Implementing Dynamic Multipoint VPN for IPv6

First Published: July 11, 2008
Last Updated: November 24, 2010

This document describes how to implement Dynamic Multipoint VPN for IPv6 feature, which allows users to better scale large and small IPsec Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IP security (IPsec) encryption, and the Next Hop Resolution Protocol (NHRP). In Dynamic Multipoint Virtual Private Network (DMVPN) for IPv6, the public network (the Internet) is a pure IPv4 network, and the private network (the intranet) is IPv6 capable.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for Implementing DMVPN for IPv6” section on page 26.

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

Contents

- Prerequisites for Implementing DMVPN for IPv6, page 2
- Restrictions for Implementing DMVPN for IPv6, page 2
- Information About Implementing DMVPN for IPv6, page 2
- How to Configure DMVPN for IPv6, page 4
- Configuration Examples for Implementing DMVPN for IPv6, page 20
- Additional References, page 24
- Feature Information for Implementing DMVPN for IPv6, page 26
Prerequisites for Implementing DMVPN for IPv6

- This document assumes that you are familiar with IPv6 and IPv4. See the publications referenced in the “Additional References” section for IPv6 and IPv4 configuration and command reference information.
- Perform basic IPv6 addressing and basic connectivity as described in “Implementing IPv6 Addressing and Basic Connectivity.”
- Supported routing protocols include Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), On-Demand Routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP). One of these protocols must be enabled for DMVPN for IPv6 to work.

Restrictions for Implementing DMVPN for IPv6

- IPV6 can be configured only on the protected network.
- Every IPv6 NHRP interface is configured with one IPv6 unicast address. This address can be a globally reachable or unique local address.
- Every IPv6 NHRP interface is configured with one IPv6 link-local address that is unique across all the DMVPN hosts in the DMVPN cloud (that is, the hubs and spokes).
- IPv6 VRFs are not supported fully by IPv6 routing protocols such as EIGRP or OSPF. Therefore, DMVPN for IPv6 does not support IPv6 VRFs.
- The WAN network has to be a IPv4 network.

Information About Implementing DMVPN for IPv6

- DMVPN for IPv6 Overview, page 2

DMVPN for IPv6 Overview

The DMVPN feature combines NHRP routing, multipoint generic routing encapsulation (mGRE) tunnels, and IPsec encryption to provide users an ease of configuration via crypto profiles—which override the requirement for defining static crypto maps—and dynamic discovery of tunnel endpoints. This feature relies on the following Cisco enhanced standard technologies:

- NHRP—A client and server protocol where the hub is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes to build direct tunnels.
- mGRE tunnel interface—An mGRE tunnel interface allows a single GRE interface to support multiple IPsec tunnels and simplifies the size and complexity of the configuration.
- IPsec encryption—An IPsec tunnel interface allows for the protection of site-to-site IPv6 traffic with native encapsulation.
In DMVPN for IPv6, the public network (the Internet) is a pure IPv4 network, and the private network (the intranet) is IPv6 capable. The intranets could be a mix of IPv4 or IPv6 clouds connected to each other using the DMVPN technologies, with the underlying carrier being traditional IPv4.

**NHRP Routing**

The NHRP protocol resolves a given intranet address (IPv4 or IPv6) to an Internet address (IPv4 nonbroadcast multiaccess [NBMA] address).

In Figure 1, the intranets that are connected over the DMVPN network are IPv6 clouds, and the Internet is a pure IPv4 cloud. Spokes S1 and S2 are connected to the Hub H over the Internet using a statically configured mGRE tunnel. The address of the tunnel itself is in the IPv6 domain, because it is another node on the intranet. The source and destinations of the tunnel (the mGRE endpoints), however, are always in IPv4, in the Internet domain. The mGRE tunnel is aware of the IPv6 network because the GRE passenger protocol is an IPv6 packet, and the GRE transport (or carrier) protocol is an IPv4 packet.

**Figure 1  IPv6 Topology That Triggers NHRP**

When an IPv6 host in LAN L1 sends a packet destined to an IPv6 host in LAN L2, the packet is first routed to the gateway (which is Spoke S1) in LAN L1. Spoke S1 is a dual-stack router, which means both IPv4 and IPv6 are configured. The IPv6 routing table in S1 points to a next hop, which is the IPv6 address of the tunnel on Spoke S2. This is a VPN address that must be mapped to an NBMA address, triggering NHRP.

**IPv6 NHRP Redirect and Shortcut Features**

When IPv6 NHRP redirect is enabled, NHRP examines every data packet in the output feature path. If the data packet enters and leaves on the same logical network, it sends an NHRP traffic indication message to the originator of the data packet. In NHRP, a logical network is identified by the NHRP network ID, which groups multiple physical interfaces into a single logical network.
When IPv6 NHRP shortcut is enabled, NHRP intercepts every data packet in the output feature path. It checks to see if there is an NHRP cache entry to the destination of the data packet and, if yes, it replaces the current output adjacency with the one present in the NHRP cache. The data packet is therefore switched out using the new adjacency provided by NHRP.

IPv6 Routing

NHRP is automatically invoked for mGRE tunnels carrying the IPv6 passenger protocol. When a packet is routed and the packet is sent to the switching path, NHRP looks up the given next hop and, if required, initiates an NHRP resolution query. If the resolution is successful, NHRP populates the tunnel endpoint database, which then populates the Cisco Express Forwarding adjacency table. The subsequent packets are Cisco Express Forwarding switched if Cisco Express Forwarding is enabled.

IPv6 Addressing and Restrictions

IPv6 allows multiple unicast addresses on a given IPv6 interface. IPv6 also allows special address types, such as anycast, multicast, link-local addresses, and unicast addresses.

DMVPN for IPv6 has the following addressing restrictions:

- Every IPv6 NHRP interface is configured with one IPv6 unicast address. This address can be a globally reachable or unique local address.
- Every IPv6 NHRP interface is configured with one IPv6 link-local address that is unique across all the DMVPN hosts in the DMVPN cloud (that is, the hubs and spokes).
  - If no other tunnels on the router are using the same tunnel source, then the tunnel source address can be embedded into an IPv6 address.
  - If the router has only one DMVPN IPv6 tunnel, then manual configuration of the IPv6 link-local address is not required. Instead, use the `ipv6 enable` command to autogenerate a link-local address.
  - If the router has more than one DMVPN IPv6 tunnel, then the link-local address must be manually configured using the `ipv6 address fe80::2001 link-local` command.

How to Configure DMVPN for IPv6

To enable mGRE and IPsec tunneling for hub and spoke routers, you must configure an IPsec profile that uses a global IPsec policy template and configure your mGRE tunnel for IPsec encryption. This section contains the following procedures:

- Configuring an IPsec Profile in DMVPN for IPv6, page 5 (required)
- Configuring the Hub for IPv6 over DMVPN, page 6 (required)
- Configuring the Spoke for IPv6 over DMVPN, page 10 (required)
- Verifying DMVPN for IPv6 Configuration, page 14 (optional)
- Monitoring and Maintaining DMVPN for IPv6 Configuration and Operation, page 15 (optional)
Configuring an IPsec Profile in DMVPN for IPv6

The IPsec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPsec profile. Only commands that pertain to an IPsec policy can be issued under an IPsec profile; you cannot specify the IPsec peer address or the access control list (ACL) to match the packets that are to be encrypted.

Prerequisites

Before configuring an IPsec profile, you must do the following:

- Define a transform set by using the `crypto ipsec transform-set` command.
- Make sure that Internet Security Association Key Management Protocol (ISAKMP) is configured with default ISAKMP settings. For further information about default ISAKMP settings, see the Implementing IPsec in IPv6 Security module and the Cisco IOS IPv6 Command Reference.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto identity name`
4. `crypto ipsec profile name`
5. `set transform-set transform-set-name`
6. `set identity`
7. `set security-association lifetime {seconds seconds | kilobytes kilobytes}`
8. `set pfs [group1 | group2]`
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>crypto identity name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto identity router1</td>
</tr>
<tr>
<td></td>
<td>Configures the identity of the router with a given list of distinguished names (DNs) in the certificate of the router.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>crypto ipsec profile name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto ipsec profile example1</td>
</tr>
<tr>
<td></td>
<td>Defines the IPsec parameters that are to be used for IPsec encryption between “spoke and hub” and “spoke and spoke” routers.</td>
</tr>
<tr>
<td></td>
<td>This command places the router in crypto map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>set transform-set transform-set-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-crypto-map)# set transform-set example-set</td>
</tr>
<tr>
<td></td>
<td>Specifies which transform sets can be used with the IPsec profile.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>set identity</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-crypto-map)# set identity router1</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies identity restrictions to be used with the IPsec profile.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>set security-association lifetime {seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-crypto-map)# set security-association lifetime seconds 1800</td>
</tr>
<tr>
<td></td>
<td>(Optional) Overrides the global lifetime value for the IPsec profile.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>set pfs [group1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-crypto-map)# set pfs group2</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this IPsec profile.</td>
</tr>
</tbody>
</table>

**Configuring the Hub for IPv6 over DMVPN**

This task describes how to configure the hub router for IPv6 over DMVPN for mGRE and IPsec integration (that is, associate the tunnel with the IPsec profile configured in the previous procedure).
SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. ipv6 address {ipv6-address|prefix-length |prefix-name sub-bits|prefix-length}
5. ipv6 address ipv6-address |prefix-length link-local
6. ipv6 mtu bytes
7. ipv6 nhrp authentication string
8. ipv6 nhrp map multicast dynamic
9. ipv6 nhrp network-id network-id
10. tunnel source {ip-address |ipv6-address |interface-type interface-number}
11. tunnel mode {aurp |cayman |dvmrp |eon |gre |gre multipoint |gre ipv6 |ipip [decapsulate-any] |ipsec ipv4 |iptalk |ipv6 |ipsec ipv6 |mpls |nos |rbscp}
12. tunnel protection ipsec profile name [shared]
13. bandwidth {interzone |total |session} {default |zone zone-name} bandwidth-size
14. ipv6 nhrp holdtime seconds
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface tunnel number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface tunnel 5</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ipv6 address {ipv6-address/prefix-length</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 address 2001:DB8:1:1::72/64</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ipv6 address ipv6-address/prefix-length link-local</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 address fe80::2001 link-local</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ipv6 mtu bytes</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 mtu 1400</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ipv6 nhrp authentication string</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 nhrp authentication examplexx</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ipv6 nhrp map multicast dynamic</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 nhrp map multicast dynamic</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>ipv6 nhrp network-id network-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 nhrp network-id 99</td>
</tr>
</tbody>
</table>
# Implementing Dynamic Multipoint VPN for IPv6

## How to Configure DMVPN for IPv6

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>`tunnel source {ip-address</td>
<td>ipv6-address</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# tunnel source ethernet 0</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>`tunnel mode {aurp</td>
<td>cayman</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# tunnel mode gre multipoint</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>tunnel protection ipsec profile name [shared]</code></td>
<td>Associates a tunnel interface with an IPsec profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# tunnel protection ipsec profile example_profile</code></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>`bandwidth {interzone</td>
<td>total</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# bandwidth total 1200</code></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>ipv6 nhrp holdtime seconds</code></td>
<td>Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# ipv6 nhrp holdtime 3600</code></td>
<td></td>
</tr>
</tbody>
</table>

## Configuring the NHRP Redirect and Shortcut Features On the Hub

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel *number*
4. ipv6 address `{ipv6-address/prefix-length \ prefix-name sub-bits/prefix-length}`
5. ipv6 nhrp redirect [timeout *seconds*]
6. ipv6 nhrp shortcut
Implementing Dynamic Multipoint VPN for IPv6

How to Configure DMVPN for IPv6

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface tunnel number</td>
<td>Configures a tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface tunnel 5</td>
<td>The number argument specifies the number of the tunnel interfaces that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 address {ipv6-address/prefix-length</td>
<td>prefix-name sub-bits/prefix-length}</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ipv6 address 2001:DB8:1:1::72/64</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ipv6 nhrp redirect [timeout seconds]</td>
<td>Enables NHRP redirect.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ipv6 nhrp redirect</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ipv6 nhrp shortcut</td>
<td>Enables NHRP shortcut switching.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ipv6 nhrp shortcut</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring the Spoke for IPv6 over DMVPN**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface tunnel number
4. ipv6 address {ipv6-address/prefix-length | prefix-name sub-bits/prefix-length}
5. ipv6 address ipv6-address/prefix-length link-local
6. ipv6 mtu bytes
7. ipv6 nhrp authentication string
8. ipv6 nhrp map ipv6-address nbma-address
9. ipv6 nhrp map multicast ipv4-nbma-address
10. `ipv6 nhrp nhs ipv6-nhs-address [net-address]`
11. `ipv6 nhrp network-id network-id`
12. `tunnel source {ip-address | ipv6-address | interface-type interface-number}`
13. `tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre ipv6 | ipip
   [decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp}`
   or
   `tunnel destination {host-name | ip-address | ipv6-address}`
14. `tunnel protection ipsec profile name [shared]`
15. `bandwidth {interzone | total | session} {default | zone zone-name} bandwidth-size`
16. `ipv6 nhrp holdtime seconds`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface tunnel number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface tunnel 5</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures a tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>The <code>number</code> argument specifies the number of the tunnel interfaces that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ipv6 address {ipv6-address/prefix-length</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if) ipv6 address 2001:DB8:1:1::72/64</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures an IPv6 address based on an IPv6 general prefix and enablers IPv6 processing on an interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ipv6 address ipv6-address/prefix-length link-local</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 address fe80::2001 link-local</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures an IPv6 link-local address for an interface and enable IPv6 processing on the interface.</td>
</tr>
<tr>
<td></td>
<td>A unique IPv6 link local address (across all DMVPN nodes in a DMVPN network) must be configured.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ipv6 mtu bytes</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 mtu 1400</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Sets the MTU size of IPv6 packets sent on an interface.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ipv6 nhrp authentication string</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 nhrp authentication examplexx</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures the authentication string for an interface using the NHRP.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ipv6 nhrp map ipv6-address nbma-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ipv6 nhrp map 2001:DB8:3333:4::5 10.1.1.1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Statically configures the IPv6-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only IPv4 NBMA addresses are supported, not ATM or Ethernet addresses.</td>
</tr>
</tbody>
</table>
### Steps to Configure DMVPN for IPv6

1. **Step 9**
   - **Command:** `ipv6 nhrp map multicast ipv4-nbma-address`
   - **Example:**
     ```
     Router(config-if)# ipv6 nhrp map multicast 10.11.11.99
     ```
   - **Purpose:** Maps destination IPv6 addresses to IPv4 NBMA addresses.

2. **Step 10**
   - **Command:** `ipv6 nhrp nhs ipv6-nhs-address [net-address]`
   - **Example:**
     ```
     Router(config-if)# ipv6 nhrp nhs 2001:DB8:3333:4::5 2001:DB8::/64
     ```
   - **Purpose:** Specifies the address of one or more IPv6 NHRP servers.

3. **Step 11**
   - **Command:** `ipv6 nhrp network-id network-id`
   - **Example:**
     ```
     Router(config-if)# ipv6 nhrp network-id 99
     ```
   - **Purpose:** Enables the NHRP on an interface.

4. **Step 12**
   - **Command:** `tunnel source {ip-address | ipv6-address | interface-type interface-number}`
   - **Example:**
     ```
     Router(config-if)# tunnel source ethernet 0
     ```
   - **Purpose:** Sets the source address for a tunnel interface.

5. **Step 13**
   - **Command:** `tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre ipv6 | ipip | decapsulate-any | ipsec ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp}`
   - **Purpose:** Sets the encapsulation mode to mGRE for the tunnel interface.
   - **Example:**
     ```
     Router(config-if)# tunnel mode gre multipoint
     ```
   - Use this command if data traffic can use dynamic spoke-to-spoke traffic.
   - **Purpose:** Specifies the destination for a tunnel interface.
   - **Example:**
     ```
     Router(config-if)# tunnel destination 10.1.1.1
     ```
   - Use this command if data traffic can use hub-and-spoke tunnels.

6. **Step 14**
   - **Command:** `tunnel protection ipsec profile name [shared]`
   - **Example:**
     ```
     Router(config-if)# tunnel protection ipsec profile example1
     ```
   - **Purpose:** Associates a tunnel interface with an IPsec profile.
   - **Note:** The `name` argument specifies the name of the IPsec profile; this value must match the name specified in the `crypto ipsec profile name` command.
Verifying DMVPN for IPv6 Configuration

Perform this optional task to display information to verify DMVPN for IPv6 configuration. Use the following optional commands as needed to verify configuration and operation.

**SUMMARY STEPS**

1. `enable`
2. `show dmvpn [ipv4 | ipv6] [peer [nbma | tunnel [ip-address | ipv6-address]]] [network {ip-address | mask}] [vrf vrf-name] [interface tunnel number] [detail] [static] [debug-condition]
3. `show ipv6 nhrp [dynamic [ipv6-address] | incomplete | static [address | interface] [brief | detail] [purge]
4. `show ipv6 nhrp multicast [ipv6-address | interface]
5. `show ipv6 nhrp summary
6. `show ipv6 nhrp traffic [interface tunnel number]`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable |
| **Step 2** show dmvpn [ipv4 | ipv6] [peer [nbma | tunnel [ip-address | ipv6-address]] [network [ip-address mask] [vrf vrf-name] [interface tunnel number] [detail] [static] [debug-condition] | Displays DMVPN-specific session information. |
| **Example:** Router> show dmvpn 2001:DB8:1:1::72/64 |
| **Step 3** show ipv6 nhrp [dynamic [ipv6-address] | incomplete | static] [address | interface] [brief | detail] [purge] | Displays NHRP mapping information. |
| **Example:** Router# show ipv6 nhrp |
| **Step 4** show ipv6 nhrp multicast [ipv6-address] | Displays NHRP multicast mapping information. |
| **Example:** Router# show ipv6 nhrp multicast |
| **Step 5** show ipv6 nhrp summary | Displays NHRP mapping summary information. |
| **Example:** Router# show ipv6 nhrp summary |
| **Step 6** show ipv6 nhrp traffic [interface tunnel number] | Displays NHRP traffic statistics information. |
| **Example:** Router# show ipv6 nhrp traffic |

Monitoring and Maintaining DMVPN for IPv6 Configuration and Operation

SUMMARY STEPS

1. enable
2. clear dmvpn session [peer [nbma | tunnel ipv4-address | ipv6-address]] [interface tunnel number] [vrf vrf-name] [static]
3. clear ipv6 nhrp [ipv6-address | counters]
4. debug dmvpn [condition [unmatched]] [peer [nbma | tunnel | ipv4-address | ipv6-address]] [vrf [vrf-name] [interface {tunnel number} error | detail | packet | all] nhrp [crypto | tunnel | socket | all]
5. debug nhrp [ipv4 | ipv6] [cache | extension | packet | rate]
6. `debug nhrp condition [peer [nbma | tunnel [ip-address | ipv6-address]] | interface tunnel number | [vrf vrf-name]]`

7. `debug nhrp {ipv4 | ipv6} error`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> `clear dmvpn session [peer [nbma</td>
<td>tunnel ipv4-address</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# clear dmvpn session</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `clear ipv6 nhrp [ipv6-address</td>
<td>counters]`</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# clear ipv6 nhrp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `debug dmvpn [condition [unmatched]</td>
<td>[peer [nbma</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# debug dmvpn</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> `debug nhrp {ipv4</td>
<td>ipv6} [cache</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# debug nhrp ipv6</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> `debug nhrp condition [peer [nbma</td>
<td>tunnel [ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# debug nhrp condition</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> `debug nhrp {ipv4</td>
<td>ipv6} error`</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router# debug nhrp ipv6 error</code></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

- Sample Output from the show dmvpn Command, page 17
Sample Output from the show ipv6 nhrp Command, page 18
Sample Output for the debug nhrp Command, page 19

Sample Output from the show dmvpn Command

The following sample output is from the `show dmvpn` command, with the `ipv6` and `detail` keywords, for the hub:

```
Router# 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 : Ox BB0ED02, transform : esp-3des 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 : Ox B79B277B, transform : esp-3des esp-sha-hmac
    Socket State: Open
```

The following sample output is from the `show dmvpn` command, with the `ipv6` and `detail` keywords, for the spoke:
Router# `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 10.0.0.1, 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-3des esp-sha-hmac
Socket State: Open

Sample Output from the show ipv6 nhrp Command
The following sample output is from the `show ipv6 nhrp` command for the hub and the spoke:

Hub
Router# `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
Implementing Dynamic Multipoint VPN for IPv6

How to Configure DMVPN for IPv6

Spoke

Router# 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

Sample Output from the show ipv6 nhrp multicast Command

The following sample output is from the `show ipv6 nhrp multicast` command for the hub and the spoke:

Hub

Router# show ipv6 nhrp multicast

<table>
<thead>
<tr>
<th>I/F</th>
<th>NBMA address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>192.169.2.10</td>
</tr>
<tr>
<td>Tunnel1</td>
<td>192.169.2.11</td>
</tr>
</tbody>
</table>

Spoke

Router# show ipv6 nhrp multicast

<table>
<thead>
<tr>
<th>I/F</th>
<th>NBMA address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>192.169.2.9</td>
</tr>
</tbody>
</table>

Sample Output for the show ipv6 nhrp traffic Command

The following sample output is from the `show ipv6 nhrp traffic` command:

Router# show ipv6 nhrp traffic

Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 8
   1 Resolution Request 1 Resolution Reply 6 Registration Request
   0 Registration Reply 0 Purge Request 0 Purge Reply
   0 Error Indication 0 Traffic Indication
Rcvd: Total 5
   1 Resolution Request 1 Resolution Reply 0 Registration Request
   2 Registration Reply 0 Purge Request 0 Purge Reply
   0 Error Indication 1 Traffic Indication

Sample Output for the debug nhrp Command

The following sample output is from the `debug nhrp` command with the `ipv6` keyword:

Router# debug nhrp ipv6

Aug 9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
   dst: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Configuration Examples for Implementing DMVPN for IPv6

- Example: Configuring an IPsec Profile, page 20
- Example: Configuring the Hub for DMVPN, page 20
- Example: Configuring the NHRP Redirect and Shortcut Features On the Hub, page 22
- Example: Configuring the Spoke for DMVPN, page 22

Example: Configuring an IPsec Profile

Router(config)# crypto identity router1
Router(config)# crypto ipsec profile example1
Router(config-crypto-map)# set transform-set example-set
Router(config-crypto-map)# set identity router1
Router(config-crypto-map)# set security-association lifetime seconds 1800
Router(config-crypto-map)# set pfs group2

Example: Configuring the Hub for DMVPN

Router# show running-config

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Hub-99
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
clock timezone IST 0
!
mmi polling-interval 60
!
no mmi auto-configure
!
no mmi pvc
!
mmi snmp-timeout 180

ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!

ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
crypto isakmp policy 1
banner pre-share
crypto isakmp key cisco123 address 10.0.0.0 0.0.0.0
!
crypto ipsec transform-set cisco-ts esp-3des esp-md5-hmac
mode transport
!
crypto ipsec profile cisco-ipsec
set transform-set cisco-ts

interface Tunnel0
bandwidth 100000
ip address 10.1.1.99 255.255.255.0
no ip redirects
ip nhrp map multicast dynamic
delay 50000
ipv6 address 2001:DB8:99/64 2001:DB8::99/64
ipv6 address FE80::0B:0B:0B:8F link-local
ipv6 enable
ipv6 eigrp 1
no ipv6 split-horizon eigrp 1
no ipv6 next-hop-self eigrp 1
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 99
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec
!
interface Ethernet0/0
ip address 10.11.11.99 255.255.255.0
!
interface Ethernet0/1
no ip address
shutdown
!
interface Ethernet0/2
no ip address
shutdown
interface Ethernet0/3
no ip address
shutdown
!
interface Ethernet1/0
no ip address
ipv6 address 2001:DB8:EEEE::99/64
ipv6 enable
ipv6 eigrp 1
!
interface Ethernet1/1
no ip address
shutdown
!
interface Ethernet1/2
no ip address
shutdown
!
interface Ethernet1/3
no ip address
shutdown
!
Example: Configuring the NHRP Redirect and Shortcut Features On the Hub

Router(config)# interface tunnel 5
Router(config-if)# ipv6 address 2001:DB8:1:1::72/64
Router(config-if)# ipv6 nhrp redirect
Router(config-if)# ipv6 nhrp shortcut

Example: Configuring the Spoke for DMVPN

Router# show running-config

Version 12.4
Service timestamps debug datetime msec
Service timestamps log datetime msec
No service password-encryption
Hostname Spoke-11
Boot-start-marker
Boot-end-marker
Logging message-counter syslog
No aaa new-model
Clock timezone IST 0
Mmi polling-interval 60
No mmi auto-configure
No mmi pvc
Mmi snmp-timeout 180
Ip auth-proxy max-nodata-conns 3
Ip admission max-nodata-conns 3
Ip cef
Ipv6 unicast-routing
Ipv6 cef
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 10.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set cisco-ts esp-3des esp-md5-hmac
mode transport
!
crypto ipsec profile cisco-ipsec
set transform-set cisco-ts
!
interface Tunnel0
bandwidth 100000
no ip address
no ip redirects
delay 50000
ipv6 address 2001:DB8::11/64
ipv6 address FE80::0B:0B:0B:0B link-local
ipv6 eigrp 1
no ipv6 split-horizon eigrp 1
no ipv6 next-hop-self eigrp 1
ipv6 nhrp map 2001:DB8::11/64 10.11.11.99
ipv6 nhrp map multicast 10.11.11.99
ipv6 nhrp network-id 99
ipv6 nhrp nh 2001:DB8::99
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec
!
interface Ethernet0/0
ip address 10.11.11.11 255.255.255.0
ipv6 enable
ipv6 nd ra mtu suppress
!
interface Ethernet0/1
no ip address
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
interface Ethernet1/0
ip address 172.16.11.11 255.255.255.0
ipv6 address 2001:DB8:dddd::1/64
ipv6 enable
ipv6 nd ra mtu suppress
ipv6 eigrp 1
!
interface Ethernet1/1
no ip address
shutdown
ipv6 enable
ipv6 nd ra mtu suppress
!
interface Ethernet1/2
   no ip address
   shutdown
!
interface Ethernet1/3
   no ip address
   shutdown
!
ip forward-protocol nd
!
ip http server
   no ip http secure-server
!
ipv6 router eigrp 1
   no shutdown
   control-plane
!
line con 0
   exec-timeout 0 0
   logging synchronous
line aux 0
line vty 0 4
   login
!
exception data-corruption buffer truncate

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 basic connectivity</td>
<td>“Implementing IPv6 Addressing and Basic Connectivity,” Cisco IOS IPv6 Configuration Guide</td>
</tr>
<tr>
<td>IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS IPv6 Command Reference</td>
</tr>
<tr>
<td>DMVPN commands for IPv4</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
<tr>
<td>NHRP for IPv4</td>
<td>“Configuring NHRP” module of the Cisco IOS IP Addressing Services Configuration Guide</td>
</tr>
<tr>
<td>NHRP commands for IPv4</td>
<td>“NHRP Commands” section of the Cisco IOS IP Addressing Services Command Reference</td>
</tr>
</tbody>
</table>
## Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2332</td>
<td>NBMA Next Hop Resolution Protocol (NHRP)</td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for Implementing DMVPN for IPv6

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

Table 1 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.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMVPN for IPv6</td>
<td>12.4(20)T</td>
<td>The Dynamic Multipoint VPN feature allows users to better scale large and small IPsec Virtual Private Networks by combining generic routing encapsulation tunnels, IPsec encryption, and NHRP. In DMVPN for IPv6, the public network (the Internet) is a pure IPv4 network, and the private network (the intranet) is IPv6 capable.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008–2011 Cisco Systems, Inc. All rights reserved.