

DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device

The DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device feature allows Next Hop Resolution Protocol (NHRP) spoke-to-spoke tunnels to be built in Dynamic Multipoint Virtual Private Networks (DMVPNs), even if one or more spokes is behind a Network Address Translation (NAT) device.

- Feature Information for DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device, on page 1
- Restrictions for DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device, on page 1
- Information About DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device, on page 2
- Additional References, on page 6

Feature Information for DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device

In order for two spokes to build tunnels between them, they need to know the post-NAT address of the other spoke.

Consider the following restrictions when using spoke-to-spoke tunneling in NAT environments:

- **Multiple NAT translations** --A packet can go across multiple NAT devices in a nonbroadcast multiaccess (NBMA) DMVPN cloud and make several (unimportant) translations before it reaches its destination. The last translation is the important translation because it is used to create the NAT translation for all devices that reach a spoke through the last NAT device.

- **Hub or spoke can be reached through pre-NAT addresses** --It is possible for two or more spokes to be behind the same NAT device, which can be reached through a pre-NAT IP address. Only the post-NAT IP address is relied on even if it means that a tunnel may take a less desirable path. If both spokes use NAT through the same device, then a packet may not travel inside-out or outside-in as expected by the NAT device and translations may not occur correctly.
- **Interoperability between NAT and non-NAT capable devices** --In networks that are deployed with DMVPN, it is important that a device with NHRP NAT functionality operate together with non-NAT supported devices. A capability bit in the NHRP packet header indicates to any receiver whether a sending device understands a NAT extension.
- **Same NAT translation** --A spoke's post-NAT IP address must be the same when the spoke is communicating with its hubs and when it is communicating with other spokes. For example, a spoke must have the same post-NAT IP address no matter where it is sending tunnel packets within the DMVPN network.
- If one spoke is behind one NAT device and another different spoke is behind another NAT device, and Port Address Translation (PAT) is the type of NAT used on both NAT devices, then a session initiated between the two spokes cannot be established.

One example of a PAT configuration on a NAT interface is:

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

Information About DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device

The following sections describe how the DMVPN Dynamic Tunnels Between Spokes Behind a NAT Device feature allows spoke-to-spoke tunnels to be built even if one or both spoke devices are behind a NAT device:

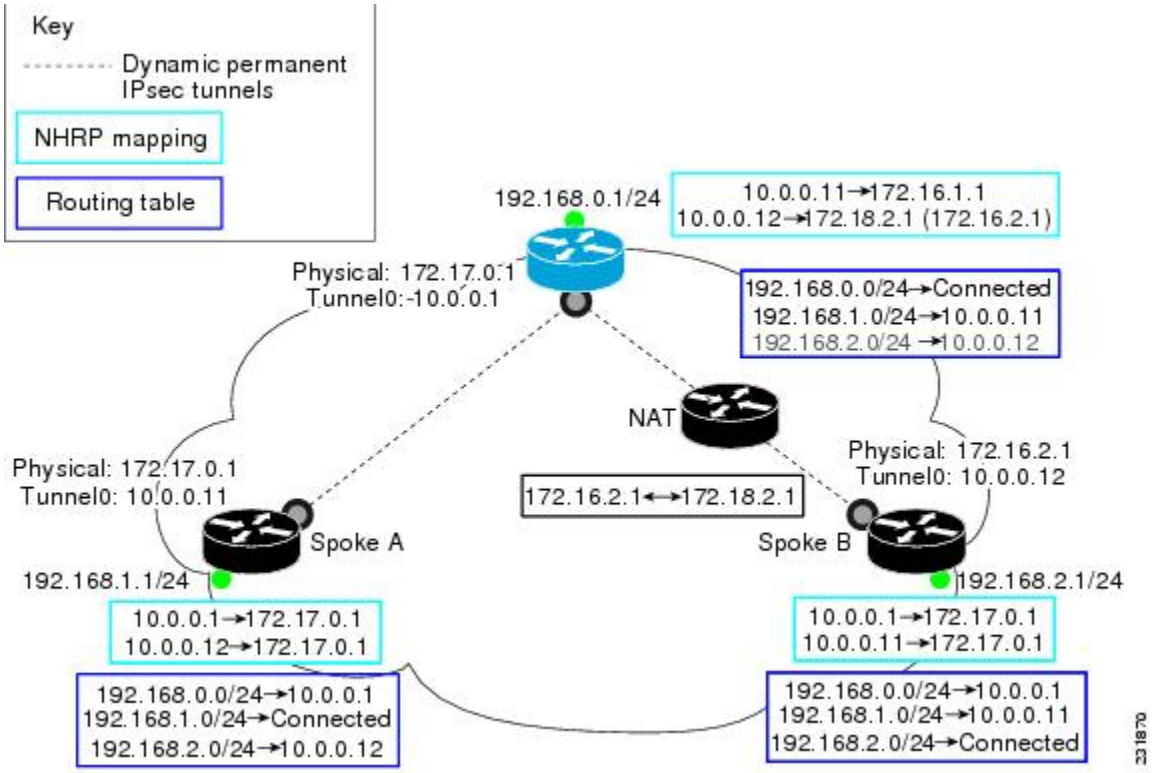
DMVPN Spoke-to-Spoke Tunneling Limited to Spokes Not Behind a NAT Device

NAT allows a single device, such as a router, to act as agent between the Internet (or "public network") and a local (or "private") network, and is often used because of the scarcity of available IP addresses. A single unique IP address is required to represent an entire group of devices to anything outside the NAT device. NAT is also deployed for security and administration purposes.

In DMVPN networks, spoke-to-spoke tunneling is limited to spokes that are not behind the NAT device. If one or both spokes are behind a NAT device, a spoke-to-spoke tunnel cannot be built to or from the NAT device because it is possible for the spoke-to-spoke tunnel traffic to fail or be lost for an extended period.

The figure below and the following sections describe how DMVPN works when spoke-to-spoke tunneling is limited to spokes that are not behind a NAT device.

Figure 1: Implementation of DMVPN Spoke-to-Spoke Tunneling Limited to Spokes Not Behind a NAT Device



NHRP Registration

When an NHRP registration is received, the hub checks the source IP address on the encapsulating GRE/IP header of the NHRP packet with the source NBMA IP address, which is contained in the NHRP registration packet. If these IP addresses are different, then NHRP knows that NAT is changing the outer IP header source address. The hub preserves both the pre- and post-NAT address of the registered spoke.

Note If encryption is used, then IPsec transport mode must be used to enable NHRP.

The following **show ip nhrp** command output example shows the source IP address of the NHRP packet and tunnel information for Spoke B in the figure above:

Note The NBMA (post-NAT) address for Spoke B is 172.18.2.1 (the claimed NBMA (pre-NAT) source address is 172.16.2.1).

```
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 Resolution

The following describes the NHRP resolution process between Spoke A and Spoke B shown in the figure above, where Spoke B is behind a NAT device with pre-NAT address of 172.16.2.1 and a post-NAT address of 172.18.2.1:

- The NHRP table entry for Spoke B on the hub contains both the post-NAT and pre-NAT addresses. When the hub receives an NHRP resolution request for the VPN address (tunnel address) of Spoke B, it answers with its own NBMA address instead of Spoke B's NBMA address.
- When the hub receives an NHRP resolution request sourced from Spoke B for any other spoke, the hub also answers with its own NBMA address. This ensures that any attempt to build a spoke-to-spoke tunnel with Spoke B results in the data packets being sent through the hub rather than through a spoke-to-spoke tunnel.

For example:

- Data traffic from source IP address 192.168.1.1 (behind Spoke A) to destination IP address 192.168.2.1 (behind Spoke B) triggers Spoke A to send a resolution request for Spoke B (10.0.0.12) to the next hop router (hub).
- The hub receives the resolution request and finds a mapping entry for Spoke B (10.0.0.12). Because Spoke B is behind a NAT device, it acts as a proxy and replies with its own NBMA address (172.17.0.1).
- The hub also receives a resolution request from Spoke B for Spoke A (10.0.0.11). Because Spoke B is behind a NAT device, it acts as a proxy and replies with its own NBMA address (172.17.0.1). This restricts any spoke-to-spoke traffic to or from Spoke B to travel through the hub router, which is done rather than having a tunnel between the spokes.

NHRP Spoke-to-Spoke Tunnel with a NAT Device

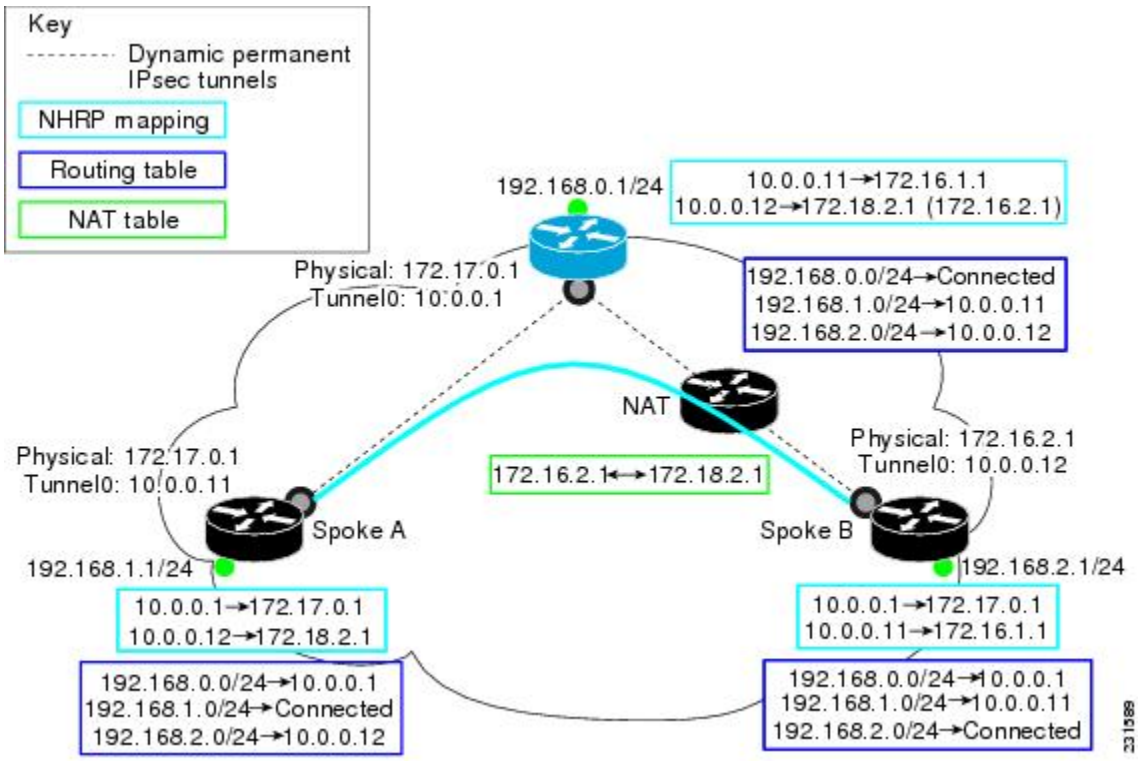
The NHRP Spoke-to-Spoke Tunnel with NAT feature introduces NAT extension in the NHRP protocol and is enabled automatically. The NHRP NAT extension is a Client Information Entry (CIE) entry with information about the protocol and post-NAT NBMA address. This additional information allows the support of spoke-to-spoke tunnels between spokes where one or both are behind a NAT device without the problem of losing traffic for an extended period.



Note The spoke-to-spoke tunnel may fail to come up, but it is detected and the data traffic flows through the hub, rather than being lost.

The figure below shows how the NHRP spoke-to-spoke tunnel works with NAT.

Figure 2: NHRP Between Spoke-to-Spoke Tunnels



NHRP Registration Process

The following steps describe the NHRP registration process:

1. A spoke sends a registration request with the NAT-Capability=1 parameter and a NAT NHRP extension of the NBMA address of the hub as configured on the spoke.
2. The hub compares the NHRP (NAT) extension with its configured NBMA address and determines whether it is or is not behind a NAT device. The hub also makes a note of whether the spoke is behind a NAT device by comparing the incoming GRE/IP source address with the spoke's NBMA address in the NHRP packet.
3. The registration reply from the hub to the spoke includes a NAT NHRP extension with the post-NAT address of the spoke, if the hub detects if it is behind a NAT device.
4. If the spokes get a NAT NHRP extension in the NHRP registration reply, it then records its post-NAT IP address for possible use later.

NHRP Resolution and Purge Process

The following steps describe the NHRP resolution and purge process:

1. When a spoke is behind a NAT device, it includes a NAT NHRP extension when it sends NHRP resolution requests.
2. The hub receives the resolution request. If the spoke is behind a NAT device and there is no NAT extension, then the hub adds a NAT extension before forwarding this extension to the next node (spoke or next hop

server) along the path. However, if the hub is forwarding the request to a non-NAT extension capable node, it rewrites the source-NBMA inside the packet to be the post-NAT IP address for the requesting spoke rather than its pre-NAT IP address.

3. The receiver (spoke) uses a NAT NHRP extension record (NAT capable) or the source NBMA address (non-NAT capable information) to build the tunnel. This spoke's reply includes its own NAT extension if it is behind a NAT device.



Note Hubs do not answer NHRP resolution requests on behalf of spokes. Hubs always forward NHRP resolution requests to the end spoke that has the requested tunnel IP address or services the requested data from the host IP address.

The following describes the NHRP resolution process between Spoke A and Spoke B shown in the figure above, where Spoke B is behind a NAT device with pre-NAT address 172.16.2.1 and post-NAT address of 172.18.2.1:

- Data traffic to the 192.168.2.0/24 network from hosts behind Spoke A triggers an NHRP resolution request for Spoke B's tunnel IP address (10.0.0.12) to be sent through the hub. The hub receives a resolution request and forwards it to Spoke B. Spoke B creates a dynamic spoke-to-spoke tunnel using the source NBMA IP address for Spoke A from the NHRP resolution request and sends an NHRP resolution reply directly to Spoke A. It includes its post-NAT address in the NAT NHRP-extension header.
- Alternatively, traffic to the192.168.1.0/24 network from hosts behind the NAT device on Spoke B triggers an NHRP resolution request for Spoke A's tunnel IP address (10.0.0.11). Spoke B adds its own post-NAT IP address in the NHRP NAT-extension in the resolution request. The hub receives a resolution request and forwards it to Spoke A. Spoke A parses the NHRP NAT-extension and builds a tunnel using Spoke B's post-NAT address and replies directly to Spoke B.

Additional References

Related Documents

Related Topic	Document Title
NHRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
Dynamic Multipoint VPN	"Dynamic Multipoint VPN (DMVPN)" module in the *Cisco IOS XE Security Configuration Guide: Secure Connectivity*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html