を QoS ポリシー group2_parent にそれぞれマップする方法も示しています。

```
class-map match-all group1_Routing
 match ip precedence 6
class-map match-all group2_Routing
 match ip precedence 6
class-map match-all group2_voice
 match access-group 100
class-map match-all group1_voice
 match access-group 100
policy-map group1
 class group1_voice
    priority 1000
 class group1_Routing
    bandwidth percent 20
policy-map group1_parent
 class class-default
    shape average 3000000
  service-policy group1
policy-map group2
 class group2_voice
    priority percent 20
 class group2_Routing
    bandwidth percent 10
policy-map group2_parent
 class class-default
    shape average 2000000
  service-policy group2
interface tunnel 1
 ip address 209.165.200.225 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp map multicast dynamic
 ip nhrp map group spoke_group1 service-policy output group1_parent
 ip nhrp map group spoke_group2 service-policy output group2_parent
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
 ip nhrp registration unique
 tunnel source fastethernet 2/1/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN
interface fastethernet 2/1/1
 ip address 209.165.200.226 255.255.255.224
```

例：DMVPN の Per-Tunnel QoS の確認

次の例では、スポークから受信された Next Hop Resolution Protocol（NHRP）グループに関する情報と、各スポーク トンネルに適用されている Quality of Service（QoS）ポリシーを表示する方法を示します。このコマンドはハブで実行できます。

```
Device# show dmvpn 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 209.165.200.225, VRF ""
   Tunnel Src./Dest. addr: 209.165.200.226/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
Type:Hub, Total NBMA Peers (v4/v6): 3
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1   209.165.200.227     192.0.2.2     UP 00:19:20    D        192.0.2.2/32
NHRP group: spoke_group1
 Output QoS service-policy applied: group1_parent
    1   209.165.200.228     192.0.2.3     UP 00:19:20    D        192.0.2.3/32
NHRP group: spoke_group1
 Output QoS service-policy applied: group1_parent
    1    209.165.200.229     192.0.2.4     UP 00:19:23    D        192.0.2.4/32
NHRP group: spoke_group2
 Output QoS service-policy applied: group2_parent
Crypto Session Details:
--------------------------------------------------------------------------------
Interface: tunnel1
Session: [0x04AC1D00]
  IKE SA: local 209.165.200.226/500 remote 209.165.200.227/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 209.165.200.227
  IPSEC FLOW: permit 47 host 209.165.200.226 host 209.165.200.227
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x9B264329, transform : ah-sha-hmac
    Socket State: Open
Interface: tunnel1
Session: [0x04AC1C08]
  IKE SA: local 209.165.200.226/500 remote 209.165.200.228/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 209.165.200.228
  IPSEC FLOW: permit 47 host 209.165.200.226 host 209.165.200.228
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x36FD56E2, transform : ah-sha-hmac
    Socket State: Open
Interface: tunnel1
Session: [0x04AC1B10]
  IKE SA: local 209.165.200.226/500 remote 209.165.200.229/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 209.165.200.229
  IPSEC FLOW: permit 47 host 209.165.200.226 host 209.165.200.229
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xAC96818F, transform : ah-sha-hmac
    Socket State: Open
Pending DMVPN Sessions:
```

次に、スポークから受信された NHRP グループに関する情報を表示する方法の例を示します。このコマンドはハブで実行できます。

```
Device# show ip nhrp

192.0.2.240/32 via 192.0.2.240
   Tunnel1 created 00:22:49, expire 00:01:40
```

```
   Type: dynamic, Flags: registered
   NBMA address: 209.165.200.227
     Group: spoke_group1
192.0.2.241/32 via 192.0.2.241
   Tunnel1 created 00:22:48, expire 00:01:41
   Type: dynamic, Flags: registered
   NBMA address: 209.165.200.228
     Group: spoke_group1
192.0.2.242/32 via 192.0.2.242
   Tunnel1 created 00:22:52, expire 00:03:27
   Type: dynamic, Flags: registered
   NBMA address: 209.165.200.229
     Group: spoke_group2
```

次に、ハブの NHRP グループ マッピングの詳細、およびマッピングで定義されている各 NHRP グループを使用しているトンネルのリストを表示する方法の例を示します。このコマンドはハブで実行できます。

```
Device# show ip nhrp group-map

Interface: tunnel1
          NHRP group: spoke_group1
  QoS policy: group1_parent
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  198.51.100.220/203.0.113.240
  198.51.100.221/203.0.113.241
          NHRP group: spoke_group2
  QoS policy: group2_parent
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  198.51.100.222/203.0.113.242
```

次に、トンネル エンドポイントに適用されている特定の QoS ポリシーに関する統計情報を表示する方法の例を示します。このコマンドはハブで実行できます。

```
Device# show policy-map multipoint

Interface tunnel1 <--> 203.0.113.252
          Service-policy output: group1_parent
    Class-map: class-default (match-any)
      29 packets, 4988 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 750 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 3000000, bc 12000, be 12000
      target shape rate 3000000
      Service-policy : group1
        queue stats for all priority classes:
          queue limit 250 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: group1_voice (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: access-group 100
          Priority: 1000 kbps, burst bytes 25000, b/w exceed drops: 0
        Class-map: group1_Routing (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 6
          Queueing
          queue limit 150 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 20% (600 kbps)
        Class-map: class-default (match-any)
          29 packets, 4988 bytes
```

```
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
          queue limit 350 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
Interface tunnel1 <--> 203.0.113.253
          Service-policy output: group1_parent
    Class-map: class-default (match-any)
      29 packets, 4988 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 750 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 3000000, bc 12000, be 12000
      target shape rate 3000000
      Service-policy : group1
        queue stats for all priority classes:
          queue limit 250 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: group1_voice (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: access-group 100
          Priority: 1000 kbps, burst bytes 25000, b/w exceed drops: 0
        Class-map: group1_Routing (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 6
          Queueing
          queue limit 150 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 20% (600 kbps)
        Class-map: class-default (match-any)
          29 packets, 4988 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
          queue limit 350 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
Interface tunnel1 <--> 203.0.113.254
           Service-policy output: group2_parent
    Class-map: class-default (match-any)
      14 packets, 2408 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 2000000, bc 8000, be 8000
      target shape rate 2000000
      Service-policy : group2
        queue stats for all priority classes:
          queue limit 100 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: group2_voice (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: access-group 100
          Priority: 20% (400 kbps), burst bytes 10000, b/w exceed drops: 0
        Class-map: group2_Routing (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 6
          Queueing
          queue limit 50 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

```
  bandwidth 10% (200 kbps)
Class-map: class-default (match-any)
  14 packets, 2408 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  queue limit 350 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```

DMVPN の Per-Tunnel QoS の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
IP NHRP コマンド	『Cisco IOS IP Addressing Services Command Reference』
基本的なシスコ エクスプレス フォワーディングの設定	『*IP Switching Cisco Express Forwarding Configuration Guide*』
NHRP の設定	『*IP Addressing: NHRP Configuration Guide*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

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 の Per-Tunnel QoS 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 *19*：***DMVPN*** の ***Per-Tunnel QoS*** の機能情報

機能名	リリース	機能情報
Per-Tunnel QoS	Cisco IOS XE Release 3.11S	DMVPN の Per-Tunnel QoS 機能は、DMVPN のトンネルごとの QoS サポートを提供し、IPSec トンネル インターフェイスのトンネルごとの QoS パフォーマンスを向上させます。 Cisco IOS XE Release 3.11S では、この機能が強化されて IPv6 アドレスがサポートされるようになりました。 次のコマンドが導入または変更されました。**ip nhrp group**、**ip nhrp map**、**ip nhrp map group**、**nhrp group**、**nhrp map group**、**show dmvpn**、**show ip nhrp**、**show ip nhrp group-map**、**show nhrp group-map**、**show policy-map multipoint tunnel**
QoS：DMVPN のスポーク間 Per-Tunnel QoS	Cisco IOS XE Release 3.15S	QoS：DMVPN のスポーク間 Per-Tunnel QoS 機能により、DMVPN クライアントは Next Hop Resolution Protocol（NHRP）を使用してスポークツースポーク接続を構築し、トンネル別 QoS ポリシーを使用している別の DMVPN クライアントとのダイレクト クリプト トンネルを確立できます。 次のコマンドが導入または変更されました。**nhrp attribute group**、**show dmvpn**、**show ip nhrp**、**show ip nhrp group**

第 13 章

TrustSec DMVPN インライン タギング サポートの設定

TrustSec DMVPN インライン タギング サポート機能により、IPsec は Cisco TrustSec（CTS）セキュリティ グループ タグ（SGT）を IPsec ピア間で伝送できます。

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。

TrustSec DMVPN インライン タギング サポートの設定の前提条件

インターネット キー交換バージョン 2（IKEv2）および IPsec をルータで設定する必要があります。詳細については、「Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site」および「Configuring Security for VPNs with IPsec」の章を参照してください。

この機能は、Cisco ISR G2 890、1900、2900、3900、および 3900E ルータでのみサポートされています。

TrustSec DMVPN インライン タギング サポートの設定に関する制約事項

TrustSec DMVPN インライン タギング サポート機能は IKEv2 でのみネゴシエート可能で、IKEv2 を使用して次をサポートします。

- DMVPN
- ダイナミック仮想トンネル インターフェイス（dVTI）
- トンネル保護を使用した GRE
- サイト間 VPN
- スタティック クリプト マップ
- スタティック仮想トンネル インターフェイス（sVTI）

TrustSec DMVPN インライン タギング サポート機能は、次をサポートしません。

- Cisco AnyConnect
- Cisco VPNClient
- IKEv1 を使用した DMVPN
- EasyVPN
- FlexVPN
- GetVPN
- IKEv1 IPsec メソッド
- SSLVPN

TrustSec DMVPN インライン タギング サポートの設定について

Cisco TrustSec

Cisco TrustSec（CTS）アーキテクチャでは、ID、信頼性、およびポリシーを組み合わせ、ユーザトランザクションを保護してロールベースのポリシーを適用することで、信頼できるネットワーク デバイスのドメインを確立し、セキュアなネットワークを構築できます。CTS は認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、CTS ネットワークへの進入時にパケットにタグを付けることで各パケットの分類が維持されます。これにより、パケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。パケットまたはフレームは、スイッチやファイアウォールなどのネットワーク中継を可能にするセキュリティ グループ タグ（SGT）を使用してタグ付けされ、分類に基づいてアクセス コントロール ポリシーが適用されます。

TrustSec の IPsec インライン タギング機能は、SGT を他のネットワーク デバイスに伝播する際に使用します。

（注） この機能がサポートされていない場合は、SGT Exchange Protocol over TCP（SXP）機能を使用できます。

CTS および SXP の詳細については、『Cisco TrustSec Switch Configuration Guide』を参照してください。

SGT および IPsec

IPsec はアルゴリズム、キー、および機能のネゴシエーションに IKE プロトコルを使用します。IKEv2 は、IPSec のネゴシエーションと SGT 機能に関する通知に使用されます。ピアで SGT タギング機能が認識されると、SGT タグ番号（16 ビット）が SGT Cisco メタデータ（CMD）ペイロードとして IPsec に追加され、受信側のピアに送信されます。

アクセス レイヤ デバイスが着信パケットを認証します。アクセス レイヤ デバイスは認証サーバから SGT を受信し、IP アドレスと SGT を着信パケットに割り当てます。つまり、IP アドレスを SGT にバインドします。この IP アドレスと SGT のバインディングがアップストリーム デバイスに伝搬され、SGT ベースのポリシーとインライン タギングが適用されます。

発信側で IKEv2 が SGT 機能をネゴシエートするように設定されている場合、発信側は SA_INIT 要求で SGT 機能情報を提示します。応答側で IKEv2 が SGT 機能をネゴシエートするように設定されている場合、応答側が SA_INIT 応答で確認応答し、発信側と応答側はピアへのすべてのパケットに対してインライン タギングを使用することを IPsec に通知します。

ピアでインライン タギングがサポートされている場合、出力時に IPsec は SGT 機能とプレフィクスを IPsec ペイロードに追加します。サポートされていない場合、パケットはタグ付けされません。

入力時に、IPsec は SGT 機能についてパケットを検査します。タグが使用可能な場合、IPsec はタグ情報を取得してデバイスに情報を渡します（インライン タギングがネゴシエートされる場合のみ）。タグがないパケットは、IPsec によって通常のパケットとして処理されます。

次の表で、出力および入力時の IPsec の動作について説明します。

表 *20*：出力パスでの *IPsec* の動作

インライン タギングのネゴシエーション	**CTS** による **SGT** の提供	**IPsec** の動作
Yes	Yes	SGT CMD をパケットに追加します。
Yes	No	SGT CMD を追加せずにパケットを送信します。
No	Yes または No	SGT CMD を追加せずにパケットを送信します。

表 *21*：入力パスでの *IPsec* の動作

パケットのタグ付け	インライン タギングのネゴシエーション	**IPsec** の動作
Yes	Yes	パケットの SGT CMD を処理します。
Yes	No	パケットの SGT CMD を処理しません。
No	Yes または No	パケットを通常の IPsec パケットとして処理します。

IKEv2 の発信側と応答側での SGT

IKEv2 セッションで SGT をイネーブルにするには、**crypto ikev2 cts** コマンドを使用して SGT 機能サポートをピアに送信する必要があります。SGT はシスコ独自の機能です。したがって、SA_INIT 交換ではベンダー ID（VID）ペイロードとして送信されます。

次の表で、SGT 機能が発信側と応答側で設定されているシナリオについて説明します。

表 *22* : *IKEv2* の発信側と応答側の *SGT* 機能

SGT が発信側でイネーブル	SGT が応答側でイネーブル	動作..
Yes	Yes	発信側と応答側の間で VID が交換され、SGT インライン タギング機能で IPsec SA がイネーブルになります。
Yes	No	発信側は VID を提示しますが、応答側は VID を無視します。IPsec SA は SGT インライン タギング機能でイネーブルになりません。
No	Yes	発信側は VID を提示せず、応答側は VID ペイロードを送信しません。IPsec SA は SGT インラインタギング機能でイネーブルになりません。
No	No	発信側は VID を提示せず、応答側も VID ペイロードを送信しません。IPsec SA は SGT インラインタギング機能でイネーブルになりません。

フラグメンテーションの処理

フラグメンテーションは、次の 2 つの方法で処理されます。

- IPsec 前のフラグメンテーション：IPsec がフラグメント化されたパケットを受信すると、各フラグメントがタグ付けされます。
- IPsec 後のフラグメンテーション：IPsec パケットが暗号化後にフラグメント化された場合、最初のフラグメントがタグ付けされます。

TrustSec DMVPN インライン タギング サポートの設定方法

IPsec インライン タギングのイネーブル化

はじめる前に

IKEv2 および IPsec を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sgt inline**
4. **exit**

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	**configure terminal** 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	**cts sgt inline** 例： `Device(config)# cts sgt inline`	DMVPN の TrustSec をイネーブルにします。このコマンドは、総称ルーティング カプセル化（GRE）とトンネル インターフェイス モードに対してのみ有効です。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

TrustSec DMVPN インライン タギング サポートのモニタリングと確認

TrustSec DMVPN インライン タギング サポート設定をモニタおよび確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show dmvpn**
3. **show ip nhrp nhs detail**
4. **show tunnel endpoints**
5. **show adjacency***interface-type interface-number* **detail**

手順の詳細

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。

ステップ 2 **show dmvpn**

例：
```
Device# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 1.1.1.99              10.1.1.99    UP 00:00:01    SC
```
Dynamic Multipoint VPN（DMVPN）固有のセッション情報を表示するには、このコマンドを使用します。

ステップ 3 **show ip nhrp nhs detail**

例：
```
Device# show ip nhrp nhs detail

Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.99  RE NBMA Address: 1.1.1.99 priority = 0 cluster = 0  req-sent 44  req-failed 0  repl-recv
 43 (00:01:37 ago)
 TrustSec Enabled
```

Next Hop Resolution Protocol（NHRP）ネクスト ホップ サーバ（NHS）情報を表示するには、このコマンドを使用します。

ステップ 4 **show tunnel endpoints**

例：

```
Device# show tunnel endpoints

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 1.1.1.99 Refcount 3 Base 0xF3FB79B4 Create Time 00:03:15
   overlay 10.1.1.99 Refcount 2 Parent 0xF3FB79B4 Create Time 00:03:15
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries; TrustSec enabled
```

マルチポイント総称ルーティング カプセル化（mGRE）モードでトンネルを実行している場合に、トンネル エンドポイントのアドレス解決に使用されるトンネル エンドポイント データベースの内容を表示するには、このコマンドを使用します。

ステップ 5 **show adjacency***interface-type interface-number* **detail**

例：

```
Device# show adjaceny tunnel0 detail

Protocol Interface                 Address
IP       Tunnel0                   10.1.1.99(2)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 1
                                   Encap length 32
                                   4500000000000000FF2FB76901010101
                                   0101016300008909080001010001000 0
                                   Tun endpt
                                   Next chain element:
.
.
.
```

プロトコルに関する情報を表示するには、このコマンドを使用します。

TrustSec DMVPN インライン タギング サポートの設定例

例：IPsec インライン タギングのイネーブル化

次の例では、スタティック VTI の発信側とダイナミック VTI の応答側で IPsec インライン タギングをイネーブルにする方法を示します。この設定を使用してクリプト マップおよび VTI を設定できます。

スタティック VTI の発信側の設定

```
crypto ikev2 proposal p1
 encryption 3des
 integrity md5
```

```
 group 2
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address ::/0
  pre-shared-key cisco
 !
 peer v4
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
!
!
crypto ikev2 profile prof3
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
!
crypto ikev2 cts sgt
!
crypto ipsec transform-set trans esp-3des esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set trans
 set ikev2-profile prof3
 match address ipv4acl
!
!
interface Loopback1
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001::4:1/112
!
interface Loopback2
 ip address 209.165.200.1 255.255.255.224
 ipv6 address 2001::40:1/112
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.210.74 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.240.0.0
 duplex auto
 speed auto
 ipv6 address 2001::5:1/112
 ipv6 enable
 crypto map cmap
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.16.0.2
ip route 10.12.255.200 255.0.0.0 172.31.255.254
!
ip access-list extended ipv4acl
 permit ip host 209.165.201.1host 192.168.12.125
 permit ip host 209.165.200.1 host 172.18.0.1
 permit ip host 172.28.0.1 host 10.10.10.1
 permit ip host 10.12.255.200 host 192.168.14.1
!
logging esm config
```

```
ipv6 route ::/0 2001::5:2
!
!
!
!
!!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
```

ダイナミック VTI の応答側の設定

```
crypto ikev2 proposal p1
 encryption 3des
 integrity md5
 group 2
!
crypto ikev2 policy policy1
 proposal p1
!
crypto ikev2 keyring key
 peer peer
  address 172.160.1.1 255.240.0.0
  pre-shared-key cisco
 !
 peer v4_p2
  address 172.31.255.1 255.240.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring key
 virtual-template 25
!
crypto ikev2 cts sgt
!
crypto ipsec transform-set trans esp-null esp-sha-hmac
!
crypto ipsec profile prof_ipv4
 set transform-set trans
 set ikev2-profile prof1_ipv4
!
!
interface Loopback0
 ip address 192.168.12.1 255.255.0.0
!
interface Loopback1
 no ip address
!
interface Loopback2
 ip address 172.18.0.1 255.240.0.0
!
```

```
interface Loopback10
 no ip address
 ipv6 address 2001::8:1/112
!
interface Loopback11
 no ip address
 ipv6 address 2001::80:1/112
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.0.0.0
 duplex auto
 speed auto
 ipv6 address 2001::7:1/112
 ipv6 enable
!
interface GigabitEthernet0/1
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.210.144 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 no ip address
 shutdown
!
interface FastEthernet0/0/1
 no ip address
!
interface FastEthernet0/0/2
 no ip address
!
interface FastEthernet0/0/3
 no ip address
!
!
interface Virtual-Template25 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile prof_ipv4
!
interface Vlan1
 no ip address
!
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 172.17.0.0 255.240.0.0 10.10.10.1
!
logging esm config
ipv6 route ::/0 2001::7:2
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2
 no activation-character
 no exec
```

```
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

TrustSec DMVPN インライン タギング サポートの参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
Cisco TrustSec および SXP の設定	『Cisco TrustSec Switch Configuration Guide』
IPsec の設定	*IPsec* を使用した *VPN* のセキュリティの設定
IKEv2 の設定	『*Configuring Internet Key Exchange Version 2 (IKEv2) and FlexVPN Site-to-Site*』
Cisco Secure Access Control Server	Cisco Secure ACS のコンフィギュレーション ガイド

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

TrustSec DMVPN インライン タギング サポートの機能情報

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 *23*：*TrustSec DMVPN* インライン タギング サポートの設定に関する機能情報

機能名	リリース	機能情報
TrustSec DMVPN インライン タギング サポート	Cisco IOS XE Release 3.13S	TrustSec DMVPN インライン タギング サポート機能により、IPsec は Cisco TrustSec（CTS）セキュリティ グループ タグ（SGT）を IPsec ピア間で伝送できます。 次のコマンドが導入または変更されました。**cts sgt inline**、**show dmvpn**、**show ip nhrp nhs**、**show tunnel endpoints**、**show adjacency**

第 14 章

スポーク間 NHRP サマリー マップ

スポーク間 NHRP サマリー マップ機能は、ネットワーク上の NHRP 解決トラフィックを集約および削減します。

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。

スポーク間 NHRP サマリー マップについて

スポーク間 NHRP サマリー マップ

DMVPN フェーズ 3 では、ルート集約がハブで実行されます。ハブは、スポークが別のスポークの背後にあるネットワークに到達するためのネクストホップです。パケットを受信すると、ハブはローカル スポークにリダイレクト メッセージを送信し、宛先ネットワークの Next Hop Resolution Protocol（NHRP）解決要求を送信するように指示します。この解決要求がハブによって宛先 LAN ネットワークのリモート スポークに転送されます。リモート スポークは解決要求に応答し、ローカル スポークとのトンネルを開始します。

スポークはローカル ホストの NHRP 解決要求に応答するときに、ルーティング情報ベース（RIB）の明示的な IP アドレス ネットワークとサブネット マスクを使用します。リモート スポークの背後にあるホストがローカル スポークの背後にあるネットワーク内のホストとパケットを交換するには、これらの複数のネットワークに同様の NHRP メッセージが必要です。膨大な数のスポークや各スポークの背後にある大規模なネットワークに対する NHRP メッセージを処理することは困難です。

最初の NHRP 解決応答で、特定のネットワークではなくローカル スポークの背後にあるネットワークに関する情報が提供されるときの、スポーク間の NHRP メッセージの数を制限できます。スポーク間 NHRP サマリー マップでは、NHRP 解決応答で RIB の IP アドレス ネットワークとサブネット マスクではなく、設定済みの IP アドレス ネットワークとサブネット マスクを使用します。RIB に含まれる IP アドレス ネットワークの数が、設定済みの IP アドレス ネットワークより多い（サブネット マスク長がより短い）場合も、スポークは設定済みの IP アドレス ネットワークとサブネット マスクを NHRP 解決応答で使用します。これにより、ネットワーク内の NHRP 解決トラフィックが集約および削減されます。スポークで NHRP サマリー マップを設定するには、**ipnhrpsummary-map** コマンドを使用します。

スポーク間 NHRP サマリー マップの動作の仕組み

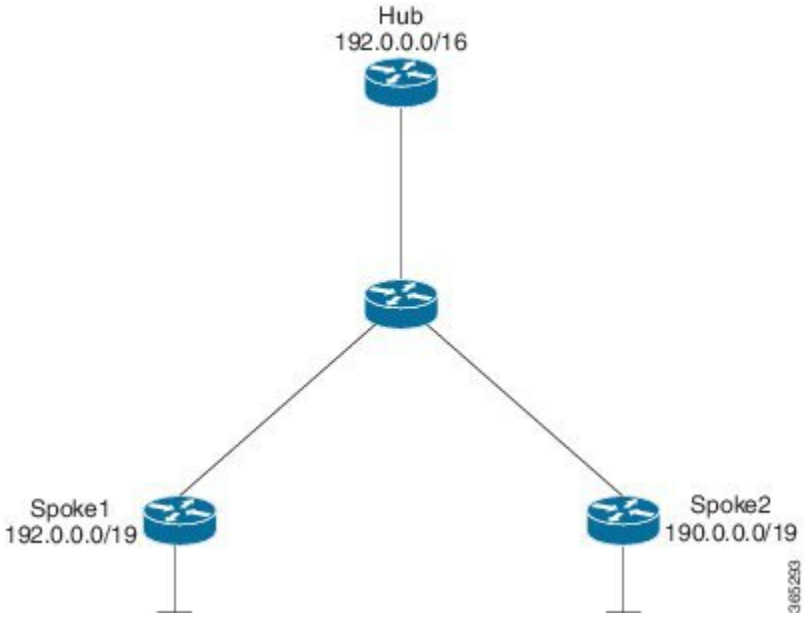
解決要求を受信すると、スポークは次のように動作します。

1. RIB で IP アドレスとサブネット マスクを参照して返します。
2. IP アドレスとサブネット マスクを設定済みの NHRP サマリー マップと照合し、宛先 IP アドレスが含まれているかどうかを確認します。
3. NHRP 解決応答でサマリー マップをリモート スポークに送信します。リモート スポークの NHRP はローカル スポークのネクストホップを使って IP アドレスとサブネット マスクを RIB に追加します。

ローカル スポークの背後にあるネットワーク全体が、1 つの NHRP 解決要求によってリモート スポークで識別されます。

次の図に、スポーク間 NHRP サマリー マップの仕組みを示します。

図 *9*：スポーク間 *NHRP* サマリー マップ



ローカル LAN 上にあるアドレス空間 192.0.0.0/19 のローカル スポークには、すべての 32-24 RIB エントリ（192.0.0.0/24,….192.0.31.0/24）があります。このローカル アドレス空間のアドバタイズに EIGRP のようなルーティング プロトコルが使用される場合、ネットワークを 192.0.0.0/19 に集約してハブにアドバタイズするようにルーティング プロトコルが設定されます。ハブはこれを 192.0.0.0/16 にさらに集約して他のスポークにアドバタイズします。他のスポークは、RIB 内のハブのネクストホップを使用して、192.0.0.0/16 ルーティング テーブル エントリでのみ始まります。

リモート ホストが 192.0.12.1 と通信する場合、ローカル スポークは 192.0.12.1/32 の NHRP 解決要求を受信します。ローカル スポークは RIB を参照し、NHRP 解決応答で 192.0.12.0/24 を返します。

ローカル スポークに NHRP サマリー マップ（例：ip nhrp summary-map 192.0.0.0/19）が設定されている場合、ローカル スポークが 192.0.12.1 の解決要求を受信して RIB を確認すると、192.0.12.0/24 が返されます。次にローカル スポークは、サマリー マップ設定 192.0.0.0/19 で宛先 192.0.12.1/32 が含まれているかどうかを確認し、NHRP 解決応答で 192.0.0.0/19 を返します。

IPv6 オーバーレイに対する NHRP サマリー マップ サポート

スポーク間 NHRP サマリー マップ機能は IPv6 でサポートされており、**ipv6nhrpsummary-map** コマンドを使用して設定します。

スポーク間 NHRP サマリー マップの設定方法

スポークでのスポーク間 NHRP サマリー マップの設定

（注） 次の作業によってスポーク デバイスを設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacetunnel***number*
4. **ipaddress***ip-addressmasksecondaryip-addressmask*
5. **ipnhrpauthentication***string*
6. **ipnhrpsummary-map** {*ip-address*|*mask*}
7. **ipnhrpnetwork-id***number*
8. **ipnhrpnhs** [*hub-tunnel-ip-address*] **nbma** [*hub-wan--ip*] **multicast**
9. **ipnhrpshortcut**
10. **tunnelsource** {*ip-address* | *typenumber*}
11. **tunnelmodegremultipoint**
12. **tunnelkey***key-number*
13. **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*：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	**ipaddress***ip-addressmasksecondaryip-addressmask* 例： `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	トンネル インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 （注） 同一の DMVPN ネットワーク内に存在するすべてのハブおよびスポークには、同じ IP サブネットに属するアドレスを指定する必要があります。
ステップ 5	**ipnhrpauthentication***string* 例： `Device(config-if)# ip nhrp authentication donttell`	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。
ステップ 6	**ipnhrpsummary-map** {*ip-address*|*mask*} 例： `Device(config-if)# ip nhrp summary-map 10.0.0.0/24`	ネットワーク上の NHRP 解決トラフィックを集約および削減します。
ステップ 7	**ipnhrpnetwork-id***number* 例： `Device(config-if)# ip 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。 • *number*：非ブロードキャスト マルチアクセス（NBMA）ネットワークの、グローバルに一意である 32 ビット ネットワーク識別子を指定します。
ステップ 8	**ipnhrpnhs** [*hub-tunnel-ip-address*] **nbma** [*hub-wan--ip*] **multicast** 例： `Device(config-if)# ip nhrp nhs 10.0.0.1 nbma 172.17.0.1 multicast`	ハブ ルータを NHRP ネクストホップ サーバとして設定します。
ステップ 9	**ipnhrpshortcut** 例： `Device(config-if)# ip 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。

	コマンドまたはアクション	目的
ステップ 10	**tunnelsource** {*ip-address* | *typenumber*} 例： `Device(config-if)# tunnel source Gigabitethernet 0/0/0`	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	**tunnelmodegremultipoint** 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マルチポイント総称ルーティング カプセル化（mGRE）に設定します。 • この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。
ステップ 12	**tunnelkey***key-number* 例： `Device(config-if)# tunnel key 100000`	（任意）トンネルインターフェイスのIDキーをイネーブルにします。 • *key-number*：トンネル キーを識別するための数値を指定します。同一のDMVPNネットワーク内に存在するすべてのハブおよびスポークに対して、同じ値を設定する必要があります。
ステップ 13	**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。

スポーク間 NHRP サマリー マップの確認

手順の概要

1. **enable**
2. **showipnhrp**

手順の詳細

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　showipnhrp

例：
次に、スポークでの show コマンドの出力例を示します。

```
Device# show ip nhrp

15.0.0.1/32 (vrf1) via 15.0.0.1
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: used
   NBMA address: 123.0.0.1
15.0.0.20/32 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router nhop rib
   NBMA address: 42.0.0.1
190.0.0.0/22 (vrf1) via 15.0.0.10
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: local
   NBMA address: 121.0.0.1
    (no-socket)
201.0.0.0/22 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router rib nho
   NBMA address: 42.0.0.1
```

Next Hop Resolution Protocol（NHRP）マッピングの情報を表示します。

スポーク間 NHRP サマリー マップのトラブルシューティング

手順の概要

1. **debug dmvpn all nhrp**

手順の詳細

debug dmvpn all nhrp
スポークが解決要求に対して受信した IP アドレスとサブネット マスクを確認します。

例：

```
Device# debug dmvpn all nhrp
```

```
NHRP-RT: Attempting to create instance PDB for vrf global(0x0)(0x0)
NHRP-CACHE: Tunnel0: Cache add for target 67.0.0.1/32 vrf global(0x0) label none next-hop 67.0.0.1


NHRP-CACHE: Tunnel0: Cache add for target 67.0.0.0/24 vrf global(0x0) label none next-hop 15.0.0.30

            80.0.0.1
NHRP-CACHE: Inserted subblock node(2 now) for cache: Target 67.0.0.0/24 nhop 15.0.0.30
NHRP-CACHE: Converted internal dynamic cache entry for 67.0.0.0/24 interface Tunnel0 vrf global(0x0)
 to external
NHRP-RT: Adding route entry for 67.0.0.0/24 (Tunnel0 vrf:global(0x0)) to RIB
NHRP-RT: Route addition to RIB Successful
NHRP-RT: Route watch started for 67.0.0.0/23
NHRP-CACHE: Updating label on Tunnel0 for 15.0.0.30 vrf global(0x0), old none new none nhop 15.0.0.30
NHRP-CACHE: Tunnel0: Cache update for target 15.0.0.30/32 vrf global(0x0) label none next-hop
15.0.0.30
            80.0.0.1
NHRP-CACHE: Deleting incomplete entry for 67.0.0.1/32 interface Tunnel0 vrf global(0x0)
NHRP-CACHE: Still other cache entries with same overlay nhop 67.0.0.1
NHRP-RT: Received route watch notification for  67.0.0.0/24
NHRP-RT: Covering prefix is 67.0.0.0/22
NHRP-RT: Received route watch notification for  67.0.0.0/24
NHRP-RT: (0x0):NHRP RIB entry for  67.0.0.0/24  is unreachable
```

スポーク間 NHRP サマリー マップの設定例

例：スポーク間 NHRP サマリー マップ

例：スポーク間 NHRP サマリー マップ

次に、サマリー マップ用にハブで DMVPN フェーズ 3 を設定する例を示します。

```
interface Tunnel0
 ip address 15.0.0.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 2
 ip nhrp authentication cisco123
 ip nhrp network-id 23
 ip nhrp redirect
 ip summary-address eigrp 2 190.0.0.0 255.255.252.0
 ip summary-address eigrp 2 201.0.0.0 255.255.252.0
 tunnel source GigabitEthernet1/0/0
 tunnel mode gre multipoint
 tunnel key 6
end
```

次の例では、スポーク 1 でスポーク間 NHRP サマリー マップを設定する方法を示します。

```
interface Tunnel0
 vrf forwarding vrf1
 ip address 15.0.0.10 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp summary-map 190.0.0.0/22
 ip nhrp network-id 5
```

```
 ip nhrp nhs 15.0.0.1 nbma 123.0.0.1 multicast
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1/0
 tunnel mode gre multipoint
 tunnel key 6
end
```

次の例では、スポーク 2 でスポーク間 NHRP サマリー マップを設定する方法を示します。

```
interface Tunnel0
 ip address 15.0.0.20 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp summary-map 201.0.0.0/22
 ip nhrp network-id 5
 ip nhrp nhs 15.0.0.1 nbma 123.0.0.1 multicast
 ip nhrp shortcut
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 6
end
```

次に、ハブでの show ip nhrp コマンドの出力例を示します。

```
Device# show ip nhrp

15.0.0.10/32 via 15.0.0.10
   Tunnel0 created 00:22:26, expire 00:07:35
   Type: dynamic, Flags: registered used nhop
   NBMA address: 41.0.0.1
15.0.0.20/32 via 15.0.0.20
   Tunnel0 created 00:13:43, expire 00:09:36
   Type: dynamic, Flags: registered used nhop
   NBMA address: 42.0.0.1
```

次に、スポーク 1 での show ip nhrp コマンドの出力例を示します。

```
Device# show ip nhrp

15.0.0.1/32 (vrf1) via 15.0.0.1
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: used
   NBMA address: 123.0.0.1
15.0.0.20/32 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router nhop rib
   NBMA address: 42.0.0.1
190.0.0.0/22 (vrf1) via 15.0.0.10
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: local
   NBMA address: 121.0.0.1
    (no-socket)
201.0.0.0/22 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router rib nho
   NBMA address: 42.0.0.1
```

次に、スポーク 2 での show ip nhrp コマンドの出力例を示します。

```
Device# show ip nhrp

15.0.0.1/32 via 15.0.0.1
   Tunnel0 created 09:08:16, never expire
   Type: static, Flags: used
   NBMA address: 123.0.0.1
15.0.0.10/32 via 15.0.0.10
   Tunnel0 created 00:00:04, expire 01:59:55
```

```
   Type: dynamic, Flags: router nhop rib
   NBMA address: 121.0.0.1
190.0.0.0/22 via 15.0.0.10
   Tunnel0 created 00:00:04, expire 01:59:55
   Type: dynamic, Flags: router rib nho
   NBMA address: 121.0.0.1
201.0.0.0/22 via 15.0.0.20
   Tunnel0 created 09:08:16, never expire
   Type: static, Flags: local
   NBMA address: 42.0.0.1
    (no-socket)
```

スポーク間 NHRP サマリー マップの参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

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

スポーク間 NHRP サマリー マップの機能情報

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 *24*：スポーク間 *NHRP* サマリー マップの機能情報

機能名	リリース	機能情報
スポーク間 NHRP サマリー マップ	Cisco IOS XE Release 3.17S	スポーク間 Next Hop Resolution Protocol（NHRP）サマリー マップ機能は、ネットワーク上の NHRP 解決トラフィックを集約および削減します。 この機能により、次のコマンドが導入または変更されました。**ip nhrp summary-map**、**ipv6 summary-map**

第 15 章

DMVPN での BFD サポート

DMVPN での双方向フォワーディング検出（BFD）サポートにより、障害検出通知が迅速に制御プロトコルに送信され、ネットワーク全体のコンバージェンス時間が短縮されることで、高速ピア障害検出が実現します。

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 での BFD サポートの前提条件

DMVPN の BFD は IPv4 と IPv6 の両方のオーバーレイ アドレスをサポートしており、転送アドレス ファミリに依存しません。

BFD の前提条件の詳細については、「Prerequisites for Bidirectional Forwarding Detection」を参照してください。

DMVPN での BFD サポートに関する制約事項

- 現在、NHRP は BFD のダウン イベントでのみ機能します。アップ イベントでは機能しません。
- BFD サポートを受ける BFD を両方のピアで設定する必要があります。いずれかのピアに BFD が設定されていないと、もう 1 つのピアはダウン状態または不明な状態の BFD セッションを作成します。
- ポイントツーポイント（P2P）トンネルの場合は、DMVPN での BFD サポートを設定する前に、ネクスト ホップ サーバ（NHS）を設定する必要があります。
- スポーク間更新が想定どおりに動作するように、ピアに設定された BFD 間隔は BFD エコー モードと同じである必要があります。
- Cisco アグリゲーション サービス ルータ 1000 シリーズでは、現在プラットフォームの BFD セッション数が 4095 に制限されているため、BFD を設定した単一の DMVPN ハブを最大 4095 セッションまで拡張できます。クラスタリング、サーバ ロードバランシング（SLB）、階層設計などの通常の方法で従来どおりに DMVPN を拡大縮小することもできます。これは、BFD が設定されていない DMVPN のスケールには影響しません。

DMVPN での BFD サポートについて

BFD の動作

BFD は、インターフェイス、データリンク、および転送プレーンを含めて、2 つの隣接ルータ間の転送パスで、オーバーヘッドの少ない短期間の障害検出方法を提供します。

BFD はインターフェイス レベルおよびプロトコル レベルでイネーブルにする検出プロトコルです。シスコでは BFD 非同期モードをサポートしています。このモードは、2 台のシステム間で BFD 制御パケットを送信することでルータ間の BFD ネイバー セッションをアクティブ化して維持します。したがって、BFD セッションを作成するには、両方のシステム（または BFD ピア）で BFD を設定する必要があります。適切なプロトコル（NHRP およびオーバーレイに関するルーティング プロトコル）に対して、インターフェイス レベルおよびルータ レベルで BFD をイネーブル

にすると、BFD セッションが作成されて BFD タイマーがネゴシエートされます。BFD ピアはネゴシエートされた間隔で BFD 制御パケットの相互送信を開始します。

DMVPN での BFD サポートの利点

- リンク障害をより速く検出できます。
- 非暗号化の導入環境の場合、スポークは NHRP 登録がタイムアウトするまでハブの障害を検出できません。また、ハブはルーティングによる再コンバージェンスが早い段階で可能であっても、ハブのキャッシュが期限切れになるまでスポークの障害を検出できません。BFD ではこのような障害を迅速に検出できます。
- たとえばハブがスポークの代わりに応答するように設定されている場合に、BFD は権限のないセッション間の転送パスを検証します。
- BFD はトンネルを通過しない IKE キープアライブまたは DPD とは異なり、トンネルを含むエンドツーエンドのデータ パスを検証します。
- BFD プローブはオフロード可能です。

DMVPN での BFD サポート用に特別な NHRP 設定を行う必要はありません。NHRP 対応インターフェイスで BFD をイネーブルにするだけです。DMVPN 設定については、「Dynamic Multipoint VPN の設定方法」を参照してください。

DMVPN での BFD サポートの設定方法

DMVPN での BFD サポートの設定

BFD 間隔は、次のようにトンネル インターフェイスで直接設定できます。

```
enable
configure terminal
interface tunnel1
bfd interval 1000 min_rx 1000 multiplier 5
no echo
```

次に示すように、テンプレートを定義してトンネルインターフェイスに適用することで、BFD 間隔を設定することもできます

```
enable
configure terminal
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 5
interface tunnel1
bfd template sample
```

例：DMVPN での BFD サポート

例：DMVPN での BFD サポート

次に、ハブで DMVPN での BFD サポートを設定する例を示します。

```
bfd-template single-hop sample
 interval min-tx 1000 min-rx 1000 multiplier 5
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp network-id 5
 ip nhrp redirect
 ip mtu 1400
 ip tcp adjust-mss 1360
 bfd template sample
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 6
!
interface GigabitEthernet0/0/0
 ip address 10.0.0.1 255.0.0.0
 negotiation auto
!
router eigrp 2
network 10.0.0.0 0.0.0.255
bfd all-interfaces
auto-summary
!
```

次に、スポークで DMVPN での BFD サポートを設定する例を示します。

```
bfd-template single-hop sample
 interval min-tx 1000 min-rx 1000 multiplier 5
!
interface Tunnel1
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp network-id 5
 ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
 bfd template sample
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 6
!
interface GigabitEthernet0/0/0
 mtu 4000
 ip address 11.0.0.1 255.0.0.0
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/0/1
 mtu 6000
 ip address 111.0.0.1 255.255.255.0
 negotiation auto
!
router eigrp 2
 network 11.0.0.0 0.0.0.255
 network 111.0.0.0 0.0.0.255
 network 10.0.0.0 0.0.0.255
bfd all-interfaces
```

```
auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

次に、スポークでのコンバージェンスを高速化する例を示します。

```
interface Tunnel1
ip address 18.0.0.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp network-id 12
ip nhrp nhs 10.0.0.1 nbma 10.0.0.10 multicast
bfd template sample
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel key 18
tunnel protection ipsec profile MY_PROFILE
!
bfd-template single-hop sample
interval min-tx 1000 min-rx 1000 multiplier 3
echo
!
router eigrp 2
bfd interface Tunnel1    ------------------------> Specify the interface on which the routing
 protocol must act for BFD up/down events
network 11.0.0.0 0.0.0.255
network 111.0.0.0 0.0.0.255
```

上記の設定を使用すると、BFD のダウンがレポートされた直後に（3 秒で検出）、EIGRP は RIB からインストールされたルートを削除します。

次の出力例は、ハブのサマリー出力を示しています。

```
device#show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 172.17.0.1             10.0.0.1    UP 00:00:14     D
     1 172.17.0.2             10.0.0.2   BFD 00:00:03     D
```

BFD が新しい状態であるということは、セッションは下位レイヤ（IKE、IPSec、および NHRP）で認識されるように UP 状態ですが、BFD がセッションを DOWN と認識したことを意味します。通常どおり、この状態はセッションが UP 状態ではない最下位レイヤを示しています。また、これは親キャッシュ エントリにのみ適用されます。この原因としては、BFD によって DOWN と検出されたこと、または BFD が反対側で設定されていないことが考えられます。

次の出力例は、スポークのサマリー出力を示しています。

```
device#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
```

```
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2 172.17.0.2             10.0.0.2   BFD 00:00:02   DT1
                              10.0.0.2    UP 00:00:02   DT2
     1 172.17.0.11           10.0.0.11    UP 00:05:35     S
```

次の例は、**show ip/ipv6 nhrp** コマンドの出力を示しています。

```
device#show ip nhrp
10.0.0.2/32 via 10.0.0.2
   Tunnel2 created 00:00:15, expire 00:04:54
   Type: dynamic, Flags: router nhop rib bfd
   NBMA address: 172.17.0.2
10.0.0.11/32 via 10.0.0.11
   Tunnel2 created 00:09:04, never expire
   Type: static, Flags: used bfd
   NBMA address: 172.17.0.11
192.168.1.0/24 via 10.0.0.1
   Tunnel2 created 00:00:05, expire 00:04:54
   Type: dynamic, Flags: router unique local
   NBMA address: 172.17.0.1
    (no-socket)
192.168.2.0/24 via 10.0.0.2
   Tunnel2 created 00:00:05, expire 00:04:54
   Type: dynamic, Flags: router rib nho
   NBMA address: 172.17.0.2
```

上記の例の BFD フラグは、このピアに BFD セッションがあることを意味しています。このマーキングは親エントリ専用です。

次の例は、**show tunnel endpoints** コマンドの出力を示しています。

```
device#show tunnel endpoints
 Tunnel2 running in multi-GRE/IP mode

 Endpoint transport 172.17.0.2 Refcount 3 Base 0x2ABF53ED09F0 Create Time 00:00:07
   overlay 10.0.0.2 Refcount 2 Parent 0x2ABF53ED09F0 Create Time 00:00:07
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 2 entries; BFD(0x2):U
 Endpoint transport 172.17.0.11 Refcount 3 Base 0x2ABF53ED0B80 Create Time 00:09:07
   overlay 10.0.0.11 Refcount 2 Parent 0x2ABF53ED0B80 Create Time 00:09:07
   Tunnel Subblocks:
      tunnel-nhrp-sb:
         NHRP subblock has 1 entries; BFD(0x1):U
```

すべてのトンネル エンドポイントに対して、新しいテキスト「**BFD(handle):state**」が追加されます。状態は UP（U）、DOWN（D）、NONE（N）、または INVALID（I）のいずれかです。

- BFD がピアに設定されていない場合、または最初にセッションが UP ではない場合は、状態が N になります。

次の例は、**show nhrp interfaces** コマンドの出力を示しています。インターフェイス上の設定状態またはグローバルな設定状態が示されます（動作状態ではありません）。

```
device#show nhrp interfaces
NHRP Config State
-----------------
 Global:
    BFD: Registered

 Tunnel1:
    BFD: Disabled

 Tunnel2:
    BFD: Enabled
```

これは内部の隠しコマンドです。現在は、NHRP が BFD のクライアントであるかどうか、および BFD が NHRP インターフェイスでイネーブルになっているかどうかが表示されます。

DMVPN での BFD サポートの参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
『Dynamic Multipoint VPN コンフィギュレーション ガイド』	『Dynamic Multipoint VPN コンフィギュレーション ガイド』
『IP Routing: BFD Configuration Guide』	『IP Routing: BFD Configuration Guide』

MIB

MIB	MIB のリンク
• CISCO-MIB • NHRP MIB • Cisco NHRP Extension MIB • BFD MIB • トンネル MIB • IPSec MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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 での BFD サポートの機能情報

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 *25*：*DMVPN* での *BFD* サポートの機能情報

機能名	リリース	機能情報
DMVPN での BFD サポート	Cisco IOS Release 16.3	DMVPN での双方向フォワーディング検出（BFD）サポート機能により、障害検出通知が迅速にルーティング プロトコルに送信され、ネットワーク全体のコンバージェンス時間が短縮されることで、高速ピア障害検出が実現します。 この機能により、次のコマンドが変更されました。**show dmvpn**、**show ip nhrp**、**show ipv6 nhrp**、**show tunnel endpoints**、**show nhrp interfaces**