



Implementing Dynamic Multipoint VPN for IPv6

First Published: July 11, 2008

Last Updated: July 22, 2011

This document describes how to implement the 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.

In Cisco IOS Release 15.2(1)T, IPv6 support on DMVPN was extended to the public network (the Internet) facing the Internet service provider (ISP). The IPv6 transport for DMVPN feature builds IPv6 WAN-side capability into NHRP tunnels and the underlying IPsec encryption, and enables IPv6 to transport payloads on the Internet.



Note

The IPv6 transport for DMVPN feature is enabled by default. You need not upgrade your private internal network to IPv6 for the IPv6 transport for DMVPN feature to function. You can have either IPv4 or IPv6 addresses on your local networks.

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 24.

Use Cisco Feature Navigator to find information about platform support and Cisco 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](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Restrictions for Implementing DMVPN for IPv6, page 2](#)
- [Information About Implementing DMVPN for IPv6, page 2](#)
- [How to Configure DMVPN for IPv6, page 5](#)
- [Configuration Examples for Implementing DMVPN for IPv6, page 20](#)
- [Additional References, page 22](#)
- [Feature Information for Implementing DMVPN for IPv6, page 24](#)

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](#).”
- One of the following protocols must be enabled for DMVPN for IPv6 to work: Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), On-Demand Routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
- 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 DMVPN hosts in the DMVPN cloud (that is, the hubs and spokes).
- Before a multipoint GRE (mGRE) and IPsec tunnel can be established, you must define an Internet Key Exchange (IKE) policy by using the **crypto isakmp policy** command.

Restrictions for Implementing DMVPN for IPv6

- IPv6 can be configured only on a protected network.
- Every IPv6 NHRP interface is configured with one IPv6 unicast address. This address can be a globally reachable address or a unique local address.
- Every IPv6 NHRP interface is configured with one IPv6 link-local address that is unique across all DMVPN nodes in the DMVPN cloud (that is, the hubs and spokes).
- IPv6 VRFs are not fully supported by IPv6 routing protocols such as EIGRP or OSPF. Therefore, DMVPN for IPv6 does not support IPv6 VRFs.
- Per tunnel QoS, DHCP-Tunnels Support, and 2547oDMVPN—Enabling Traffic Segmentation within DMVPN features are not supported for IPv6.
- Internet Key Exchange version 1 (IKEv1) and Network Address Translation 66 (NAT66) are not supported.

Information About Implementing DMVPN for IPv6

- [DMVPN for IPv6 Overview, page 3](#)

- [mGRE Support over IPv6, page 5](#)

DMVPN for IPv6 Overview

The DMVPN feature combines NHRP routing, multipoint generic routing encapsulation (mGRE) tunnels, and IPsec encryption to provide users 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 facilitates for the protection of site-to-site IPv6 traffic with native encapsulation.

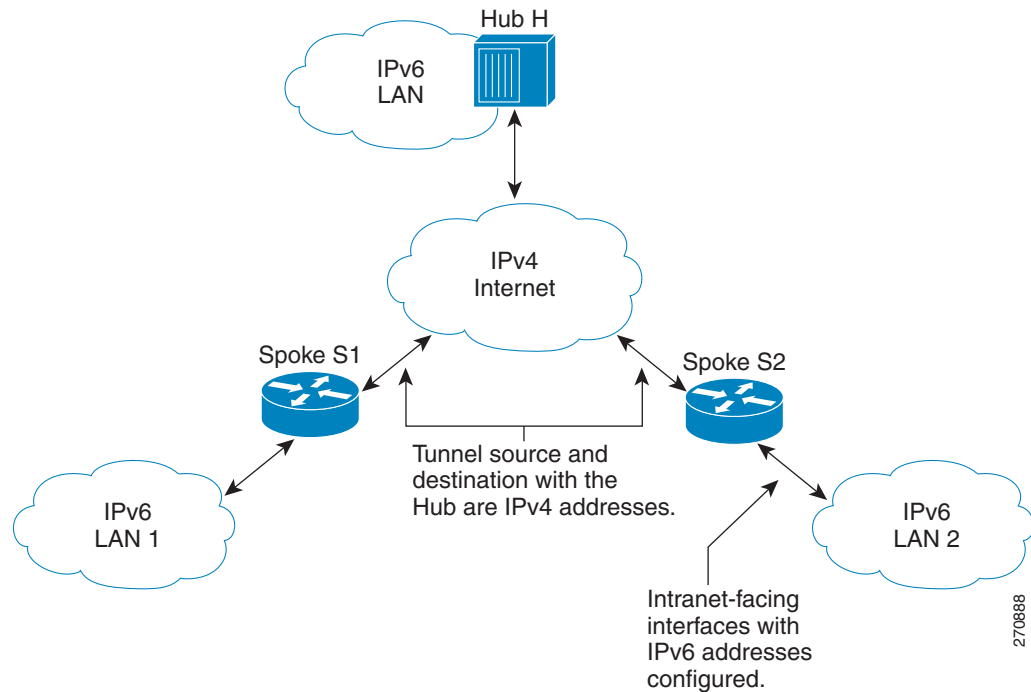
In DMVPN for IPv6, the public network (the Internet) is a pure IPv4 network, and the private network (the intranet) is IPv6 capable. The intranets could be a mix of IPv4 or IPv6 clouds connected to each other using DMVPN technologies, with the underlying carrier being a traditional IPv4 network.

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 Hub H over the Internet using a statically configured tunnel. The address of the tunnel itself is the IPv6 domain, because it is another node on the intranet. The source and destinations address 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 on it. 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, NHRP sends an NHRP traffic indication message to the source 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 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 in turn 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 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.

mGRE Support over IPv6

Multiple sites of a DMVPN are interconnected by IPv6. A single logical mGRE tunnel interface interconnects one VPN site to another. An IPv6 subnet connects a tunnel interface with other tunnel interfaces from various VPN sites. All tunnel interfaces connecting VPN sites act as hosts on the logical IPv6 subnet. This structure is referred to as the tunnel overlay network.

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 8](#) (required)
- [Configuring the NHRP Redirect and Shortcut Features on the Hub, page 10](#) (required)
- [Configuring the Spoke for IPv6 over DMVPN, page 11](#) (required)
- [Verifying DMVPN for IPv6 Configuration, page 14](#) (optional)
- [Monitoring and Maintaining DMVPN for IPv6 Configuration and Operation, page 19](#) (optional)

Configuring an IPsec Profile in DMVPN for IPv6

The IPsec profile shares most 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.

Perform this task to configure an IPsec profile in DMVPN for IPv6.

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 the Internet Security Association Key Management Protocol (ISAKMP) profile 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. **exit**
5. **crypto ipsec profile** *name*
6. **set transform-set** *transform-set-name*
7. **set identity**
8. **set security-association lifetime** {*seconds seconds* | *kilobytes kilobytes*}
9. **set pfs** [*group1* | *group2*]
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto identity <i>name</i> Example: Router(config)# crypto identity router1	Configures the identity of the router with a given list of distinguished names (DNs) in the certificate of the router.
Step 4	exit Example: Router(config-crypto-identity)# exit	Exits crypto identity configuration mode and enters global configuration mode.
Step 5	crypto ipsec profile <i>name</i> Example: Router(config)# crypto ipsec profile example1	Defines the IPsec parameters that are to be used for IPsec encryption between “spoke and hub” and “spoke and spoke” routers. This command places the router in crypto map configuration mode.

	Command or Action	Purpose
Step 6	<pre>set transform-set transform-set-name</pre> <p>Example: Router(config-crypto-map)# set transform-set example-set</p>	Specifies which transform sets can be used with the IPsec profile.
Step 7	<pre>set identity</pre> <p>Example: Router(config-crypto-map)# set identity router1</p>	(Optional) Specifies identity restrictions to be used with the IPsec profile.
Step 8	<pre>set security-association lifetime {seconds seconds kilobytes kilobytes}</pre> <p>Example: Router(config-crypto-map)# set security-association lifetime seconds 1800</p>	(Optional) Overrides the global lifetime value for the IPsec profile.
Step 9	<pre>set pfs [group1 group2]</pre> <p>Example: Router(config-crypto-map)# set pfs group2</p>	(Optional) Specifies that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this IPsec profile.
Step 10	<pre>end</pre> <p>Example: Router(config-crypto-map)# end</p>	Exits crypto map configuration mode and returns to privileged EXEC mode.

Configuring the Hub for IPv6 over DMVPN

Perform this task 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 ip** | **gre [ipv6]** | **gre multipoint [ipv6]** | **ipip** | **decapsulate-any** | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
12. **tunnel protection ipsec profile** *name* [**shared**]
13. **bandwidth** {*kbits* | **inherit** [*kbits*] | **receive** [*kbits*]}
14. **ipv6 nhrp holdtime** *seconds*
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode. <ul style="list-style-type: none"> 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.
Step 4	ipv6 address { <i>ipv6-address/prefix-length</i> <i>prefix-name sub-bits/prefix-length</i> } Example: Router(config-if)# ipv6 address 2001:DB8:1:1::72/64	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	ipv6 address <i>ipv6-address/prefix-length</i> link-local Example: Router(config-if)# ipv6 address fe80::2001 link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. <ul style="list-style-type: none"> A unique IPv6 link-local address (across all DMVPN nodes in a DMVPN network) must be configured.
Step 6	ipv6 mtu <i>bytes</i> Example: Router(config-if)# ipv6 mtu 1400	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.
Step 7	ipv6 nhrp authentication <i>string</i> Example: Router(config-if)# ipv6 nhrp authentication examplexx	Configures the authentication string for an interface using the NHRP. <p>Note The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.</p>
Step 8	ipv6 nhrp map multicast dynamic Example: Router(config-if)# ipv6 nhrp map multicast dynamic	Allows NHRP to automatically add routers to the multicast NHRP mappings.
Step 9	ipv6 nhrp network-id <i>network-id</i> Example: Router(config-if)# ipv6 nhrp network-id 99	Enables the NHRP on an interface.

	Command or Action	Purpose
Step 10	<p>tunnel source {<i>ip-address</i> <i>ipv6-address</i> <i>interface-type interface-number</i>}</p> <p>Example: Router(config-if)# tunnel source ethernet 0</p>	Sets the source address for a tunnel interface.
Step 11	<p>tunnel mode {<i>aurp</i> <i>cayman</i> <i>dmvrp</i> <i>eon</i> gre gre multipoint [<i>ipv6</i>] gre ipv6 ipip [<i>decapsulate-any</i>] ipsec ipv4 iptalk ipv6 ipsec ipv6 mpls nos rbscp}</p> <p>Example: Router(config-if)# tunnel mode gre multipoint</p>	Sets the encapsulation mode to mGRE for the tunnel interface.
Step 12	<p>tunnel protection ipsec profile <i>name</i> [shared]</p> <p>Example: Router(config-if)# tunnel protection ipsec profile example_profile</p>	<p>Associates a tunnel interface with an IPsec profile.</p> <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile; this value must match the name specified in the crypto ipsec profile name command.
Step 13	<p>bandwidth {<i>kbps</i> inherit [<i>kbps</i>] receive [<i>kbps</i>]}</p> <p>Example: Router(config-if)# bandwidth 1200</p>	<p>Sets the current bandwidth value for an interface to higher-level protocols.</p> <ul style="list-style-type: none"> The <i>bandwidth-size</i> argument specifies the bandwidth in kilobits per second. The default value is 9. The recommended bandwidth value is 1000 or greater.
Step 14	<p>ipv6 nhrp holdtime <i>seconds</i></p> <p>Example: Router(config-if)# ipv6 nhrp holdtime 3600</p>	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses.
Step 15	<p>end</p> <p>Example: Router(config-if)# end</p>	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the NHRP Redirect and Shortcut Features on the Hub

Perform this task to configure 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**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel number Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode. <ul style="list-style-type: none">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.
Step 4	ipv6 address { <i>ipv6-address/prefix-length</i> <i>prefix-name sub-bits/prefix-length</i> } Example: Router(config-if)# ipv6 address 2001:DB8:1:1::72/64	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	ipv6 nhrp redirect [<i>timeout seconds</i>] Example: Router(config-if)# ipv6 nhrp redirect	Enables NHRP redirect. Note You must configure the ipv6 nhrp redirect command on a hub.
Step 6	ipv6 nhrp shortcut Example: Router(config-if)# ipv6 nhrp shortcut	Enables NHRP shortcut switching. Note You must configure the ipv6 nhrp shortcut command on a spoke.
Step 7	end Example: Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the Spoke for IPv6 over DMVPN

Perform this task to configure 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 | ipv6-nbma-address*}
 10. **ipv6 nhrp nhs** *ipv6-nhs-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 [ipv6] | gre ipv6 | ipip [decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp*}
- or
14. **tunnel destination** {*host-name | ip-address | ipv6-address*}
 14. **tunnel protection ipsec profile** *name [shared]*
 15. **bandwidth** {*kbits | inherit [kbits] | receive [kbits]*}
 16. **ipv6 nhrp holdtime** *seconds*
 17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode. <ul style="list-style-type: none"> The <i>number</i> 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.
Step 4	ipv6 address { <i>ipv6-address/prefix-length prefix-name sub-bits/prefix-length</i> } Example: Router(config-if) ipv6 address 2001:DB8:1:1::72/64	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

	Command or Action	Purpose
Step 5	<p>ipv6 address <i>ipv6-address/prefix-length</i> link-local</p> <p>Example: Router(config-if)# ipv6 address fe80::2001 link-local</p>	<p>Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.</p> <ul style="list-style-type: none"> A unique IPv6 link-local address (across all DMVPN nodes in a DMVPN network) must be configured.
Step 6	<p>ipv6 mtu <i>bytes</i></p> <p>Example: Router(config-if)# ipv6 mtu 1400</p>	<p>Sets the MTU size of IPv6 packets sent on an interface.</p>
Step 7	<p>ipv6 nhrp authentication <i>string</i></p> <p>Example: Router(config-if)# ipv6 nhrp authentication examplexx</p>	<p>Configures the authentication string for an interface using the NHRP.</p> <p>Note The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.</p>
Step 8	<p>ipv6 nhrp map <i>ipv6-address nbma-address</i></p> <p>Example: Router(config-if)# ipv6 nhrp map 2001:DB8:3333:4::5 10.1.1.1</p>	<p>Statically configures the IPv6-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.</p> <p>Note Only IPv4 NBMA addresses are supported, not ATM or Ethernet addresses.</p>
Step 9	<p>ipv6 nhrp map multicast <i>ipv4-nbma-address</i></p> <p>Example: Router(config-if)# ipv6 nhrp map multicast 10.11.11.99</p>	<p>Maps destination IPv6 addresses to IPv4 NBMA addresses.</p>
Step 10	<p>ipv6 nhrp nhs <i>ipv6-nhs-address</i></p> <p>Example: Router(config-if)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 2001:0DB8::/64</p>	<p>Specifies the address of one or more IPv6 NHRP servers.</p>
Step 11	<p>ipv6 nhrp network-id <i>network-id</i></p> <p>Example: Router(config-if)# ipv6 nhrp network-id 99</p>	<p>Enables the NHRP on an interface.</p>
Step 12	<p>tunnel source {<i>ip-address</i> <i>ipv6-address</i> <i>interface-type interface-number</i>}</p> <p>Example: Router(config-if)# tunnel source ethernet 0</p>	<p>Sets the source address for a tunnel interface.</p>

	Command or Action	Purpose
Step 13	<pre>tunnel mode {aurp cayman dvmrp eon gre gre multipoint [ipv6] gre ipv6 ipip [decapsulate-any] ipsec ipv4 iptalk ipv6 ipsec ipv6 mpls nos rbscp}</pre> <p>OR</p> <pre>tunnel destination {host-name ip-address ipv6-address}</pre> <p>Example: Router(config-if)# tunnel mode gre multipoint</p> <p>OR</p> <pre>Router(config-if)# tunnel destination 10.1.1.1</pre>	<p>Sets the encapsulation mode to mGRE for the tunnel interface.</p> <ul style="list-style-type: none"> Use the tunnel mode command if data traffic can use dynamic spoke-to-spoke traffic. <p>OR</p> <p>Specifies the destination for a tunnel interface.</p> <ul style="list-style-type: none"> Use the tunnel destination command if data traffic can use hub-and-spoke tunnels.
Step 14	<pre>tunnel protection ipsec profile name [shared]</pre> <p>Example: Router(config-if)# tunnel protection ipsec profile example1 </p>	<p>Associates a tunnel interface with an IPsec profile.</p> <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile; this value must match the name specified in the crypto ipsec profile name command.
Step 15	<pre>bandwidth {interzone total session} {default zone zone-name} bandwidth-size</pre> <p>Example: Router(config-if)# bandwidth total 1200</p>	<p>Sets the current bandwidth value for an interface to higher-level protocols.</p> <ul style="list-style-type: none"> The <i>bandwidth-size</i> argument specifies the bandwidth in kilobits per second. The default value is 9. The recommended bandwidth value is 1000 or greater. The bandwidth setting for the spoke need not equal the bandwidth setting for the DMVPN hub. It is usually easier if all of the spokes use the same or similar value.
Step 16	<pre>ipv6 nhrp holdtime seconds</pre> <p>Example: Router(config-if)# ipv6 nhrp holdtime 3600</p>	<p>Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses.</p>
Step 17	<pre>end</pre> <p>Example: Router(config-if)# end</p>	<p>Exits interface configuration mode and returns to privileged EXEC mode.</p>

Verifying DMVPN for IPv6 Configuration

Perform this optional task to display information to verify the DMVPN for IPv6 configuration.

SUMMARY STEPS

- enable**
- show dmvpn [ipv4 [vrf vrf-name] | ipv6 [vrf vrf-name]] [debug-condition | [interface tunnel number | peer {nbma ip-address | network network-mask | tunnel ip-address}]] [static] [detail]]**

3. **show ipv6 nhrp** [**dynamic** *[ipv6-address]* | **incomplete** | **static**] [*address | interface*] [**brief** | **detail**] [**purge**]
4. **show ipv6 nhrp multicast** [*ipv4-address | interface | ipv6-address*]
5. **show ip nhrp multicast** [*nbma-address | interface*]
6. **show ipv6 nhrp summary**
7. **show ipv6 nhrp traffic** [*interface tunnel number*]
8. **show ip nhrp shortcut**
9. **show ip route**
10. **show ipv6 route**
11. **show nhrp debug-condition**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show dmvpn [ipv4 [<i>vrf vrf-name</i>] ipv6 [<i>vrf vrf-name</i>]] [debug-condition [interface tunnel number peer {<i>nbma ip-address</i> network network-mask tunnel ip-address}] [static] [detail]</p> <p>Example: Router# show dmvpn 2001:0db8:1:1::72/64</p>	<p>Displays DMVPN-specific session information.</p>
Step 3	<p>show ipv6 nhrp [dynamic [<i>ipv6-address</i>] incomplete static] [<i>address interface</i>] [brief detail] [purge]</p> <p>Example: Router# show ipv6 nhrp</p>	<p>Displays NHRP mapping information.</p>
Step 4	<p>show ipv6 nhrp multicast [<i>ipv4-address interface ipv6-address</i>]</p> <p>Example: Router# show ipv6 nhrp multicast</p>	<p>Displays NHRP multicast mapping information.</p>
Step 5	<p>show ip nhrp multicast [<i>nbma-address interface</i>]</p> <p>Example: Router# show ip nhrp multicast</p>	<p>Displays NHRP multicast mapping information.</p>
Step 6	<p>show ipv6 nhrp summary</p> <p>Example: Router# show ipv6 nhrp summary</p>	<p>Displays NHRP mapping summary information.</p>

	Command or Action	Purpose
Step 7	show ipv6 nhrp traffic [<i>interface tunnel number</i>] Example: Router# show ipv6 nhrp traffic	Displays NHRP traffic statistics information.
Step 8	show ip nhrp shortcut Example: Router# show ip nhrp shortcut	Displays NHRP shortcut information.
Step 9	show ip route Example: Router# show ip route	Displays the current state of the IPv4 routing table.
Step 10	show ipv6 route Example: Router# show ipv6 route	Displays the current contents of the IPv6 routing table.
Step 11	show nhrp debug-condition Example: Router# show nhrp debug-condition	Displays the NHRP conditional debugging information.

Examples

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 Tunnell 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: Tunnell
IKE SA: local 192.169.2.9/500 remote 192.169.2.10/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 192.169.2.10
IPSEC FLOW: permit 47 host 192.169.2.9 host 192.169.2.10
  Active SAs: 2, origin: crypto map
  Outbound SPI : 0x BBOED02, transform : esp-3des esp-sha-hmac
  Socket State: Open

Interface: Tunnell
IKE SA: local 192.169.2.9/500 remote 192.169.2.11/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 192.169.2.11
IPSEC FLOW: permit 47 host 192.169.2.9 host 192.169.2.11
  Active SAs: 2, origin: crypto map
  Outbound SPI : 0xB79B277B, transform : esp-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 Tunnell 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: Tunnell
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

```

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

    I/F      NBMA address      Flags: dynamic
Tunnel1    192.169.2.10
Tunnel1    192.169.2.11      Flags: dynamic

```

Spoke

```

Router# show ipv6 nhrp multicast

    I/F      NBMA address      Flags: static
Tunnel1    192.169.2.9

```

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
```

Monitoring and Maintaining DMVPN for IPv6 Configuration and Operation

Perform this optional task as needed to display information to monitor and maintain the DMVPN for IPv6 configuration and operation.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	clear dmvpn session [interface tunnel number peer {ipv4-address fqdn-string ipv6-address} vrf vrf-name] [static] Example: Router# clear dmvpn session	Clears DMVPN sessions.
Step 3	clear ipv6 nhrp [ipv6-address counters] Example: Router# clear ipv6 nhrp	Clears all dynamic entries from the NHRP cache.

	Command or Action	Purpose
Step 4	debug dmvpn { all error detail packet } { all <i>debug-type</i> }	Displays debug DMVPN session information.
	Example: Router# debug dmvpn	
Step 5	debug nhrp [cache extension packet rate]	Enables NHRP debugging.
	Example: Router# debug nhrp ipv6	
Step 6	debug nhrp condition [interface tunnel <i>number</i> peer { nbma { <i>ipv4-address</i> <i>fqdn-string</i> <i>ipv6-address</i> } tunnel { <i>ip-address</i> <i>ipv6-address</i> }} vrf <i>vrf-name</i>]	Enables NHRP conditional debugging.
	Example: Router# debug nhrp condition	
Step 7	debug nhrp error	Displays NHRP error-level debugging information.
	Example: Router# debug nhrp ipv6 error	

Examples

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: Attempting to send packet via DEST
      - 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.
Aug  9 13:13:41.486: NHRP: Tunnel NBMA addr 11.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486: src: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32,
      dst: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
```

Configuration Examples for Implementing DMVPN for IPv6

- [Example: Configuring an IPsec Profile, page 21](#)
- [Example: Configuring the Hub for DMVPN, page 21](#)
- [Example: Configuring the NHRP Redirect and Shortcut Features on the Hub, page 21](#)
- [Example: Configuring the Spoke for DMVPN, page 21](#)

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# configure terminal
Router(config)# interface tunnel 5
Router(config-if)# ipv6 address 2001:DB8:1:1::72/64
Router(config-if)# ipv6 address fe80::2001 link-local
Router(config-if)# ipv6 mtu 1400
Router(config-if)# ipv6 nhrp authentication examplexx
Router(config-if)# ipv6 nhrp map multicast dynamic
Router(config-if)# ipv6 nhrp network-id 99
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel protection ipsec profile example_profile
Router(config-if)# bandwidth 1200
Router(config-if)# ipv6 nhrp holdtime 3600
```

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# configure terminal
Router (config)# crypto ikev2 keyring DMVPN
Router (config)# peer DMVPN
Router (config)# address 0.0.0.0 0.0.0.0
Router (config)# pre-shared-key cisco123
Router (config)# peer DMVPNv6
Router (config)# address ::/0
Router (config)# pre-shared-key cisco123v6
Router (config)# crypto ikev2 profile DMVPN
Router (config)# match identity remote address 0.0.0.0
Router (config)# match identity remote address ::/0
Router (config)# authentication local pre-share
Router (config)# authentication remote pre-share
Router (config)# keyring DMVPN
Router (config)# dpd 30 5 on-demand
Router (config)# crypto ipsec transform-set DMVPN esp-aes esp-sha-hmac
Router (config)# mode transport
Router (config)# crypto ipsec profile DMVPN
Router (config)# set transform-set DMVPN
Router (config)# set ikev2-profile DMVPN
Router(config)# interface tunnel 5
Router(config-if)# bandwidth 1000
```

```

Router(config-if)# ip address 10.0.0.11 255.255.255.0
Router(config-if)# ip mtu 1400
Router(config-if)# ip nhrp authentication test
Router(config-if)# ip nhrp network-id 100000
Router(config-if)# ip nhrp nhs 10.0.0.1 nbma 2001:DB8:0:FFFF:1::1 multicast
Router(config-if)# vip nhrp shortcut
Router(config-if)# delay 1000
Router(config-if)# ipv6 address 2001:DB8:0:100::B/64
Router(config-if)# ipv6 mtu 1400
Router(config-if)# ipv6 nd ra mtu suppress
Router(config-if)# no ipv6 redirects
Router(config-if)# ipv6 eigrp 1
Router(config-if)# ipv6 nhrp authentication testv6
Router(config-if)# ipv6 nhrp network-id 100006
Router(config-if)# ipv6 nhrp nhs 2001:DB8:0:100::1 nbma 2001:DB8:0:FFFF:1::1 multicast
Router(config-if)# ipv6 nhrp shortcut
Router(config-if)# tunnel source Ethernet0/0
Router(config-if)# tunnel mode gre multipoint ipv6
Router(config-if)# tunnel key 100000
Router(config-if)# end

```

.
.

Additional References

Related Documents

Related Topic	Document Title
IPv6 supported feature list	“Start Here: Cisco IOS Software Release Specifics for IPv6 Features” module of the <i>Cisco IOS IPv6 Configuration Guide</i>
IPv6 IPsec	“Implementing IPsec in IPv6 Security” module of the <i>Cisco IOS IPv6 Configuration Guide</i>
IPv6 basic connectivity	“Implementing IPv6 Addressing and Basic Connectivity” module of the <i>Cisco IOS IPv6 Configuration Guide</i>
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IPv6 Command Reference
DMVPN implementation for IPv4	“Dynamic Multipoint VPN (DMVPN)” module of the <i>Cisco IOS Security Configuration Guide</i>
DMVPN commands for IPv4	Cisco IOS Security Command Reference
NHRP for IPv4	“Configuring NHRP” module of the <i>Cisco IOS IP Addressing Services Configuration Guide</i>
NHRP commands for IPv4	The “NHRP Commands” section of the <i>Cisco IOS IP Addressing Services Command Reference</i>

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
Cisco NHRP Extension MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2332	<i>NBMA Next Hop Resolution Protocol (NHRP)</i>
RFC 2677	<i>Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)</i>

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

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 1 Feature Information for Implementing DMVPN for IPv6

Feature Name	Releases	Feature Information
DMVPN for IPv6	12.4(20)T	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.
mGRE over IPV6	15.2(1)T	The following section provides information about this feature: <ul style="list-style-type: none"> mGRE Support over IPv6, page 5
IPv6 transport for DMVPN	15.2(1)T	The IPv6 transport for DMVPN feature builds IPv6 WAN-side capability into NHRP tunnels and the underlying IPsec encryption, and enables IPv6 to transport payloads on the Internet. The IPv6 transport for DMVPN feature is enabled by default.

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.