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。

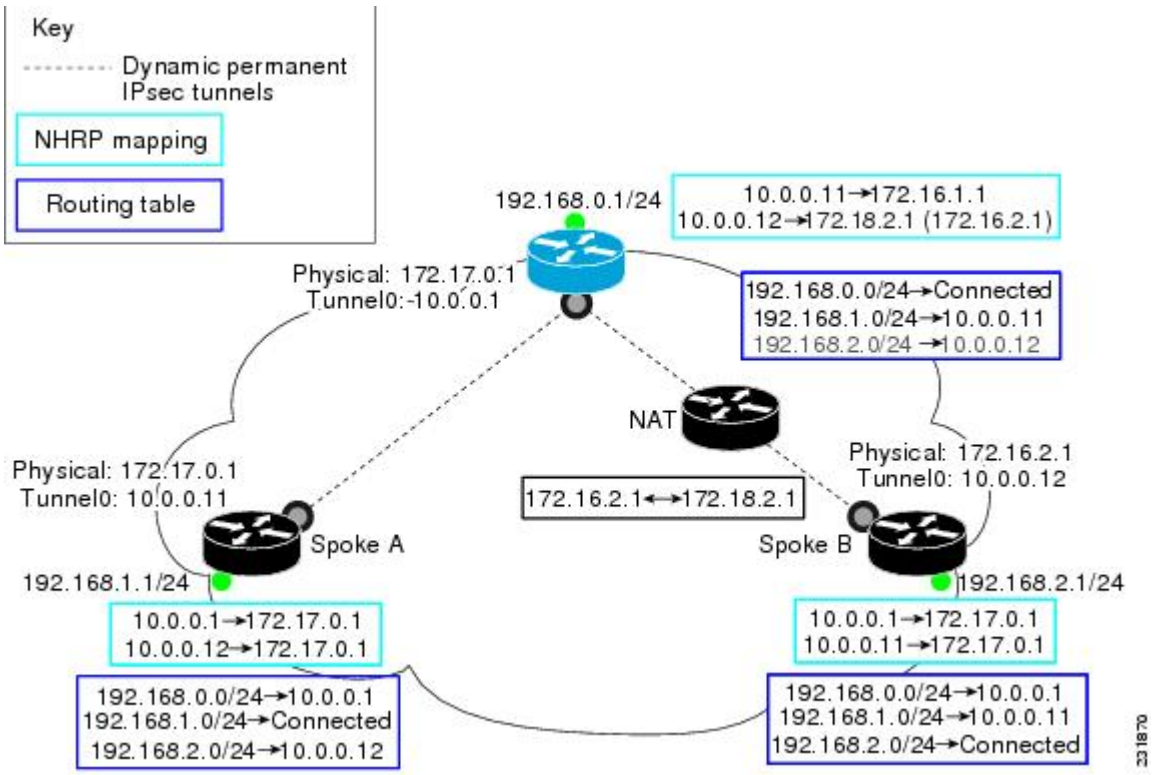
NATデバイスの背後に配置されていないスポークに制限されるDMVPN スポークツースポーク トンネリング

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 *1*：*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。

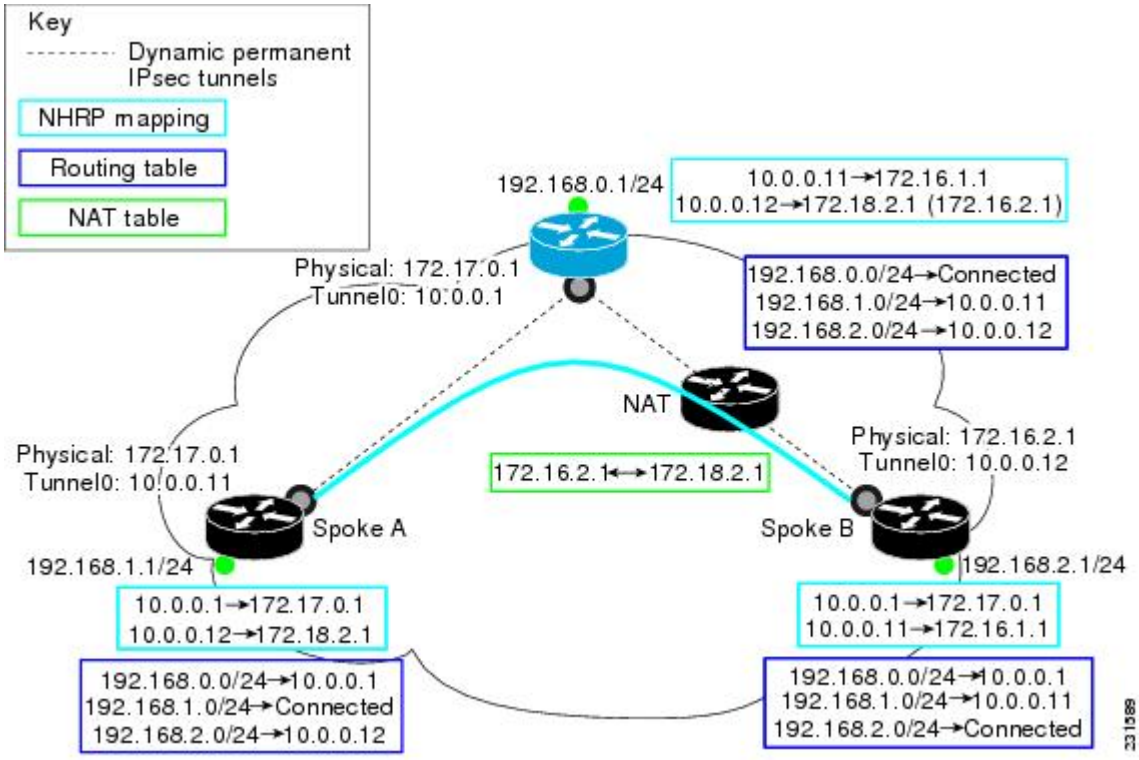
NAT デバイスを使用した NHRP スポークツースポーク トンネル

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 *2*：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 *1*：*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。