NHRP の設定

Next Hop Resolution Protocol（NHRP）は、Non-Broadcast Multi-Access（NBMA）ネットワークをダイナミックにマッピングする Address Resolution Protocol（ARP; アドレス解決プロトコル）と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されたシステムは、そのネットワークに参加している他のシステムの NBMA（物理）アドレスをダイナミックに学習でき、これらのシステムが直接通信できるようになります。

NHRP は、ハブが Next Hop Server（NHS; ネクスト ホップ サーバ）であり、スポークが Next Hop Client（NHC; ネクスト ホップ クライアント）である、クライアントおよびサーバのプロトコルです。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。

このモジュール内の機能情報の検索

ご使用の Cisco IOS ソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「NHRP 設定の機能情報」（P.38）を参照してください。

プラットフォームと、Cisco IOS および Catalyst OS ソフトウェア イメージに関するサポート情報の検索

プラットフォームのサポートと、Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

- 「NHRP について」（P.2）
- 「NHRP の設定方法」（P.9）
- 「NHRP の設定例」（P.30）
- 「参考資料」（P.37）
- 「NHRP 設定の機能情報」（P.38）

NHRP について

NHRP を設定するには、次の概念を理解する必要があります。

- 「NHRP および NBMA のネットワークの相互作用の仕組み」（P.2）
- 「ダイナミックに構築されたハブアンドスポーク ネットワーク」（P.3）
- 「ダイナミック Spoke-to-Spoke トンネル」（P.5）
- 「Spoke-to-Spoke トンネルのスポーク更新メカニズム」（P.8）

NHRP および NBMA のネットワークの相互作用の仕組み

WAN ネットワークのほとんどは、ポイントツーポイント リンクの集まりです。仮想トンネル ネットワーク（Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルなど）もまた、ポイントツーポイント リンクの集まりです。これらのポイントツーポイント リンクの接続を効率的にスケーリングするために、通常は、単一またはマルチレイヤのハブアンドスポーク ネットワークにグループ化します。マルチポイント インターフェイス（GRE トンネル インターフェイスなど）を使用して、このようなネットワークのハブ ルータの設定を減らすことができます。その結果として生じるネットワークが Non-Broadcast Multi-Access（NBMA）ネットワークです。

単一のマルチポイント インターフェイスを通って到達可能なトンネル エンドポイントが複数あるため、この NBMA ネットワーク上で multipoint GRE（mGRE; マルチポイント GRE）トンネル インターフェイスからパケットを転送するには、論理トンネル エンドポイントの IP アドレスから物理トンネル エンドポイントの IP アドレスへのマッピングが必要です。このマッピングはスタティックに設定することが可能ですが、これは、マッピングがダイナミックに検出または学習できる場合に推奨します。

NHRP は、これらの NBMA ネットワークの問題を軽減する ARP と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されているシステムは、ネットワークの一部である他のシステムの NBMA アドレスをダイナミックに学習します。このため、これらのシステムは、トラフィックに中間ホップを使用せずに直接通信できるようになります。

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。部分メッシュ NBMA ネットワークには通常、NBMA ネットワークの背後に複数の論理ネットワークがあります。このような構成において、NBMA ネットワークを通るパケットは、出口ルータ（宛先ネットワークに最も近いルータ）に到着するまでに、NBMA ネットワーク上で複数のホップを発生させる必要がある場合があります。NHRP を IPsec と組み合わせる場合、NBMA ネットワークは基本的には、物理 IP ネットワーク上にあるポイントツーポイントの論理トンネル リンクの集まりです。

これらの NBMA ネットワークをサポートするために、NHRP では次の 2 つの機能を使用できます。

1. NHRP 登録。NHRP を使用して、Next Hop Client（NHC; ネクスト ホップ クライアント）が Next Hop Server（NHS; ネクスト ホップ サーバ）にダイナミックに登録されます。この登録機能により、特に、NHC がダイナミック物理 IP アドレスを持つか、物理 IP アドレスをダイナミックに変更する Network Address Translation（NAT; ネットワーク アドレス変換）ルータの背後にある場合には、NHS で設定を変更しなくても、NHC が NBMA ネットワークに参加できるようになります。この場合、NHC の論理バーチャル プライベート ネットワーク（VPN IP）と物理（NBMA IP）のマッピングを NHS で事前に設定することができません。詳細については、「NHRP 登録」（P.4）を参照してください。
2. NHRP 解決。NHRP を使用して、1 つの NHC（スポーク）は、同じ NBMA ネットワーク内の別の NHC（スポーク）の論理 VPN IP と物理 NBMA IP のマッピングをダイナミックに検出できます。この検出を行わない場合、あるスポークの背後にあるホストから別のスポークの背後にあるホストに向かう IP パケットは、NHS（ハブ）ルータを経由する必要があります。このプロセスは、ハブを出入りするこれらのパケットをマルチポイント インターフェイス上で処理するため、ハブ

の物理帯域幅および CPU の使用率が上がります。NHRP を使用すると、NBMA ネットワークに接続されているシステムは、ネットワークの一部である他のシステムの NBMA アドレスをダイナミックに学習します。このため、これらのシステムは、トラフィックに中間ホップを使用せずに直接通信できるようになります。この機能は、中間ホップ（NHS）の負荷を軽減し、NBMA ネットワークの帯域幅全体を、ハブ ルータの帯域幅よりも広げることができます。

ダイナミックに構築されたハブアンドスポーク ネットワーク

NHRP により、NBMA ネットワークは最初、スポークの NHC とハブの NHS から複数の階層レイヤを構成できるハブアンドスポーク ネットワークとして配置されます。NHC は、NHS に到達するためのスタティック マッピング情報を使用して設定され、NHS に接続して NHRP 登録を NHS に送信します。この設定により、NHS はスポークのマッピング情報をダイナミックに学習できるため、ハブで必要な設定が減り、さらにスポークでダイナミック NBMA（物理）IP アドレスを取得できるようになります。

ベース ハブアンドスポーク ネットワークがダイナミックに構築されると、NHRP 解決の要求と応答を使用して、Spoke-to-Spoke マッピング情報をダイナミックに検出できるため、スポークはハブをバイパスし、直接相互にやり取りできます。このプロセスにより、スタティック完全メッシュ ネットワークを事前設定する必要なく、データ トラフィック パターンに基づいてスポーク間接続のダイナミック メッシュを構築できます。ダイナミック メッシュ ネットワークを使用すると、大規模な NBMA ネットワークの完全メッシュに参加できるリソースのない、より小さいスポーク ルータの場合でも、その性能の範囲で大規模な NBMA ネットワークに参加できるようになります。より小さいスポーク ルータは、可能なすべての Spoke-to-Spoke リンクを構築する必要はありません。これらのルータは現在使用している Spoke-to-Spoke リンクだけを構築する必要があります。

ネクスト ホップ サーバの選択

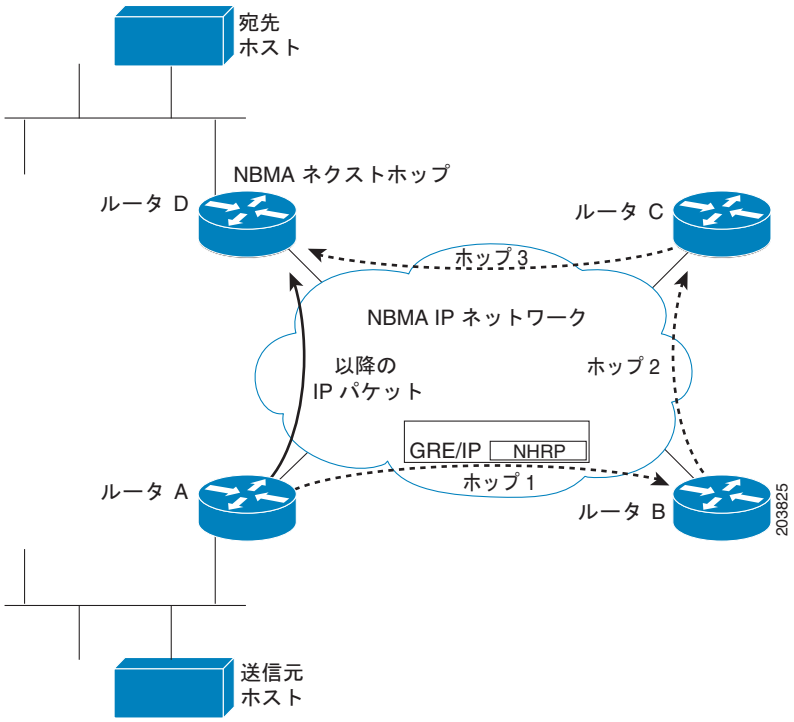
NHRP 解決要求は、ベース ハブアンドスポーク NBMA サブネットワーク内の 1 つ以上のホップ（ハブ）を通ってから、応答を生成するステーションに到達します。各ステーション（送信元ステーションを含む）は、要求を転送するネイバー NHS を選択します。NHS の選択手順では通常、NHRP 要求のネットワーク レイヤの宛先アドレスに基づいたルーティングの決定を行います。NHRP 解決要求は、最終的に NHRP 解決応答を生成するステーションに到着します。この応答側ステーションが宛先を提供するか、またはそれ自体が宛先です。応答側ステーションは、応答を送信する場所を判断するために、NHRP パケット内から送信元アドレスを使用して応答を生成します。

また、シスコによる NHRP の実装では、IEEE RFC 2332『*NBMA Next Hop Resolution Protocol (NHRP)*』のサポートと拡張も行っています。

シスコによる NHRP の実装では、マルチポイント GRE、イーサネット、Switched Multimegabit DataService（SMDS; スイッチド マルチメガビット データ サービス）、フレーム リレー、ATM を使用する、ネットワーク レイヤおよびリンク レイヤで IP バージョン 4 を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することができ、標準のイーサネット IP ARP プロトコルで十分であるため、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。

図 1 に、NBMA ネットワークに接続された 4 台のルータを示します。ルータが GRE IP トンネル パケット内の IP データ パケットをトンネリングして相互に通信するために、ネットワーク内で必要なのは IP ルータです。インフラストラクチャ レイヤのルータは、ホップ 1、ホップ 2、ホップ 3 で示される論理 IP トンネル回線接続をサポートします。ルータ A が送信元ホストから宛先ホストに IP パケットを転送しようとすると、NHRP がトリガーされます。送信元ホストに代わり、ルータ A は、GRE IP パケットにカプセル化された NHRP 解決要求パケットを送信し、このとき宛先ホストに接続されているルータ D に到達するために、ネットワーク上でホップを 3 回発生させます。ルータ A は、NHRP 解決の肯定応答を受信した後、ルータ D が NBMA IP ネクスト ホップであると判断し、この宛先への以降のデータ IP パケットは、GRE IP トンネル ホップ 1 回でルータ D に送信します。

図 1　Next Hop Resolution Protocol



NHRP を使用すると、NBMA ネクスト ホップが決まるとすぐに、送信元は（GRE IP や SMDS などのコネクションレス型 NBMA ネットワーク内で）データ パケットの宛先への送信を開始するか、または宛先への Virtual Circuit（VC; 仮想回線）接続を確立します。この接続は、コネクション型 NBMA ネットワーク（フレーム リレー、ATM など）に必要な帯域幅および Quality of Service（QoS）特性を使用して設定するか、IPsec 暗号化のピアリングを確立する必要がある場合には、Dynamic MultipointVPN（DMVPN; ダイナミック マルチポイント VPN）を使用して設定します。

NHRP が導入されていても同時に、他のアドレス解決方式を使用できます。Logical IP Subnet（LIS; 論理 IP サブネット）モデルに依存する IP ホストでは、NBMA ネットワーク上で ARP のサーバおよびサービスが必要になる場合があります。展開されたホストによっては、NHRP を実装しなくても、ARP の差異に引き続き対応できる場合があります。NHRP は、LIS モデルによって生じる最適ではないルーティングを排除するように設計され、既存の ARP サービスに干渉することなく、その ARP サービスを使用して展開できます。

NHRP 登録

NHRP 登録は、NHRP ホールド時間（**ip nhrp holdtime** *value* コマンドで設定される）の 3 分の 1 の時間ごとに、NHC からその設定済みの NHS に送信されます。ただし、**ip nhrp registration timeout** *value* コマンドが設定されている場合を除きます。この場合、登録は設定されたタイムアウト値に従って送信されます。NHRP 登録要求に対する NHRP 登録応答を受信しなかった場合、NHRP 登録要求は、1、2、4、8、16、32、64 秒のタイムアウトで再送信され、その後は再び 1 秒に戻って繰り返します。

3 回再送信した（7 秒）後、NHRP 登録応答を受信していなければ、NHS はダウンを宣言され、NHRP 解決パケットがその NHS に送信されることも、その NHS を経由することもなくなります。NHRP 登録は、引き続き 1、2、4、8、16、32、64 秒の間隔で送信され、NHRP 登録応答を受信するまで NHS を調査します。NHRP 登録応答を受信するとすぐに NHS はアップを宣言されます。NHRP 登録要求により、NHRP ホールド時間の 3 分の 1 の時間ごと、または **ip nhrp registration timeout** コマンドで設定されたタイムアウト値に従って送信するように戻されるため、NHS は再び NHRP 解決要求を受信できます。**show ip nhrp nhs detail** コマンドを使用して、NHRP NHS のステートを確認できます。

DMVPN により使用される NHRP

NHRP を使用すると、VPN を構築する際に便利です。この説明において、VPN は実際のレイヤ 3 ネットワークの上部に構築された仮想レイヤ 3 ネットワークで構成されます。VPN 上で使用するトポロジは、基盤とするネットワークにほとんど依存関係がありません。また、VPN 上で実行するプロトコルについても、まったく依存関係はありません。Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）は、IPsec に追加して GRE IP トンネルを暗号化することにより、保護が可能となる GRE IP 論理トンネルを基盤としています。

Cisco IOS Release 10.3 以降のリリースを実行するすべてのルータには NHRP を実装できるため、NHS または NHC として動作可能です。NHRP を使用する DMVPN（GRE IP + IPsec）の基本機能を入手するには、Cisco IOS Release 12.3(9)、12.3(8)T、またはそれ以降のリリースを実行する必要があります。

（注） NHRP に対する最新の機能拡張や機能強化を使用するには、Cisco IOS Release 12.4 または Cisco IOS Release 12.4T を使用する必要があります。

ダイナミック Spoke-to-Spoke トンネル

Spoke-to-Spoke トンネルはダイナミックに構築されるように設計されています。つまり、トンネルを使用するデータ トラフィックが存在するときだけ作成され、トンネルを使用しているデータ トラフィックがなくなると削除されます。

NHS による NHC の NHRP 登録の他に、NHRP は、NHC（スポーク）がネットワークのインフラストラクチャ（IP ネットワーク、SMDS）上のショートカット パスを検索したり、スイッチド インフラストラクチャ ネットワーク（フレーム リレーおよび ATM）上で別の NHC（スポーク）に直接向かうショートカット Switched Virtual Circuit（SVC; 相手先選択接続）を構築したりして、NHS（ハブ）経由のホップをバイパスする機能を提供します。この機能により、非常に大規模な NHRP NBMA ネットワークの構築が可能になります。このように、ハブの帯域幅や CPU に制限があっても、NHRP NBMA ネットワークの帯域幅全体は制限を受けません。この機能により、可能なすべての接続を事前に検出せずに、完全メッシュ対応のネットワークを効率的に作成できます。このタイプのネットワークは、ダイナミック メッシュ ネットワークと呼ばれます。このネットワークは、NHRP およびダイナミック ルーティング プロトコル情報（とデータ トラフィック）を送信する NHC と NHS のベース ハブアンドスポーク ネットワーク、およびリンクを使用するデータ トラフィックがあれば作成され、データ トラフィックが止まれば切断されるダイナミック ダイレクト Spoke-to-Spoke リンクで構成されます。

ダイナミック メッシュ ネットワークにより、個々のスポーク ルータは、NBMA ネットワーク内であれば任意の場所に直接接続できます。ただし、同時接続が可能な数には限りがあります。この機能により、ネットワーク内の各スポークは、他のスポークがその性能の範囲で参加することを制限することなく、その性能の範囲ですべてのネットワークに参加できます。完全メッシュ ネットワークを構築する場合、すべてのスポークは、可能なすべてのトンネルを同時に処理できる大きさが必要です。

たとえば、1000 ノードのネットワークの場合、1 つの完全メッシュ スポークが常に 999 個のトンネル（他のノードにそれぞれ 1 つずつ）をサポートする必要があるため、大きくかつ高性能である必要があります。ダイナミック メッシュ ネットワークの場合、1 つのスポークは、その NHS（ハブ）への限られた数のトンネルと、他のスポークへの現在アクティブなトンネルをサポートするだけで済みます。また、スポークがこれ以上 Spoke-to-Spoke トンネルを構築できない場合は、そのデータ トラフィックをスポーク / ハブ / スポーク パス経由で送信します。この設計により、優先する単一ホップ パスを使用できない場合でも、接続が常に必ず維持されるようになります。

DMVPN および NHRP の開発フェーズ

ここで説明する開発フェーズとは、実際に mGRE を NHRP および IPsec と組み合わせる DMVPN フェーズのことです。フェーズ 2 とフェーズ 3 は、ダイナミック Spoke-to-Spoke トンネルのサポートに必要な機能を提供するため重要です。

- **フェーズ 1** はハブアンドスポーク機能のみです。フェーズ 1 は Spoke-to-Spoke トンネルをサポートしないため、ここではこのフェーズについて説明しません。
- **フェーズ 2** では Spoke-to-Spoke 機能を追加します。
- **フェーズ 3** では NBMA ネットワークをより大きくスケーリングするために、Spoke-to-Spoke 機能を変更します。

NHRP は、NBMA ネットワークを通りスポーク / ハブ / スポーク パス経由で送信される NHRP 解決の要求パケットおよび応答パケットを使用して、Spoke-to-Spoke トンネルの作成に必要な情報を集めます。さらに、Spoke-to-Spoke トンネルを構築するためのこの情報を収集するには、NHRP をトリガーするか、NHRP がこの情報を収集するタイミングを把握している必要があります。これは、NHRP は Spoke-to-Spoke トンネルを使用するデータ トラフィックが存在するときだけ Spoke-to-Spoke トンネルを立ち上げるためです。ここでは、NHRP がこれを実行する 2 つの方法について説明します。

NHRP は、NBMA ネットワークを通りスポーク / ハブ / スポーク パス経由で送信される NHRP 解決の要求パケットおよび応答パケットを使用して、Spoke-to-Spoke トンネルの作成に必要な情報を集めます。さらに、Spoke-to-Spoke トンネルを構築するためのこの情報を収集するには、NHRP をトリガーするか、NHRP がこの情報を収集するタイミングを把握している必要があります。これは、NHRP は Spoke-to-Spoke トンネルを使用するデータ トラフィックが存在するときだけ Spoke-to-Spoke トンネルを立ち上げるためです。

ハブ経由で学習される IP ルーティング テーブルおよびルートは、Spoke-to-Spoke トンネルを構築する際に重要です。したがって、NHS（ハブ）の可用性は、NHRP ベースのネットワークが機能するために重要です。ハブが 1 つだけある場合にこのハブがダウンすると、スポークは、そのルーティング ネイバーとしてのハブを失ったため、ハブから学習したルートをそのルーティング テーブルから削除します。ただし、スポークは現在アップしている Spoke-to-Spoke トンネル（NHRP マッピング）のいずれも削除しません。Spoke-to-Spoke トンネルがそのまま存在していても、そのルーティング テーブルに宛先ネットワークへのルートがなくなっているため、スポークはそのトンネルを使用することができません。スポークにパス（Spoke-to-Spoke トンネル）があっても、（ルーティング テーブルのエントリがないため）使用するという認識がありません。

さらに、ルーティング エントリが削除されると、NHRP マッピング エントリを削除するように NHRP がトリガーされることもありません。ハブは使用されていないため、NHRP は、ハブがダウンしたときに持っていた現在のダイナミック NHRP マッピング エントリを最終的にタイムアウトさせます。この時点になって初めて NHRP はマッピング エントリを削除します。

フェーズ 2 では、正しい IP ネクスト ホップを持つルーティング テーブルにルートが残っている場合（多くはスタティック ルート）、ハブがダウンしていても、スポークはその Spoke-to-Spoke トンネルをそのまま使用できます。NHRP 解決の要求または応答はハブを通過する必要があるため、NHRP はマッピング エントリを更新できません。

フェーズ 3 では、トンネル インターフェイスを指し示すルートだけが必要です。正しい IP ネクスト ホップは必要はありません（フェーズ 3 では、NHRP は IP ネクスト ホップを無視します）。また、NHRP 解決の要求または応答はダイレクト Spoke-to-Spoke トンネル上を通るため、NHRP は NHRP マッピング エントリを更新できます。

単一の NBMA ネットワーク内（単一の mGRE、フレーム リレー、ATM インターフェイス）に 2 台（以上）の NHS ハブがある場合、1 台目（プライマリ）のハブがダウンすれば、スポーク ルータはこれまでどおり、このハブから学習したルートをルーティング テーブルから削除しますが、2 台目（バックアップ）のハブから同じルート（より高いメトリック）を再び学習するため、すぐにこれらのルートをインストールします。したがって、Spoke-to-Spoke トラフィックは、Spoke-to-Spoke トンネル上を進み続け、プライマリ ハブの停止による影響を受けません。

ここでは、Spoke-to-Spoke トンネル機能を実装する DMVPN フェーズについて説明します。

フェーズ 2

フェーズ 2 では、NHRP は NHC から NHS へのトンネルを立ち上げ、ダイナミック ルーティング プロトコルを使用して、ハブおよび他のすべてのスポークの背後にある使用可能なすべてのネットワークに関するルーティング情報を配布します。この情報には、特定の宛先ネットワークをサポートしている宛先スポークの IP ネクスト ホップが含まれます。

データ パケットが転送されると、一致するルーティング テーブル ネットワーク エントリから発信インターフェイスおよび IP ネクスト ホップを取得します。NHRP インターフェイスが発信インターフェイスの場合、その IP ネクスト ホップの NHRP マッピング エントリを探します。NHRP マッピング エントリに一致するものがない場合、マッピング情報（物理レイヤ アドレスに対する IP ネクスト ホップ アドレス）を取得するため、NHRP がトリガーされて NHRP 解決要求を送信します。NHRP 登録応答パケットには、このマッピング情報が含まれています。この情報を受信すると、スポークにはデータ パケットを正しくカプセル化するための十分な情報がそろい、インフラストラクチャ ネットワーク上でホップを 1 回発生させて、データ パケットがリモート スポークに直接到達します。この技法のデメリットの 1 つは、ハブと他のスポークの背後にある、すべての可能な宛先ネットワークに対する個別のルートをすべて、各スポークがそのルーティング テーブルに持つ必要がある点です。配布されたこのルーティング情報を保持し、最新の状態を保つことは、VPN 上で実行するルーティング プロトコルに非常に負荷がかかります。

フェーズ 3

フェーズ 3 では、NHRP は NHC と NHS のトンネルを立ち上げ、ダイナミック ルーティング プロトコルを使用して、ハブに対するすべてのスポークの背後にある使用可能なネットワークに関するルーティング情報を配布します。ハブは、次にこのルーティング情報をスポークに再送信しますが、この場合、ハブはルーティング情報をサマライズできます。すべてのネットワークの宛先に対する IP ネクスト ホップが NHS（ハブ）自身になるように設定します。この機能により、ルーティング プロトコルがハブからスポークへの配布に必要な情報の量を著しく削減できるため、ハブで実行しているルーティング プロトコルへの負荷が低減します。

データ パケットが転送されると、一致するルーティング テーブル ネットワーク エントリから発信インターフェイスおよび IP ネクスト ホップを取得します。NHRP インターフェイスが発信インターフェイスの場合、その IP ネクスト ホップの NHRP マッピング エントリを探します。この場合、IP ネクスト ホップになるハブには、NHRP マッピング エントリがすでにあり、そのハブ（NHS）とのトンネルがすでにあるため、スポークはデータ パケットだけをハブに送信します。

ハブはデータ パケットを受信し、そのルーティング テーブルをチェックします。このデータ パケットは、他のスポークの背後にあるネットワーク宛てに送信されているため、NHRP インターフェイスからそのスポークに向かうネクスト ホップに転送して戻されます。この時点で、ハブはパケットが到着し、NHRP インターフェイスから送信して戻されたことを検出します。この動作は、データ パケットが NHRP ネットワーク内で少なくとも 2 回のホップを発生させていることになり、したがって、ハブ経由のこのパスは最適なホップ 1 回のパスではありません。このため、ハブは NHRP リダイレクト メッセージをスポークに送信します。リダイレクト メッセージは、NHRP リダイレクト メッセージをトリガーしたデータ パケット IP 宛先に関する情報をスポークに提供します。

スポークが NHRP リダイレクトを受信すると、スポークは NHRP リダイレクト メッセージのデータ IP 宛先に対する NHRP 解決要求を作成して送信します。NHRP 解決要求は、その IP 宛先のネットワークに対応するリモート スポークへのパスを通って転送されます。

リモート スポークは、NHRP 解決要求パケットのデータ IP 宛先に一致する、独自の NBMA アドレスおよびサブネット全体を（自身のルーティング テーブルから）使用して NHRP 解決応答を生成します。次にリモート スポークは、NHRP 解決応答を送信してローカル スポークに直接返します。この時点で、構築したばかりのダイレクト Spoke-to-Spoke パス上でデータ トラフィックを送信するための十分な情報がそろいます。

（注） フェーズ 3 の方式は、Cisco IOS Release 12.4(6)T で導入され、NHRP の **ip nhrp redirect** および **ip nhrp shortcut** コマンドを使用します。詳細については、「Shortcut Switching Enhancements for NHRP in DMVPN Networks」モジュールを参照してください。

Spoke-to-Spoke トンネルのスポーク更新メカニズム

Spoke-to-Spoke トンネルはダイナミックに構築されるように設計されています。つまり、トンネルを使用するデータ トラフィックが存在するときだけ作成され、トンネルを使用しているデータ トラフィックがなくなると削除されます。ここでは、Spoke-to-Spoke トンネルが使用されている間は更新し（パケット損失なし）、使用されなくなった場合は Spoke-to-Spoke トンネルを検出して削除するメカニズムについて説明します。

プロセス スイッチング

NHRP マッピング エントリを使用して、データ パケットをスイッチングするたびに、マッピング エントリで「used」フラグが設定されます。ここで、NHRP バックグラウンド プロセスが実行されると（60 秒ごと）、次のアクションが発生します。

- 期限が 120 秒より長くかつ「used」フラグが設定されている場合、「used」フラグがクリアされます。
- 期限が 120 秒以内でかつ「used」フラグが設定されている場合、エントリが更新されます。
- 期限が 120 秒以内でかつ「used」フラグが設定されていない場合、何も実行されません。

CEF スイッチング

NHRP には、いつパケットが Spoke-to-Spoke トンネルを通って Cisco Express Forwarding（CEF）スイッチングされるかという情報がありません。

NHRP バックグラウンド プロセスが実行されると、次のアクションが発生します。

- 期限が 120 秒より長い場合、何も実行されません。
- 期限が 120 秒以内の場合、対応する CEF 隣接関係は「古い」とマーク付けされます。このとき、CEF 隣接関係がパケットのスイッチングに使用された場合、CEF は隣接関係を「新しい」とマーク付けし、マッピング エントリを更新するために NHRP をトリガーします。

プロセス スイッチング、CEF スイッチングのどちらの場合でも、更新とは、エントリが期限切れにならないように、他の NHRP 解決の要求が送信され、応答が必要になることを示します。期限が 0 になると、NHRP マッピング エントリは削除されます。また、このエントリがこの NBMA アドレス内の最後のマッピング エントリの場合で、ルータが CEF スイッチングを行っているときは、CEF 隣接関係がクリアされ、不完全とマーク付けされます。

IPsec の **tunnel protection ipsec profile** *name* コマンドを NHRP mGRE インターフェイスで使用する場合は、次のアクションも発生します。

1. 対応する暗号ソケット エントリが削除されます。
2. 対応する暗号マップ エントリが削除されます。
3. 対応する IPsec Security Association（SA; セキュリティ アソシエーション）および Internet Security Association and Key Management Protocol（ISAKMP）SA が削除されます。
4. ISAKMP SA の削除直前に、フェーズ 2 およびフェーズ 1 の削除通知メッセージが ISAKMP ピアに送信されます。

5. ISAKMP ピアは、対応する IPsec SA および ISAKMP SA を削除します。
6. 暗号ソケット経由で、ISAKMP ピアの NHRP マッピング エントリは、スタティック NHRP マッピング エントリである場合を除き、その期限を 5 秒に設定します。
7. NHRP マッピング エントリの期限が切れ、これがこの NBMA アドレス内の最後のマッピング エントリである場合、ISAKMP ピアも項目 1 ～ 5 を実行します。

NHRP の設定方法

基本的な NHRP 機能を実装するには、最初の 2 つの作業を実行する必要があります。NHRP が動作可能になったら、使用しているネットワーク設定に応じて、他の任意の作業を使用して、NHRP の動作をさらに設定または変更できます。

（注） 次の作業では、DMVPN（IPsec を使用する GRE IP）は、NHRP を使用する場合の主要なソリューションであるため、すべての例に引用されています。

ここでは、次の手順について説明します。

- 「マルチポイント動作のための GRE トンネルの設定」（P.9）（必須）
- 「インターフェイス上での NHRP のイネーブル化」（P.11）（必須）
- 「ステーションでのスタティック IP と NBMA のアドレス マッピングの設定」（P.12）（任意）
- 「ネクスト ホップ サーバのスタティックな設定」（P.14）（任意）
- 「NBMA アドレスが有効としてアドバタイズされる時間の変更」（P.14）（任意）
- 「NHRP 認証文字列の指定」（P.15）
- 「NHRP サーバ専用モードの設定」（P.17）（任意）
- 「NHRP のトリガーの制御」（P.18）（任意）
- 「トラフィックしきい値に基づく NHRP のトリガー」（P.21）（任意）
- 「NHRP パケット レートの制御」（P.25）（任意）
- 「転送レコードおよびリバース レコードのオプションの抑制」（P.27）（任意）
- 「NHRP 応答側 IP アドレスの指定」（P.28）（任意）
- 「NHRP キャッシュのクリア」（P.29）（任意）

マルチポイント動作のための GRE トンネルの設定

マルチポイント（NMBA）動作のための GRE トンネルを設定するには、次の作業を行います。

マルチポイント方式で動作する GRE トンネルをイネーブルにします。マルチポイント トンネル インターフェイスのトンネル ネットワークは、NBMA ネットワークと見なすことができます。同じルータ上で複数の GRE トンネルを設定する場合は、固有のトンネル ID キーまたは固有のトンネル送信元アドレスのいずれかを持っている必要があります。NHRP は、mGRE トンネル上で IP データ パケットを転送するための VPN レイヤ IP と NBMA レイヤ IP のアドレス マッピングを提供するため、mGRE トンネル インターフェイス上で必要になります。

（注） Cisco IOS Release 12.3(11)T よりも前では、すべての mGRE インターフェイスにはトンネル ID キーの設定が必要でした。Cisco IOS Release 12.3(11)T 以降では任意ですが、multipoint GRE（mGRE; マルチポイント GRE）インターフェイスを同じルータ上でトンネル ID キーを使用せずに設定する場合は、mGRE インターフェイスを固有のトンネル送信元アドレスを使用して設定する必要があります。

トンネル ID キーは各 GRE パケットで運ばれます。NHRP メッセージでは運ばれません。セキュリティ上の目的から、このキーに依存しないことを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel mode gre multipoint**
5. **tunnel key** *key-number*
6. **ip nhrp network-id** *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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**tunnel mode gre multipoint** **例：** `Router(config-if)# tunnel mode gre multipoint`	マルチポイント NBMA モードで使用する GRE トンネルをイネーブルにします。
ステップ 5	**tunnel key** *key-number* **例：** `Router(config-if)# tunnel key 3`	（任意）トンネル ID キーを設定します。 • マルチポイント トンネルで設定する NHRP の例については、「マルチポイント トンネル上の NHRP：例」（P.33）を参照してください。
ステップ 6	**ip nhrp network-id** *number* **例：** `Router(config-if)# ip nhrp network-id 1`	インターフェイスで NHRP をイネーブルにします。

インターフェイス上での NHRP のイネーブル化

ルータ上のインターフェイスに対して NHRP をイネーブルにするには、次の作業を行います。一般に、論理 NBMA ネットワーク内のすべての NHRP ステーションは、同じネットワーク ID を使用して設定する必要があります。

2 つ以上の NHRP ドメイン（GRE トンネル インターフェイス）が同じ NHRP ノード（ルータ）で使用可能な場合は、NHRP ネットワーク ID を使用して、NHRP インターフェイスの NHRP ドメインを定義し、複数の NHRP ドメイン間またはネットワーク間で区別します。2 つの NHRP ネットワーク（クラウド）を同じルータ上に設定する場合、NHRP ネットワーク ID を使用すると、両方のネットワークを分けることができます。

NHRP ネットワーク ID はローカル専用のパラメータです。これは、ローカル ルータだけに対して意味があり、NHRP パケットで他の NHRP ノードに送信されることはありません。この理由から、2 台のルータが同じ NHRP ドメインに存在する場合、ルータで設定される NHRP ネットワーク ID の実際の値は、もう一方のルータの NHRP ネットワーク ID と一致する必要はありません。NHRP パケットが GRE インターフェイス上に到着すると、そのインターフェイスで設定されている NHRP ネットワーク ID のローカル NHRP ドメインに割り当てられます。

（注） ネットワーク ID を割り当てるこの方法は、**router ospf** *process-id* コマンドのプロセス ID である Open Shortest Path First（OSPF）の概念に似ています。2 つ以上の OSPF プロセスを設定する場合、OSPF ネイバーおよびそれが提供するルーティング データは、OSPF プロセス（ドメイン）に割り当てられ、このプロセスによって、インターフェイスは別の **router ospf** *process-id* コンフィギュレーション ブロックにある *network* 引数にマッピングします。

同じ NHRP ネットワークに存在するすべてのルータ上の GRE インターフェイスでは、同じ NHRP ネットワーク ID を使用することを推奨します。こうすると、どの GRE インターフェイスがどの NHRP ネットワークのメンバであるかを追跡しやすくなります。

NHRP ドメイン（ネットワーク ID）は、ルータ上の各 GRE トンネル インターフェイスで固有に設定できます。DMVPN のフェーズ 1 またはフェーズ 2 の実行時や、GRE インターフェイスでトンネル キーを使用する場合、これは必須です。これらの固有 ID により、各 GRE インターフェイスを異なる NHRP ドメインに分類します。これは、1 つの固有な DMVPN 内にそれぞれインターフェイスが存在していることと同じです。

NHRP ドメインは、ルート上の GRE トンネル インターフェイス間をまたぐことができます。DMVPN のフェーズ 3 の実行時や、GRE トンネル インターフェイスでトンネル キーを使用しない場合、このオプションを使用できます。この場合、GRE トンネル インターフェイスで同じ NHRP ネットワーク ID を使用する効果は、2 つの GRE インターフェイスが単一の NHRP ネットワーク（DMVPN ネットワーク）に統合されることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address network-mask*
5. **ip nhrp network-id** *number*
6. **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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip address** *ip-address network-mask* **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	IP をイネーブルにし、インターフェイスに IP アドレスを提供します。
ステップ 5	**ip nhrp network-id** *number* **例：** `Router(config-if)# ip nhrp network-id 1`	インターフェイスで NHRP をイネーブルにします。
ステップ 6	**end** **例：** `Router(config)# 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。

ステーションでのスタティック IP と NBMA のアドレス マッピングの設定

ステーション（ホストまたはルータ）でスタティック IP と NBMA のアドレス マッピングを設定するには、次の作業を行います。スタティックに設定されたステーションに送信する IP マルチキャストおよびブロードキャスト パケットをイネーブルにするには、**ip nhrp map multicast** *nbma-address* コマンドを使用します。このコマンドはマルチポイント GRE トンネルでは必須ですが、ポイント間 RE トンネルでは必要ありません。

NHRP に参加するには、NBMA ネットワークに接続されたステーションを、その NHS の IP および NBMA アドレスを使用して設定する必要があります。NBMA アドレスの形式は、ご使用のメディアによって異なります。たとえば、GRE は Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスを使用し、イーサネットは MAC アドレスを使用し、SMDS は E.164 アドレスを使用します。

これらの NHS は、ステーションのデフォルト ルータやピア ルータになることもあるため、ステーションのネットワーク レイヤ転送テーブルからそのアドレスを取得できます。

ステーションが複数のリンク レイヤ ネットワーク（論理 NBMA ネットワークを含む）に接続されている場合、その NHS およびピア ルータからルーティング情報を受信するようにステーションを設定し、どの IP ネットワークがどのリンク レイヤ ネットワークを通って到達可能かを判断できるようにする必要もあります。

ステーション（ホストまたはルータ）でスタティック IP と NBMA のアドレス マッピングを設定するには、次の作業を行います。スタティックに設定されたステーションに送信する IP マルチキャストおよびブロードキャスト パケットをイネーブルにするには、**ip nhrp map multicast** *nbma-address* コマンドを使用します。この手順はマルチポイント GRE トンネルでは必須ですが、ポイント間 RE トンネルでは必要ありません。

（注） IGP ルーティング プロトコルは IP マルチキャストまたはブロードキャストを使用するため、多くの場合、**ip nhrp map multicast** コマンドが任意で必要になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** type *number*
4. **ip nhrp map** *ip-address nbma-address*
5. **ip nhrp map multicast** *nbma-address*

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp map** *ip-address nbma-address* **例：** `Router(config-if)# ip nhrp map 10.0.0.2 172.16.1.2`	ステーションでスタティック IP と NBMA のアドレス マッピングを設定します。
ステップ 5	**ip nhrp map multicast** *nbma-address* **例：** `Router(config-if)# ip nhrp map multicast 172.16.1.12`	（任意）インターフェイスに送信されるマルチキャストまたはブロードキャストのパケットを受信する NBMA アドレスを追加します。 **（注）** このコマンドはポイントツーポイント GRE トンネルでは必要ありません。

ネクスト ホップ サーバのスタティックな設定

ネクスト ホップ サーバをスタティックに設定するには、次の作業を行います。

NHS は通常、ネットワーク レイヤ転送テーブルを使用して、NHRP パケットの転送先を判断し、NBMA ネットワークからの出力ポイントを検索します。また、NHS が対応するステーションの IP アドレスに相当する一連の IP アドレス プレフィクス、および論理 NBMA ネットワーク ID を使用して、NHS をスタティックに設定することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp nhs** *nhs-address* [*net-address* [*netmask*]]

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp nhs** *nhs-address* [*net-address* [*netmask*]] **例：** `Router(config-if)# ip nhrp nhs 10.0.0.2`	ネクスト ホップ サーバをスタティックに設定します。 • ネクスト ホップ サーバが対応する複数のネットワークを設定するには、同じネクスト ホップ サーバ アドレスと、異なる IP ネットワーク アドレスを使用して **ip nhrp nhs** コマンドを繰り返します。 • 追加のネクスト ホップ サーバを設定するには、**ipnhrp nhs** コマンドを繰り返します。

NBMA アドレスが有効としてアドバタイズされる時間の変更

肯定 NHRP 応答で NBMA アドレスが有効としてアドバタイズされる時間を変更するには、次の作業を行います。この説明において、*アドバタイズ*とは、Cisco IOS XE ソフトウェアが NHRP 応答で提供しているアドレス マッピングを保持する時間を他のルータに指示することを意味します。デフォルトの時間は 7200 秒（2 時間）です。

この設定は、Spoke-to-Spoke ショートカット パスが使用されなくなった後アップの状態でいる時間、および Spoke-to-Spoke ショートカット パスのマッピング エントリが使用されている場合に更新する頻度を制御します。300 ～ 600 秒の範囲で値を使用することを推奨します。

ip nhrp holdtime コマンドは、NHRP NHC が、設定されているその NHRP NHS に NHRP 登録要求を送信する頻度を制御します。デフォルトでは、NHRP ホールド時間値の 3 分の 1 の時間（デフォルト＝2400 秒（40 分））ごとに NHRP 登録を送信します。**ip nhrp registration timeout** *value* コマンドを任意で使用すると、NHRP ホールド時間にかかわらず、NHRP 登録要求を送信する間隔を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp holdtime** *seconds*
5. **ip nhrp registration timeout** *seconds*

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp holdtime** *seconds* **例：** `Router(config-if)# ip nhrp holdtime 600`	肯定 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。 • この例では、10 分間 NHRP NBMA アドレスが有効として、肯定 NHRP 応答でアドバタイズされます。
ステップ 5	**ip nhrp registration timeout** *seconds* **例：** `Router(config-if)# ip nhrp registration timeout 100`	（任意）設定された NHRP NHS に NHRP NHC が NHRP 登録要求を送信する間隔を変更します。 • この例では、NHRP 登録要求が 100 秒ごとに送信されるようになります（デフォルト値は、NHRP ホールド時間値の 3 分の 1）。

NHRP 認証文字列の指定

インターフェイスで NHRP の認証文字列を指定するには、次の作業を行います。

認証文字列を設定すると、同じ文字列で設定されたルータだけが NHRP を使用して通信できるようになります。したがって、認証スキームを使用する場合、ファブリック上で NHRP 用に設定されたすべてのデバイスで同じ文字列を設定する必要があります。

（注） 複数の NHRP ドメインを相互に分けておくようにする場合は特に、NHRP 認証文字列の使用を推奨します。NHRP 認証文字列は暗号化されないため、NHRP ネットワークに入ろうとする NHRP ノードに対する実際の認証としては使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp authentication** *string*
5. **exit**
6. **show ip nhrp** [**dynamic** | **static**] [*type number*]
7. **show ip nhrp traffic**
8. **show ip nhrp nhs** [**detail**]

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp authentication** *string* **例：** `Router(config-if)# ip nhrp authentication specialxx`	認証文字列を指定します。 • 1 つの論理 NBMA ネットワーク内の NHRP で設定されたすべてのルータは、同じ認証文字列を共有する必要があります。
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、特権 EXEC モードに戻ります。
ステップ 6	**show ip nhrp** [**dynamic** | **static**] [*type number*] **例：** `Router# show ip nhrp`	IP NHRP キャッシュを表示します。これは、特定のインターフェイスのダイナミックまたはスタティックのキャッシュ エントリに制限できます。
ステップ 7	**show ip nhrp traffic** **例：** `Router# show ip nhrp traffic`	NHRP トラフィック統計情報を表示します。
ステップ 8	**show ip nhrp nhs** [**detail**] **例：** `Router# show ip nhrp nhs detail`	NHRP ホールド時間の詳細を表示します。

NHRP サーバ専用モードの設定

NHRP サーバ専用モードを設定するには、次の作業を行います。

NHRP ショートカット SVC を確立するための NHRP 解決要求は開始できず、NHRP 解決要求に応答だけができるようにインターフェイスを設定できます。NHRP 解決要求を行わないルータで NHRP サーバ専用モードを設定します。

インターフェイスが NHRP サーバ専用モードになっている場合、**ip nhrp server-only** [**non-caching**] コマンド キーワードを指定できるオプションがあります。この場合、NHRP は、ルータを通過する NHRP 応答などのマッピング情報を NHRP キャッシュに保存しません。メモリを節約し、NHRP ショートカットの構築を防ぐために、他の 2 つの NHRP ルータ（NHRP ハブ）間に配置されるルータでは一般的に、キャッシングなしのオプションを使用します。

NHRP サーバ専用モードを設定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp server-only** [**non-caching**]

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp server-only** [**non-caching**] **例：** `Router(config-if)# ip nhrp server-only non-caching`	NHRP サーバ専用モードを設定します。

NHRP のトリガーの制御

任意のプラットフォームで NHRP がトリガーされるタイミングを制御する方法は 2 つあります。これらの方法は次のセクションで説明されています。

- 「宛先単位での NHRP のトリガー」（P.18）
- 「パケット数単位での NHRP のトリガー」（P.20）

宛先単位での NHRP のトリガー

宛先単位で NHRP をトリガーするには、次の作業を行います。

NHRP 解決要求の送信をトリガーできる IP パケットを判断するために使用される IP アクセス リストを指定できます。デフォルトでは、すべての非 NHRP パケットが NHRP 解決要求をトリガーします。NHRP 解決要求をトリガーする IP パケットを制限するには、アクセス リストを定義してインターフェイスに適用します。

（注） NHRP 解決要求は、2 つの NHRP ノード間の直接パスを構築するために使用されます。特定のトラフィックがこのパスの構築をトリガーしないように除外されていても、パスがすでに構築されている場合は、この「除外された」トラフィックは直接パスを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

   または

   access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**]
4. **interface** *type number*
5. **ip nhrp interest** *access-list-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。 • プロンプトが表示されたら、パスワードを入力します。
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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] または **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**] **例：** `Router(config)# access-list 101 permit ip any any` または `Router(config)# access-list 101 deny ip any 10.3.0.0 0.0.255.255`	標準または拡張 IP アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* **例：** `Router(config)# interface tunnel 100`	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 5	**ip nhrp interest** *access-list-number* **例：** `Router(config-if)# ip nhrp interest 101`	NHRP 要求を制御する IP アクセス リストを指定します。 • この例では、拡張アクセス リスト 101 で許可されるパケットだけが、デフォルトの SVC トリガー レートおよびティアダウン レートの対象です。

パケット数単位での NHRP のトリガー

デフォルトでは、ソフトウェアは、NHRP の使用が可能であると判断した宛先へのデータ パケットの送信を試行する場合、その宛先に対する NHRP 要求を送信します。特定の宛先に送信されたデータ パケットが指定された数になるまで待機してから NHRP が試行されるようにシステムを設定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp use** *usage-count*

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。 • プロンプトが表示されたら、パスワードを入力します。
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	**interface** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp use** *usage-count* **例：** `Router(config-if)# ip nhrp use 5`	NHRP を試行するまでに、1 つの宛先に送信するデータ パケットの数を指定します。 • この例では、最初の 1 分間に、最初の宛先に 5 つのパケットが送信され、2 番めの宛先に 5 つのパケットが送信された場合、2 番めの宛先に対して単一の NHRP 要求が生成されています。 • その次の 1 分間に、同じトラフィックが生成され、まだ NHRP 応答を受信していない場合、システムは 2 番めの宛先に対して、その要求を再送信します。

トラフィックしきい値に基づく NHRP のトリガー

NHRP は、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）とともに実行する場合、Cisco Express Forwarding プラットフォーム上で動作できます。設定されたトラフィック レートに達したら SVC を開始するように NHRP を設定できます。同様に、別に設定されたレートまでトラフィックが低下した場合は、SVC を切断できます。

NHRP が SVC をセットアップまたは切断する前に達すべきトラフィック レートを設定できます。SVC はバースト トラフィック専用に作成されるため、リソースを節約できます。

トラフィック レートに基づいて NHRP による SVC のトリガーおよびティアダウンを設定するには、次の作業を行います。最初の作業は必須で、2 番めと 3 番めの作業は任意です。

- 「SVC をトリガーするレートの変更」（P.21）（必須）
- 「サンプリング時間およびサンプリング レートの変更」（P.23）（任意）
- 「特定の宛先へのトリガー レートおよびティアダウン レートの適用」（P.24）（任意）

SVC をトリガーするレートの変更

NHRP がこの宛先への SVC をセットアップまたは切断するキロビット / 秒（kbps）単位の数値を変更するには、次の作業を行います。

NHRP が BGP とともに実行する場合、NHRP パケットのトリガーを制御する方法が 1 つあります。この方法は、指定された BGP ネクスト ホップへの入力トラフィック レートに基づいて開始されている SVC で成り立ちます。

BGP が BGP ネクスト ホップを検出し、この BGP ルートをルーティング テーブルに入れると、NHRP 要求が BGP ネクスト ホップに送信されます。NHRP 応答を受信すると、以降のルートは、BGP ネクスト ホップに直接対応する NHRP キャッシュに置かれます。

NHRP キャッシュを取り込むために、新しい NHRP 要求が同じ BGP ネクスト ホップに送信されます。NHRP キャッシュ エントリが生成されると、同じ BGP ネクスト ホップに対する以降のマップ ステートメントも作成されます。

各 BGP ネクスト ホップへの集約トラフィックが測定され、モニタされます。集約トラフィックが、設定されたトリガー レートに達するか超過すると、NHRP は SVC を作成し、その宛先ルータに直接トラフィックを送信します。集約トラフィック レートが、設定されたティアダウン レートまで低下するかそれ以下になると、ルータは指定された宛先への SVC を切断します。

デフォルトでは、宛先への集約トラフィックが移動平均 30 秒で 1 kbps を超えると、NHRP はその宛先への SVC をセットアップします。同様に、その宛先へのトラフィックが移動平均 30 秒で 0 kbps まで下がると、NHRP は SVC を切断します。SVC のセットアップまたはティアダウンを発生させるレートを変更する方法がいくつかあります。kbps 単位のしきい値の数値、ロード間隔、またはその両方を変更できます。

前提条件

トラフィック レートに基づいて NHRP を開始する機能を設定するには、あらかじめルータで次の条件を満たす必要があります。

- GRE が設定されていること。
- CEF スイッチングまたは distributed CEF（dCEF）スイッチングがイネーブルになっていること。
- これらの拡張機能を実行するネットワーク内のすべてのルータで BGP が設定されていること。

ご使用のネットワークで CEF スイッチングまたは dCEF スイッチングを使用している場合に、NHRP を動作させるには（デフォルト値または変更した値のいずれかで）、**ip cef accounting non-recursive** コマンドを設定します。

制約事項

Cisco IOS Release 12.0 よりも前のリリースには、NHRP ドラフト バージョン 4 が実装されていました。Cisco IOS Release 12.0 以降のリリースには、NHRP ドラフト バージョン 11 が実装されています。これらのバージョンに互換性はありません。したがって、相互に通信させるためには、ネットワーク内で NHRP を実行するすべてのルータでは、同じバージョンの NHRP を実行する必要があります。すべてのルータが Cisco IOS Release 12.0 以降のリリースを実行するか、または Release 12.0 よりも前のリリースを実行するかのいずれかにする必要があり、両者の組み合わせでは実行できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp trigger-svc** *trigger-threshold teardown-threshold*

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp trigger-svc** *trigger-threshold teardown-threshold* **例：** `Router(config-if)# ip nhrp trigger-svc 100 5`	NHRP が SVC をセットアップまたは切断するレートを変更します。 • この例では、トリガーおよびティアダウンのしきい値をそれぞれ、100 kbps、5 kbps に設定します。

サンプリング時間およびサンプリング レートの変更

平均トリガー レートまたは平均ティアダウン レートを計算する時間を変更できます。デフォルトで、この時間は 30 秒です。30 ～ 300 秒の範囲で 30 秒きざみです。この時間は、Cisco IOS XE ソフトウェアだけに対して、内部的な集約トラフィック レートを計算するために使用され、アクションを実行するとしては最悪な状態となる時間を示します。場合によっては、トラフィック レートの上昇や低下に合わせて、ソフトウェアがより早く動作します。

ご使用のシスコ ハードウェア製品に Virtual Interface Processor のバージョン 2 アダプタが搭載されている場合、サンプリング時間を変更するには、この作業を実行する必要があります。デフォルトで、ポート アダプタは 10 秒ごとにルート プロセッサにトラフィック統計情報を送信します。dCEF スイッチング モードで NHRP を使用している場合は、この更新レートを 5 秒に変更する必要があります。

サンプリング時間およびサンプリング レートを変更するには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip cef traffic-statistics** [**load-interval** *seconds*]
4. **ip cef traffic-statistics** [**update-rate** *seconds*]

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。 • プロンプトが表示されたら、パスワードを入力します。
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	**ip cef traffic-statistics** [**load-interval** *seconds*] **例：** `Router(config)# ip cef traffic-statistics load-interval 120`	トリガーおよびティアダウンのしきい値を平均化するサンプリング時間の長さを変更します。 • この例では、120 秒間の平均を基準としてトリガーおよびティアダウンのしきい値が計算されます。
ステップ 4	**ip cef traffic-statistics** [**update-rate** *seconds*] **例：** `Router(config)# ip cef traffic-statistics update-rate 5`	ポート アダプタがアカウンティング統計情報を RP に送信する頻度を指定します。 • distributed CEF スイッチング モードで NHRP を使用する場合、この値を 5 秒に設定する必要があります。デフォルト値は 10 秒です。

特定の宛先へのトリガー レートおよびティアダウン レートの適用

トリガー レートおよびティアダウン レートを特定の宛先に強制するには、次の作業を行います。デフォルトでは、NHRP トリガー用にすべての宛先が計算されモニタされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

   または

   access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]
4. **interface** *type number*
1. **ip nhrp interest** *access-list-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。 • プロンプトが表示されたら、パスワードを入力します。
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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] または **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] **例：** `Router(config)# access-list 101 permit ip any any` または `Router(config)# access-list 101 deny ip any 10.3.0.0 0.0.255.255`	標準または拡張 IP アクセス リストを定義します。 • この例では、拡張アクセス リストを定義します。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface tunnel 100`	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 5	**ip nhrp interest** *access-list-number* **例：** `Router(config-if)# ip nhrp interest 101`	NHRP 要求を制御する IP アクセス リストを指定します。 • この例では、拡張アクセス リスト 101 で許可されるパケットだけが、デフォルトの SVC トリガー レートおよびティアダウン レートの対象です。

NHRP パケット レートの制御

NRHP パケットを処理する最大レートを変更するには、次の作業を行います。

ローカル NHRP プロセスが一定時間内で処理できる NHRP メッセージの数には、最大値（最大送信間隔）があります。この制限により、NHRP 要求を送信しながら暴走した NHRP プロセスや、多数の Spoke-to-Spoke トンネルをトリガーしている IP アドレス スキャンを実行中のアプリケーション（ワーム）などのイベントから、ルータが保護されます。

最大送信間隔が大きいほど、システムが処理および送信できる NHRP パケットは増加します。これらのメッセージはメモリをあまり使用せず、メッセージ単位の CPU 使用量はそれほど大きくありません。ただし、メッセージの数が過剰になれば CPU 使用量は極端に高まり、システム パフォーマンスを低下させる可能性があります。

適度な最大送信間隔を設定するには、次の情報を考慮します。

- このハブが処理しているスポーク ルータの数、および NHRP 登録要求を送信する頻度。この負荷に対応するには、次が必要です。

  スポーク数 / 登録タイムアウト × 最大送信間隔

  たとえば、スポーク 500 個、登録タイムアウト 100 秒であれば、次のようになります。

  最大送信間隔＝ 500/100×10 ＝ 50

- NBMA ネットワーク全体で常にアップ状態であることが見込まれる Spoke-to-Spoke トンネルの最大数。

  Spoke-to-Spoke トンネル /NHRP ホールド時間 × 最大送信間隔

  これは、Spoke-to-Spoke トンネルの作成、およびさらに長い時間使用される Spoke-to-Spoke トンネルの更新を対象とします。

  ここで、これらの値を足した結果に 1.5 または 2.0 を乗じ、バッファを指定します。

- 最大送信間隔を使用して、一定数で送信できる NHRP メッセージの長期平均数を保つことができますが、より大きなピークを許容できます。

デフォルトでは、ソフトウェアが NHRP パケットを送信する最大レートは、10 秒ごとに 5 パケットです。ソフトウェアは、送信できる NHRP パケット（ローカルで生成されたか、転送されたかのいずれか）に対して、インターフェイス単位のクォータを維持します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp max-send** *pkt-count* **every** *interval*

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**ip nhrp max-send** *pkt-count* **every** *interval* **例：** `Router(config-if)# ip nhrp max-send 10 every 10`	この例では、10 秒ごとに 10 個の NHRP パケット（デフォルトの 2 倍）をインターフェイスから送信できます。

転送レコードおよびリバース レコードのオプションの抑制

NBMA ネットワークでリンク レイヤ フィルタリングをダイナミックに検出する（たとえば、SMDS アドレス スクリーニング）、およびループ検出と診断の機能を提供するために、NHRP は要求パケットおよび応答パケット内にルート レコードを組み込みます。ルート レコード オプションには、（転送方向の）送信元と宛先の間、および（逆方向の）宛先と送信元の間にあるすべての中間ネクスト ホップ サーバのネットワーク（およびリンク レイヤ）アドレスが含まれています。

デフォルトでは、NHRP 要求パケットおよび応答パケットには転送レコード オプションとリバース レコード オプションが含まれます。転送レコードおよびリバース レコードのオプションを抑制するには、次の作業を行います。

（注） 特に DMVPN ネットワークでは、転送レコードおよびリバース レコードの情報は NHRP の適切な動作のために必要です。このため、この情報の抑制は設定しないでください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip nhrp record**

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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface tunnel 100`	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	**no ip nhrp record** **例：** `Router(config-if)# no ip nhrp record`	転送レコードおよびリバース レコードのオプションを抑制します。

NHRP 応答側 IP アドレスの指定

どのネクスト ホップ サーバが NHRP 応答パケットを生成するのかを把握する必要のある NHRP 要求側では、その NHRP 要求パケットに応答側アドレス オプションを含めることができます。NHRP 応答パケットを生成するネクスト ホップ サーバは、独自の IP アドレスを NHRP 応答に挿入することで応じます。ネクスト ホップ サーバは、指定されたインターフェイスのプライマリ IP アドレスを使用します。

ネクスト ホップ サーバが NHRP 応答側 IP アドレスに使用するインターフェイスを指定するには、次の作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nhrp responder** *type 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。 • プロンプトが表示されたら、パスワードを入力します。
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** *type number* **例：** `Router(config)# interface serial 0`	シリアル 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	**ip nhrp responder** *type number* **例：** `Router(config-if)# ip nhrp responder serial 0`	ネクスト ホップ サーバが NHRP 応答側 IP アドレスに使用するインターフェイスを指定します。 • この例では、応答側アドレスに対する任意の NHRP 要求が発生すると、ネクスト ホップ サーバとして動作しているこのルータによって、シリアル インターフェイス 0 のプライマリ IP アドレスが NHRP 応答パケットで提供されるようになります。 • ネクスト ホップ サーバによって転送されている NHRP 応答パケットにこのサーバの IP アドレスが含まれる場合、ネクスト ホップ サーバは、「NHRP ループ検出」のタイプのエラーを生成し、その応答を廃棄します。

NHRP キャッシュのクリア

NHRP キャッシュには、スタティックに設定した NHRP マッピングのエントリ、および NHRP パケットからアドレスを学習している Cisco IOS XE ソフトウェアによるダイナミック エントリを含めることができます。スタティックに設定されたエントリをクリアするには、インターフェイス コンフィギュレーション モードで **no ip nhrp map** コマンドを使用します。

NHRP キャッシュをクリアするには、次の作業を行います。

手順の概要

1. **enable**
2. **clear ip nhrp** [*ip-address*] [*ip-mask*]

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。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ip nhrp** [*ip-address*] [*ip-mask*] **例：** `Router# clear ip nhrp`	ダイナミック エントリの IP NHRP キャッシュをクリアします。 • このコマンドでは、スタティックに設定された IP と NBMA のいずれのアドレス マッピングも NHRP キャッシュからクリアしません。

NHRP の設定例

ここでは、次の設定例について説明します。

- 「論理 NBMA の物理ネットワーク設計：例」（P.30）
- 「NHRP レートの特定の宛先への適用：例」（P.32）
- 「マルチポイント トンネル上の NHRP：例」（P.33）
- 「NHRP の表示：例」（P.34）

論理 NBMA の物理ネットワーク設計：例

論理 NBMA ネットワークは、NHRP に参加し、同じネットワーク ID を持つインターフェイスおよびホストのグループと考えられます。図 2 に、単一の物理 NBMA ネットワーク上に設定された（円で示される）2 つの論理 NBMA ネットワークを示します。ルータ A はルータ B およびルータ C と通信できます。それらが同じネットワーク ID（2）を共有するためです。また、ルータ C はルータ D およびルータ E とも通信できます。それらがネットワーク ID 7 を共有するためです。アドレス解決が完了した後、点線で示すように、ルータ A は IP パケットをホップ 1 回でルータ C に送信でき、ルータ C はそれをホップ 1 回でルータ E に送信できます。

図 2　1 つの物理 NBMA ネットワーク上の 2 つの論理 NBMA ネットワーク

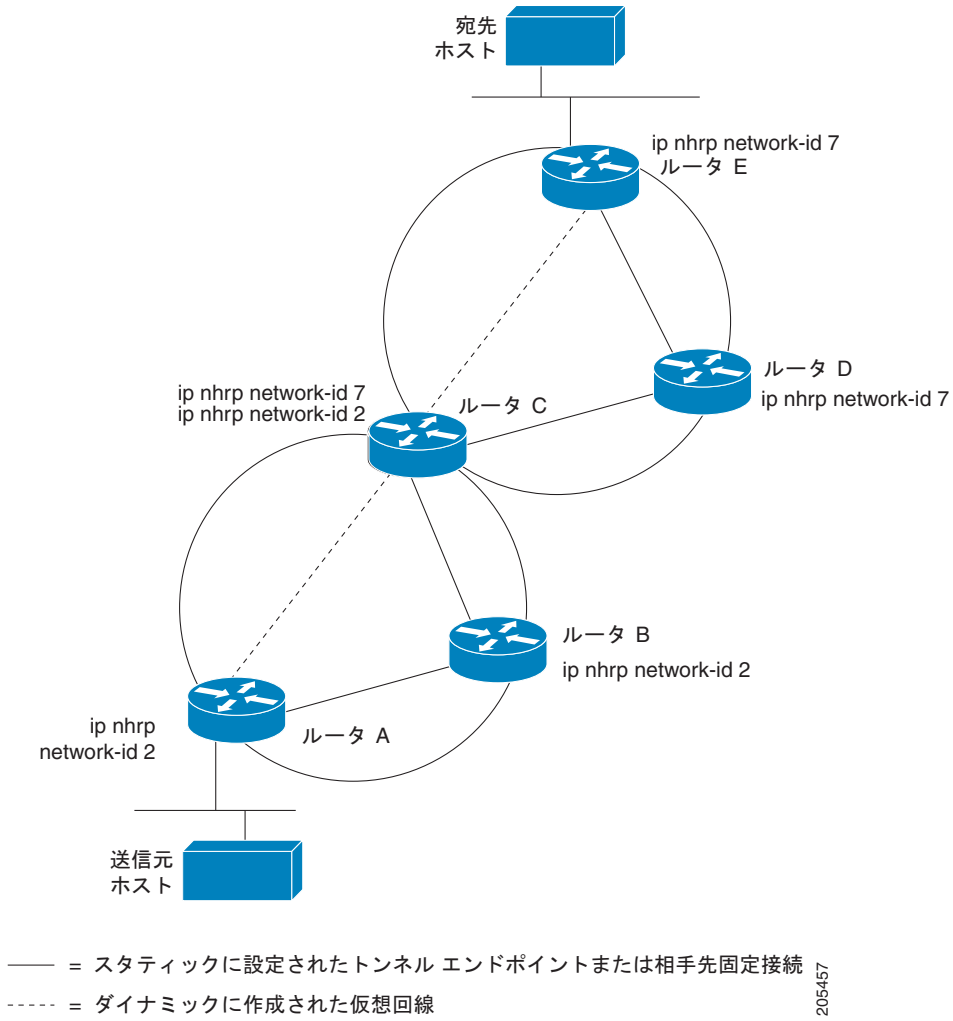


図 2 の 5 台のルータによる物理構成は、実際には 図 3 のような構成である場合もあります。送信元ホストはルータ A に接続され、宛先ホストはルータ E に接続されています。同じスイッチが 5 台すべてのルータに対応し、1 つの物理 NBMA ネットワークを構成します。

図 3　　NBMA ネットワーク例の物理構成

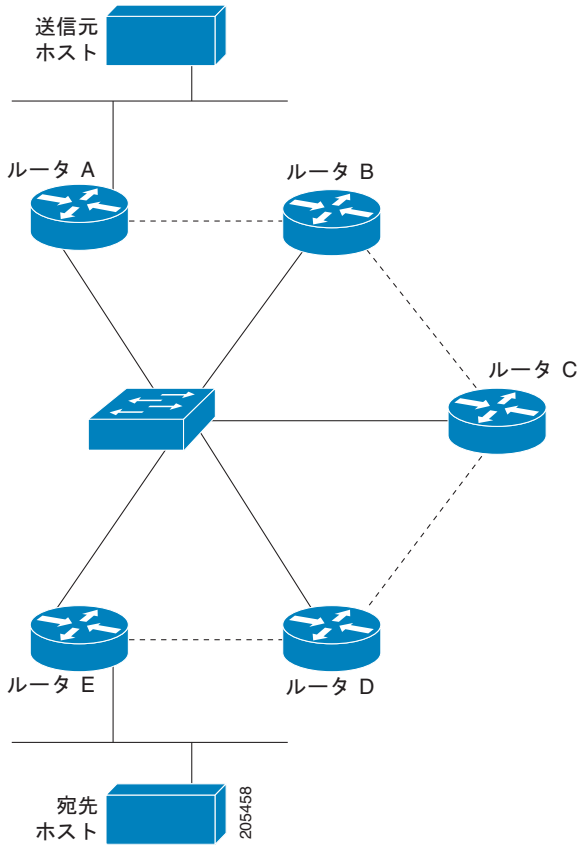


図 2 をもう一度参照してください。最初、送信元ホストから宛先ホストへの IP パケットは、NHRP が NBMA アドレスでも解決するようになるまで、スイッチに接続された 5 台すべてのルータを通過して宛先に到達します。ルータ A は、IP パケットを初めて宛先ホストに向けて転送したときに、宛先ホストの IP アドレスに対する NHRP 要求も生成します。その要求がルータ C に転送され、応答が生成されます。2 つの論理 NBMA ネットワーク間の出力ルータであるため、ルータ C が応答します。

同様に、ルータ C は独自の NHRP 要求を生成し、これに対して、ルータ E が応答します。この例でも、送信元と宛先の間に発生する IP トラフィックが NBMA ネットワークを通過するためには、2 回のホップが必要です。これは、2 つの論理 NBMA ネットワーク間で IP トラフィックを転送する必要があるためです。NBMA ネットワークが論理的に分かれていなければ、必要なホップは 1 回だけです。

NHRP レートの特定の宛先への適用：例

次の例では、デフォルトの SVC トリガー レートおよびティアダウン レートの対象は、拡張アクセス リスト 101 を通過するパケットだけです。

```
interface tunnel 100
 ip nhrp interest 101
!
access-list 101 permit ip any any
access-list 101 deny ip any 10.3.0.0 0.0.255.255
```

マルチポイント トンネル上の NHRP：例

マルチポイント トンネルを使用すると、単一のトンネル インターフェイスを複数のネイバー ルータに接続できます。ポイントツーポイント トンネルとは異なり、トンネルの宛先を設定する必要がありません。実際に、設定したとしても、トンネルの宛先は IP マルチキャスト アドレスに対応させる必要があります。トンネルの宛先として設定されたマルチキャスト アドレスに GRE パケットを送信することによって、トンネル インターフェイス上で送信されるブロードキャスト パケットおよびマルチキャスト パケットを送信できます。

マルチポイント トンネルは、トンネル キーを設定する必要があります。それ以外の場合、予期しない GRE トラフィックをトンネル インターフェイスで受信しやすくなる可能性があります。簡素化のため、トンネル キーは NHRP ネットワーク ID に対応させることを推奨します。

次の例では、ルータ A、ルータ B、ルータ C、ルータ D がすべて 1 つのイーサネット セグメントを共有します。マルチポイント トンネル ネットワーク上で最小の接続が設定されるため、部分メッシュ NBMA ネットワークとして扱うことができるネットワークが作成されます。スタティック NHRP マップ エントリによって、ルータ A はルータ B へ、ルータ B はルータ C へ、ルータ C はルータ D へ、ルータ D はルータ A へ、それぞれが到達方法を認識しています。

ルータ A が初めてルータ D への IP パケットの送信を試行すると、パケットはルータ B およびルータ C を経由して転送されます。ルータは NHRP を使用して、すぐにお互いの NBMA アドレス（この場合は、基盤となるイーサネット ネットワークに割り当てられた IP アドレス）を学習します。部分メッシュ トンネル ネットワークがただちに完全メッシュになり、この時点で、中間ホップの必要な IP トラフィックを使用せずに、どのルータでもトンネル ネットワーク上で直接通信することができます。

ルータ A、ルータ B、ルータ C、ルータ D のコンフィギュレーションの重要な部分は、次のとおりです。

ルータ A の設定

```
interface tunnel 0
 no ip redirects
 ip address 11.0.0.1 255.0.0.0
 ip nhrp map 11.0.0.2 10.0.0.2
 ip nhrp network-id 1
 ip nhrp nhs 11.0.0.2
 tunnel source ethernet 0
 tunnel mode gre multipoint
 tunnel key 1

interface ethernet 0
 ip address 10.0.0.1 255.0.0.0
```

ルータ B の設定

```
interface tunnel 0
 no ip redirects
 ip address 11.0.0.2 255.0.0.0
 ip nhrp map 11.0.0.3 10.0.0.3
 ip nhrp network-id 1
 ip nhrp nhs 11.0.0.3
 tunnel source ethernet 0
 tunnel mode gre multipoint
 tunnel key 1

interface ethernet 0
 ip address 10.0.0.2 255.0.0.0
```

ルータ C の設定

```
interface tunnel 0
 no ip redirects
```

```
 ip address 11.0.0.3 255.0.0.0
 ip nhrp map 11.0.0.4 10.0.0.4
 ip nhrp network-id 1
 ip nhrp nhs 11.0.0.4
 tunnel source ethernet 0
 tunnel mode gre multipoint
 tunnel key 1

interface ethernet 0
 ip address 10.0.0.3 255.0.0.0
```

ルータ D の設定

```
interface tunnel 0
 no ip redirects
 ip address 11.0.0.4 255.0.0.0
 ip nhrp map 11.0.0.1 10.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 11.0.0.1
 tunnel source ethernet 0
 tunnel mode gre multipoint
 tunnel key 1

interface ethernet 0
 ip address 10.0.0.4 255.0.0.0
```

NHRP の表示：例

次に、**show ip nhrp** コマンドの出力例を示します。

```
Router# show ip nhrp


10.0.0.2 255.255.255.255, tunnel 100 created 0:00:43 expire 1:59:16

 Type: dynamic Flags: authoritative

 NBMA address: 10.1111.1111.1111.1111.1111.1111.1111.1111.1111.11

10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56

 Type: static Flags: authoritative

 NBMA address: 10.1.1.2
```

表示例のフィールドは次のとおりです。

- IP と NBMA のアドレス キャッシュ内の IP アドレスおよびそのネットワーク マスク。シスコでは NHRP による NBMA 情報の集約をサポートしていないため、マスクは常に 255.255.255.255 です。
- インターフェイスのタイプと番号、および作成してからの経過時間（時: 分: 秒）。
- 肯定および否定の権限 NBMA アドレスが期限切れになる時間（時: 分: 秒）。この値は、**ip nhrpholdtime** コマンドに基づいています。
- インターフェイスのタイプ。
  - dynamic：NBMA アドレスが NHRP 要求パケットから取得されました。
  - static：NBMA アドレスがスタティックに設定されていました。
- フラグ。

- authoritative：特定の宛先に対する NBMA と IP のアドレス マッピングを維持するネクスト ホップ サーバまたはルータから、NHRP 情報が取得されたことを示します。
- implicit：ローカル ルータが受信した NHRP 解決要求の送信元のマッピング情報から、またはローカル ルータを通って転送されている NHRP 解決パケットから情報が学習されたことを示します。
- negative：否定キャッシュの場合、要求された NBMA マッピングが取得できなかったことを示します。
- unique：この NHRP マッピング エントリが固有でなければならないことを示します。IP アドレスは同じであるが NBMA アドレスが異なるマッピング エントリでは上書きできません。
- registered：NHRP マッピング エントリが NHRP 登録要求によって作成されたことを示します。
- used：過去 60 秒以内に NHRP マッピングを使用してデータ パケットが転送されたことを示します。
- router：リモート ルータの背後にあるネットワークまたはホストへのアクセスを提供しているリモート ルータからの NHRP マッピング エントリを示します。
- local：このルータが NHRP 解決要求に応答しているこのルータに対してローカルなネットワークの NHRP マッピング エントリを示します。
- （no socket）：IPsec ソケット（暗号化用）がトリガーされていない NHRP マッピング エントリを示します。これらのマッピング エントリは、データ パケットの転送には使用されません。
- nat：IPsec ソケット（暗号化用）がトリガーされていない NHRP マッピング エントリを示します。これらのマッピング エントリは、データ パケットの転送には使用されません。
- NBMA address：非ブロードキャスト マルチアクセス アドレス。アドレス形式は、使用されているネットワークのタイプに適しています（たとえば、GRE、イーサネット、SMDS、マルチポイント トンネルなど）。

次に、NHRP トラフィックの統計情報を表示する **show ip nhrp traffic** コマンドの出力例を示します。

```
Router# show ip nhrp traffic

Tunnel0

  request packets sent: 2

  request packets received: 4

  reply packets sent: 4

  reply packets received: 2

  register packets sent: 0

  register packets received: 0

  error packets sent: 0

  error packets received: 0
```

表示例で示すフィールドは次のとおりです。

- Tunnel0：インターフェイスのタイプおよび番号。
- request packets sent：このステーションから送信された NHRP 要求パケットの数。
- request packets received：このステーションで受信した NHRP 要求パケットの数。
- reply packets sent：このステーションから送信された NHRP 応答パケットの数。

- reply packets received：このステーションで受信した NHRP 応答パケットの数。
- register packets sent：このステーションから送信した NHRP 登録パケットの数。ルータおよびアクセス サーバは登録パケットを送信しないため、この値は 0 です。
- register packets received：このステーションで受信した NHRP 登録パケットの数。ルータまたはアクセス サーバは登録パケットを送信しないため、この値は 0 です。
- error packets sent：このステーションから送信された NHRP エラー パケットの数。
- error packets received：このステーションで受信した NHRP エラー パケットの数。

次に、特定のトンネル（tunnel7）に関する出力例を示します。

```
Router# show ip nhrp traffic interface tunnel7

Tunnel7: Max-send limit:100Pkts/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
```

NHRP ホールド時間＝600 で、NHRP 登録タイムアウトは設定されていません。NHRP 登録は 200 秒ごとに送信されるため、NHS がダウンしていることを検出する時間は、平均 107 秒に対して、7 ～ 207 秒の範囲です。

```
Router# show ip nhrp nhs detail

Legend:
E=Expecting replies
R=Responding

Tunnel0:
10.0.0.1 E req-sent 14793 req-failed 1 repl-recv 14751 (00:25:07 ago)
10.0.0.2 req-sent 26 req-failed 9 repl-recv 0
Legend:
E=Expecting replies
R=Responding

Tunnel1:
10.0.1.1 RE req-sent 14765 req-failed 1 repl-recv 14763 (00:01:07 ago)

Pending Registration Requests:
Registration Request: Reqid 29507, Ret 64 NHS 10.0.0.1
Registration Request: Reqid 29511, Ret 64 NHS 10.0.0.2
```

10.0.0.1 は新規（応答待ち）でダウンしています。
10.0.0.2 は既存（応答待ちなし）でアップと見なされます。
10.0.1.1 は新規（応答待ち）でアップしています。

参考資料

ここでは、NHRP の設定に関連する資料について説明します。

関連資料

関連項目	参照先
DMVPN 機能を使用すると、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル、IP Security（IPsec; IP セキュリティ）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 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を構築できます。	『*Dynamic Multipoint VPN (DMVPN)*』
Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）ネットワーク上のルータは、Next Hop Resolution Protocol（NHRP）を使用して、DMVPN NonBroadcastMultiAccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワークに接続されているルータの背後にある、他のルータおよびネットワークのアドレスを検出します。NHRP は、ハブの障害、信頼性の低下、複雑なコンフィギュレーションなど、NBMA のネットワーク問題を緩和する ARP に似たソリューションを提供します。	『*Shortcut Switching Enhancements for NHRP in DMVPN Networks*』
NRHP コマンド	『*Cisco IOS IP Addressing Services Command Reference*』

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
シスコのテクニカル サポートおよびドキュメンテーション Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、ツール、技術マニュアルへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

NHRP 設定の機能情報

表 1 に、この機能のリリース履歴を示します。

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアル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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　NHRP 設定の機能情報

機能名	リリース	機能情報
Next Hop Resolution Protocol	Cisco IOS XE Release 2.1 15.0(1)S	この機能は、Cisco ASR 1000 シリーズ ルータで統合されました。