IPv6 over DMVPN

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.

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.

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.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

- Prerequisites for IPv6 over DMVPN, on page 1
- Information About IPv6 over DMVPN, on page 2
- How to Configure IPv6 over DMVPN, on page 4
- Configuration Examples for IPv6 over DMVPN, on page 18
- Additional References, on page 22
- Feature Information for IPv6 over DMVPN, on page 23

Prerequisites for IPv6 over DMVPN

- 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).

Information About IPv6 over DMVPN

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.

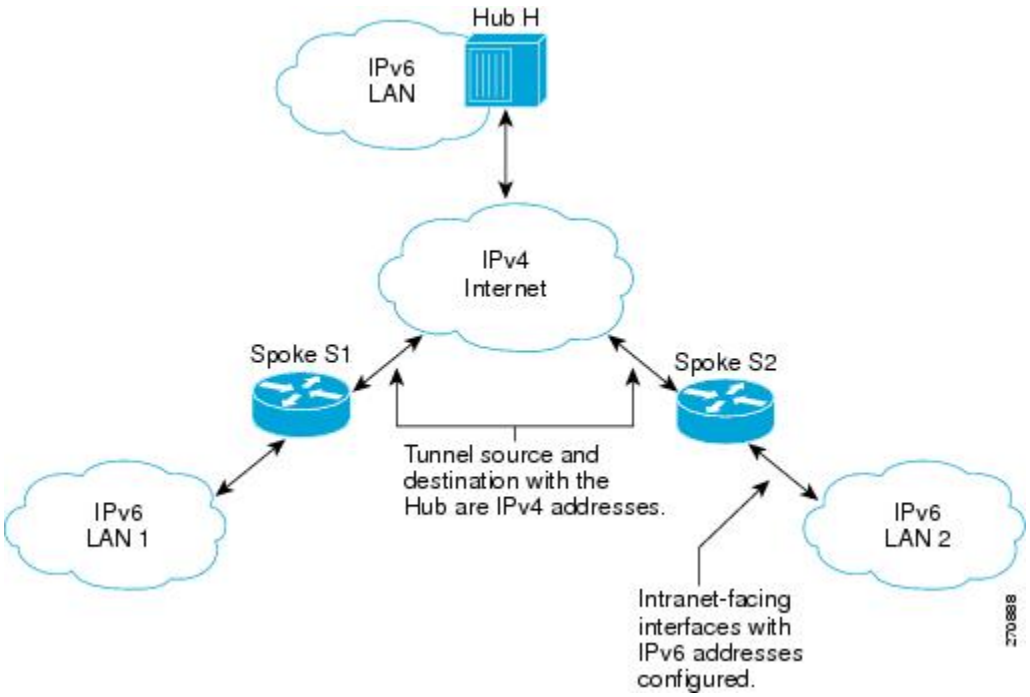
In DMVPN for IPv6, the public network (the Internet) is a pure IPv4 network, and the private network (the intranet) is IPv6 capable. The intranets could be a mix of IPv4 or IPv6 clouds connected to each other using DMVPN technologies, with the underlying carrier being a traditional IPv4 network.

NHRP Routing

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

In the figure below, 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 device, 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 device are using the same tunnel source, then the tunnel source address can be embedded into an IPv6 address.
  - If the device 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 device 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.

Note From Cisco IOS XE 17.9.1a, a new attribute **scope** is introduced for the **ipv6 nhrp nhs** command. This attribute defines the scope of IPv6 address that is used while registering with the NHS and allows you to control the scope of creating cache entries between peers.

- If scope is set to **global**, then the spoke registers only with the global unicast IPv6 address during the registration (link-local IPv6 address is not used).
- (Optional) Scope can be defined for static and dynamic NHS.

How to Configure IPv6 over DMVPN

Configuring an IPsec Profile in DMVPN for IPv6

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

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.

Before you begin

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.

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** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**]
10. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto identity** *name* **Example:** `Device(config)# crypto identity device1`	Configures the identity of the device with a given list of distinguished names (DNs) in the certificate of the device.
Step 4	**exit** **Example:** `Device(config-crypto-identity)# exit`	Exits crypto identity configuration mode and enters global configuration mode.
Step 5	**crypto ipsec profile** *name* **Example:** `Device(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.

	Command or Action	Purpose
		This command places the device in crypto map configuration mode.
Step 6	**set transform-set** *transform-set-name* **Example:** `Device(config-crypto-map)# set transform-set example-set`	Specifies which transform sets can be used with the IPsec profile.
Step 7	**set identity** **Example:** `Device(config-crypto-map)# set identity router1`	(Optional) Specifies identity restrictions to be used with the IPsec profile.
Step 8	**set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes* **Example:** `Device(config-crypto-map)# set security-association lifetime seconds 1800`	(Optional) Overrides the global lifetime value for the IPsec profile.
Step 9	**set pfs** [**group1** | **group14** | **group15** | **group16** | **group19** | **group2** | **group20** | **group24** | **group5**] **Example:** `Device(config-crypto-map)# set pfs group14`	(Optional) Specifies that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this IPsec profile. If this command is not specified, the default Diffie-Hellman (DH) group, **group1** will be enabled. • **1**—768-bit DH (No longer recommended.) • **2**—1024-bit DH (No longer recommended) • **5**—1536-bit DH (No longer recommended) • **14**—Specifies the 2048-bit DH group. • **15**—Specifies the 3072-bit DH group. • **16**—Specifies the 4096-bit DH group. • **19**—Specifies the 256-bit elliptic curve DH (ECDH) group. • **20**—Specifies the 384-bit ECDH group. • **24**—Specifies the 2048-bit DH/DSA group.
Step 10	end **Example:** `Device(config-crypto-map)# end`	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 device 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**[**ipv6**] | **gre ipv6** | **ipip decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6**| **ipsec ipv6** | **mpls** | **nos** | **rbscp**
12. Do one of the following:
    - **tunnel protection ipsec profile** *name* [**shared**]
    - **tunnel protection psk** *key*
13. **bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]}
14. **ipv6 nhrp holdtime** *seconds*
15. **ipv6 nhrp max-send** *pkt-count* **every** *seconds*
16. **ip nhrp registration** [**timeout** *seconds* | **no-unique**]
17. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 5`	Configures a tunnel interface and enters interface configuration mode. • The number argument specifies the number of the tunnel interfaces that you want to create or configure.

	Command or Action	Purpose
		There is no limit on the number of tunnel interfaces you can create.
Step 4	**ipv6 address** {*ipv6-address* / *prefix-length* | *prefix-name sub-bits* / *prefix-length* **Example:** `Device(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** *ipv6-address* / *prefix-length* **link-local** **Example:** `Device(config-if)# ipv6 address fe80::2001 link-local`	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. • A unique IPv6 link-local address (across all DMVPN nodes in a DMVPN network) must be configured.
Step 6	**ipv6 mtu** *bytes* **Example:** `Device(config-if)# ipv6 mtu 1400`	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.
Step 7	**ipv6 nhrp authentication** *string* **Example:** `Device(config-if)# ipv6 nhrp authentication examplexx`	Configures the authentication string for an interface using the NHRP. **Note** The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 8	**ipv6 nhrp map multicast dynamic** **Example:** `Device(config-if)# ipv6 nhrp map multicast dynamic`	Allows NHRP to automatically add routers to the multicast NHRP mappings. **Note** Effective with Cisco IOS XE Denali 16.3 **ipv6 nhrp map multicast dynamic** is enabled by default.
Step 9	**ipv6 nhrp network-id** *network-id* **Example:** `Device(config-if)# ipv6 nhrp network-id 99`	Enables the NHRP on an interface. Effective with Cisco IOS XE Denali 16.3 **ipv6 nhrp network-id** is enabled by default.
Step 10	**tunnel source** *ip-address* | *ipv6-address* | *interface-type interface-number* **Example:** `Device(config-if)# tunnel source ethernet 0`	Sets the source address for a tunnel interface.
Step 11	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gre multipoint**[**ipv6**] | **gre ipv6** | **ipip decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6**| **ipsec ipv6** | **mpls** | **nos** | **rbscp**	Sets the encapsulation mode to mGRE for the tunnel interface.

	Command or Action	Purpose
	Example: `Device(config-if)# tunnel mode gre multipoint`	

Step 12	Do one of the following:
	• **tunnel protection ipsec profile** *name* [**shared**]
	• **tunnel protection psk** *key*
	Example:
	`Router(config-if)# tunnel protection ipsec profile vpnprof`
	Example:
	`Router(config-if)# tunnel protection psk test1`
		Associates a tunnel interface with an IPsec profile.
		• The *name* argument specifies the name of the IPsec profile; this value must match the *name* specified in the **crypto ipsec profile** *name*command.
		or
		Simplifies the tunnel protection configuration for pre-shared key (PSK) by creating a default IPsec profile.

Step 13	**bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]} **Example:** `Device(config-if)# bandwidth 1200`	Sets the current bandwidth value for an interface to higher-level protocols. • The *bandwidth-size* argument specifies the bandwidth in kilobits per second. The default value is 9. The recommended bandwidth value is 1000 or greater.
Step 14	**ipv6 nhrp holdtime** *seconds* **Example:** `Device(config-if)# ipv6 nhrp holdtime 600`	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses. The default time is 600 seconds.
Step 15	**ipv6 nhrp max-send** *pkt-count* **every** *seconds* **Example:** `Device(config-if)# ipv6 nhrp max-send 10000 every 10`	Changes the maximum frequency at which NHRP packets can be sent. Number of packets that can be sent in the range from 1 to 65535. Default is 100 packets.
Step 16	**ip nhrp registration** [**timeout** *seconds* | **no-unique**] **Example:** `Device(config-if)# ip nhrp registration no-unique`	Enables the client to not set the unique flag in the NHRP request and reply packets. The default is no-unique.
Step 17	end **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

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. Do one of the following:
   - **ipv6 nhrp redirect** [**timeout** *seconds*]
   - **ipv6 nhrp redirect** [**interest** *acl*]
6. **ipv6 nhrp shortcut**
7. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel number** **Example:** `Device(config)# interface tunnel 5`	Configures a tunnel interface and enters interface configuration mode. • 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** {*ipv6-address* / *prefix-length* | *prefix-name sub-bits* / *prefix-length* **Example:** `Device(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	Do one of the following: • **ipv6 nhrp redirect** [**timeout** *seconds*] • **ipv6 nhrp redirect** [**interest** *acl*] **Example:** `Device(config-if)# ipv6 nhrp redirect`	Enables NHRP redirect. or Enables the user to specify an ACL. **Note** You must configure the **ipv6 nhrp redirect** command on a hub.

	Command or Action	Purpose
	Example: `Device(config-if)# ipv6 nhrp redirect interest`	
Step 6	**ipv6 nhrp shortcut** **Example:** `Device(config-if)# ipv6 nhrp shortcut`	Enables NHRP shortcut switching. • You must configure the **ipv6 nhrp shortcut** command on a spoke. **Note** Effective with Cisco IOS XE Denali 16.3 **ipv6 nhrp shortcut** is enabled by default.
Step 7	end **Example:** `Device(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*
10. **ipv6 nhrp nhs** *ipv6- nhs-address* **scope** {*global*}
11. **ipv6 nhrp network-id** *network-id*
12. **tunnel source** *ip-address* | *ipv6-address* | *interface-type interface-number*
13. Do one of the following:
    - **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gre multipoint** [**ipv6**] | **gre ipv6** | **ipip decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6**| **ipsec ipv6** | **mpls** | **nos** | **rbscp**
    - **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
14. Do one of the following:
    - **tunnel protection ipsec profile** *name* [**shared**]
    - **tunnel protection psk** *key*
15. **bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *bandwidth-size*
16. **ipv6 nhrp holdtime** *seconds*

17. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 5`	Configures a tunnel interface and enters interface configuration mode. • 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** {*ipv6-address* / *prefix-length* | *prefix-name sub-bits* / *prefix-length* **Example:** `Device(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** *ipv6-address* / *prefix-length* **link-local** **Example:** `Device(config-if)# ipv6 address fe80::2001 link-local`	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. • A unique IPv6 link-local address (across all DMVPN nodes in a DMVPN network) must be configured.
Step 6	**ipv6 mtu** *bytes* **Example:** `Device(config-if)# ipv6 mtu 1400`	Sets the MTU size of IPv6 packets sent on an interface.
Step 7	**ipv6 nhrp authentication** *string* **Example:** `Device(config-if)# ipv6 nhrp authentication examplexx`	Configures the authentication string for an interface using the NHRP. **Note** The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 8	**ipv6 nhrp map** *ipv6-address nbma-address* **Example:**	Statically configures the IPv6-to-NBMA address mapping of IPv6 destinations connected to an NBMA network.

	Command or Action	Purpose
	`Device(config-if)# ipv6 nhrp map 2001:DB8:3333:4::5 10.1.1.1`	**Note** Only IPv4 NBMA addresses are supported, not ATM or Ethernet addresses.
Step 9	**ipv6 nhrp map multicast** *ipv4-nbma-address* **Example:** `Device(config-if)# ipv6 nhrp map multicast 10.11.11.99`	Maps destination IPv6 addresses to IPv4 NBMA addresses.
Step 10	**ipv6 nhrp nhs** *ipv6- nhs-address* **scope** {*global*} **Example:** `Device(config-if)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 2001:0DB8::/64 scope global`	Specifies the address of one or more IPv6 NHRP servers.
Step 11	**ipv6 nhrp network-id** *network-id* **Example:** `Device(config-if)# ipv6 nhrp network-id 99`	Enables the NHRP on an interface. **Note** Effective with Cisco IOS XE Denali 16.3 **ipv6 nhrp network-id** is enabled by default.
Step 12	**tunnel source** *ip-address* | *ipv6-address* | *interface-type interface-number* **Example:** `Device(config-if)# tunnel source ethernet 0`	Sets the source address for a tunnel interface.

Step 13	Do one of the following:
	• **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gre multipoint** [**ipv6**] | **gre ipv6** | **ipip decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6**| **ipsec ipv6** | **mpls** | **nos** | **rbscp**
	• **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
	Example:
	`Device(config-if)# tunnel mode gre multipoint`
	Example:
	`Device(config-if)# tunnel destination 10.1.1.1`
		Sets the encapsulation mode to mGRE for the tunnel interface.
		• Use the **tunnel mode** command if data traffic can use dynamic spoke-to-spoke traffic.
		or
		Specifies the destination for a tunnel interface.
		• Use the **tunnel destination** command if data traffic can use hub-and-spoke tunnels.

Step 14	Do one of the following: • **tunnel protection ipsec profile** *name* [**shared**] • **tunnel protection psk** *key* **Example:** `Router(config-if)# tunnel protection ipsec profile vpnprof`	Associates a tunnel interface with an IPsec profile. • The *name* argument specifies the name of the IPsec profile; this value must match the *name* specified in the **crypto ipsec profile** *name*command. or

	Command or Action	Purpose
	Example: `Router(config-if)# tunnel protection psk test1`	Simplifies the tunnel protection configuration for pre-shared key (PSK) by creating a default IPsec profile.
Step 15	**bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *bandwidth-size* **Example:** `Device(config-if)# bandwidth total 1200`	Sets the current bandwidth value for an interface to higher-level protocols. • The *bandwidth-size* 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	**ipv6 nhrp holdtime** *seconds* **Example:** `Device(config-if)# ipv6 nhrp holdtime 3600`	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses.
Step 17	end **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying DMVPN for IPv6 Configuration

SUMMARY STEPS

1. **enable**
2. **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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**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**]] **Example:** `Device# show dmvpn 2001:0db8:1:1::72/64`	Displays DMVPN-specific session information.
Step 3	**show ipv6 nhrp** [**dynamic** [*ipv6-address*] | **incomplete** | **static**] [*address* | *interface*] [**brief** | **detail**] [**purge**] **Example:** `Device# show ipv6 nhrp`	Displays NHRP mapping information.
Step 4	**show ipv6 nhrp multicast** [*ipv4-address* | *interface* | *ipv6-address*] **Example:** `Device# show ipv6 nhrp multicast`	Displays NHRP multicast mapping information.
Step 5	**show ip nhrp multicast** [*nbma-address* | *interface*] **Example:** `Device# show ip nhrp multicast`	Displays NHRP multicast mapping information.
Step 6	**show ipv6 nhrp summary** **Example:** `Device# show ipv6 nhrp summary`	Displays NHRP mapping summary information.
Step 7	**show ipv6 nhrp traffic** [*interface***tunnel** *number* **Example:** `Device# show ipv6 nhrp traffic`	Displays NHRP traffic statistics information.
Step 8	**show ip nhrp shortcut** **Example:** `Device# show ip nhrp shortcut`	Displays NHRP shortcut information.

	Command or Action	Purpose
Step 9	**show ip route** **Example:** `Device# show ip route`	Displays the current state of the IPv4 routing table.
Step 10	**show ipv6 route** **Example:** `Device# show ipv6 route`	Displays the current contents of the IPv6 routing table.
Step 11	**show nhrp debug-condition** **Example:** `Device# show nhrp debug-condition`	Displays the NHRP conditional debugging information.

Monitoring and Maintaining 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:** `Device> enable`	Enables privileged EXEC mode. • 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:** `Device# clear dmvpn session`	Clears DMVPN sessions.

	Command or Action	Purpose
Step 3	**clear ipv6 nhrp** [*ipv6-address* | **counters** **Example:** `Device# clear ipv6 nhrp`	Clears all dynamic entries from the NHRP cache.
Step 4	**debug dmvpn** {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*} **Example:** `Device# debug dmvpn`	Displays debug DMVPN session information.
Step 5	**debug nhrp** [**cache** | **extension** | **packet** | **rate**] **Example:** `Device# debug nhrp ipv6`	Enables NHRP debugging.
Step 6	**debug nhrp condition** [**interface tunnel** *number* | **peer** {**nbma** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*] **Example:** `Device# debug nhrp condition`	Enables NHRP conditional debugging.
Step 7	**debug nhrp error** **Example:** `Device# debug nhrp ipv6 error`	Displays NHRP error-level debugging information.

Examples

Sample Output for the debug nhrp Command

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

```
Device# 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 IPv6 over DMVPN

Example: Configuring an IPsec Profile

```
Device(config)# crypto identity router1

Device(config)# crypto ipsec profile example1
Device(config-crypto-map)# set transform-set example-set
Device(config-crypto-map)# set identity router1

Device(config-crypto-map)# set security-association lifetime seconds 1800

Device(config-crypto-map)# set pfs group14
```

Example: Configuring the Hub for DMVPN

```
Device# configure terminal
Device(config)# interface tunnel 5

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

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

```
Device# 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 : 0x BB0ED02, transform : esp-aes 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 : 0xB79B277B, transform : esp-aes esp-sha-hmac
    Socket State: Open
```

Example: Configuring the Spoke for DMVPN

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

Device(config-if)# bandwidth 1000
Device(config-if)# ip address 10.0.0.11 255.255.255.0
Device(config-if)# ip mtu 1400
```

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

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

```
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-aes esp-sha-hmac
    Socket State: Open
```

Example: Configuring the Spoke with Global Unicast

```
SPOKE1(config-if)# show run int tun0

Building configuration...



Current configuration : 671 bytes

!

interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.254 172.16.1.1
 ip nhrp map multicast 172.16.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.254
 delay 100
 ipv6 address 2001::1/64
 ipv6 enable
 ipv6 mtu 1400
 ipv6 nhrp authentication test
 ipv6 nhrp map multicast 172.16.1.1
 ipv6 nhrp map 2001::2/64 172.16.1.1
 ipv6 nhrp network-id 20000
 ipv6 nhrp holdtime 300
 ipv6 nhrp nhs 2001::2 global         <<<<<<<<<<<<<<<<
 ipv6 eigrp 11
 bfd template sample
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile iprof
end
```

Example: Configuring the NHRP Redirect and Shortcut Features on the Hub

```
Device(config)# interface tunnel 5
Device(config-if)# ipv6 address 2001:DB8:1:1::72/64

Device(config-if)# ipv6 nhrp redirect

Device(config-if)# ipv6 nhrp shortcut
```

Example: Configuring NHRP on the Hub and Spoke

Hub

```
Device# 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

```
Device# 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
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Dynamic Multipoint VPN	*Dynamic Multipoint VPN Configuration Guide*
IPv6 commands	*IPv6 Command Reference*
Cisco IOS IPv6 features	IPv6 Feature Mapping

Related Topic	Document Title
Recommended cryptographic algorithms	Next Generation Encryption

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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 IPv6 over DMVPN

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.

Table 1: Feature Information for IPv6 over DMVPN

Feature Name	Releases	Feature Information
IPv6 over DMVPN		The DMVPN feature 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. The following commands were introduced or modified: **clear dmvpn session**, **clear ipv6 nhrp**, **crypto ipsec profile**, **debug dmvpn**, **debug dmvpn condition**, **debug nhrp condition**, **debug nhrp error**, **ipv6 nhrp authentication**, **ipv6 nhrp holdtime**, **ipv6 nhrp interest**, **ipv6 nhrp map**, **ipv6 nhrp map multicast**, **ipv6 nhrp map multicast dynamic**, **ipv6 nhrp max-send**, **ipv6 nhrp network-id**, **ipv6 nhrp nhs**, **ipv6 nhrp record**, **ipv6 nhrp redirect**, **ipv6 nhrp registration**, **ipv6 nhrp responder**, **ipv6 nhrp server-only**, **ipv6 nhrp shortcut**, **ipv6 nhrp trigger-svc**, **ipv6 nhrp use**, **set pfs**, **set security-association lifetime**, **set transform-set**, **show dmvpn**, **show ipv6 nhrp**, **show ipv6 nhrp multicast**, **show ipv6 nhrp nhs**, **show ipv6 nhrp summary**, **show ipv6 nhrp traffic**.
IPv6 Transport for DMVPN		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.