DMVPN Tunnel Health Monitoring and Recovery

The Dynamic Multipoint VPN Tunnel Health Monitoring and Recovery feature enhances the ability of the system to monitor and report Dynamic Multipoint VPN (DMVPN) events. It includes support for Simple Network Management Protocol (SNMP) Next Hop Resolution Protocol (NHRP) notifications for critical DMVPN events and support for DMVPN syslog messages. It also enables the system to control the state of the tunnel interface based on the health of the DMVPN tunnels.

Prerequisites for DMVPN Tunnel Health Monitoring and Recovery

SNMP NHRP notifications

- SNMP is enabled in the system.
- Generic SNMP configurations for Get and Set operations and for notifications are implemented in the system.
- All relevant NHRP traps are enabled.

Restrictions for DMVPN Tunnel Health Monitoring and Recovery

MIB SNMP

- SNMP SET UNDO is not supported.

- The MIB Persistence feature that enables the MIB-SNMP data to persist across reloads is not supported. However, a virtual persistence for the MIB notification control object happens, because that information is also captured via the configuration command line interface (CLI).
- Notifications and syslogs are not virtual routing and forwarding (VRF)-aware.
- The Rate Limit Exceeded notification does not differentiate between the IPv4 or IPv6 protocol type.

Interface State Control

- Interface state control can be configured on leaf spoke nodes only.
- Interface state control supports IPv4 only.

Information About DMVPN Tunnel Health Monitoring and Recovery

NHRP Extension MIB

The NHRP Extension MIB module comprises objects that maintain redirect-related statistics for both clients and servers, and for the following SNMP notifications for critical DMVPN events:

- A spoke perceives that a hub has gone down. This can occur even if the spoke was not previously registered with the hub.
- A spoke successfully registers with a hub.
- A hub perceives that a spoke has gone down.
- A hub perceives that a spoke has come up.
- A spoke or hub perceives that another NHRP peer, not related by an NHRP registration, has gone down. For example, a spoke-spoke tunnel goes down.
- A spoke or hub perceives that another NHRP peer, not related by an NHRP registration, has come up. For example, a spoke-spoke tunnel comes up.
- The rate limit set for NHRP packets on the interface is exceeded.

The agent implementation of the MIB provides a means to enable and disable specific traps, from either the network management system or the CLI.

DMVPN Syslog Messages

The DMVPN syslog feature provides syslog messages for the following events:

- All next-hop state change events. For example, when the system declares that a Next Hop Server (NHS), Next Hop Client (NHC), or a Next Hop Peer (NHP) is up or down. The severity level for these messages is set to critical.

- NHRP resolution events. For example, when a spoke sends a resolution to a remote spoke, or when an NHRP resolution times out without receiving a response. The severity level for these messages is set to informational.
- DMVPN cryptography events. For example, when a DMVPN socket entry changes from open to closed, or from closed to open. The severity level for these messages is set to notification.
- NHRP error notifications. For example, when an NHRP registration or resolution event fails, when a system check event fails, or when an NHRP encapsulation error occurs, an NHRP error notification is displayed. The severity level for these messages is set to errors.

  A sample NHRP error message is given below:

  Received Error Indication from 209.165.200.226, code: administratively prohibited(4), (trigger src: 209.165.200.228 (nbma: 209.165.200.230) dst: 209.165.202.140), offset: 0, data: 00 01 08 00 00 00 00 00 00 FE 00 68 F4 03 00 34

  The error message includes the IP address of the node where the error originates, the source nonbroadcast multiaccess (NBMA), and the destination address.
- DMVPN error notifications. For example, when the NET_ID value is not configured, or when an NHRP multicast replication failure occurs. The severity level is set to notification for the unconfigured NET_ID value message, and set to errors if an NHRP multicast replication failure occurs.
- The rate limit set for NHRP packets on the interface is exceeded. This event occurs when the NHRP packets handled by the NHRP process exceeds the rate limit set on the interface. The severity level for this message is set to warning.

Note From Cisco IOS XE 17.8.1, the **logging dmvpn rate-limit** command is enabled by default, with a rate-limit of 600 messages per minute. To disable, use the **no** form of the command. For more details, see section Troubleshooting Dynamic Multipoint VPN.

Interface State Control

The Interface State Control feature allows NHRP to control the state of the interface based on whether the tunnels on the interface are live. If NHRP detects that all NHSs configured on the interface are in the down state, NHRP can change the interface state to down. However, if NHRP detects that any one of the NHSs configured on the interface is up, then it can change the state of the interface to up.

When the NHRP changes the interface state, other Cisco services can react to the state change, for example:

- If the interface state changes, the generic routing and encapsulation (GRE) interface generates IF-MIB notifications (traps) that report a LinkUp or LinkDown message. The system uses these traps to monitor the connectivity to the DMVPN cloud.
- If the interface state changes to down, the Cisco IOS backup interface feature can be initiated to allow the system to use another interface to provide an alternative path to the failed primary path.
- If the interface state changes to down, the system generates an update that is sent to all dynamic routing protocols. The Interface State Control feature a failover mechanism for dynamic routing when the multipoint GRE (mGRE) interface is down.

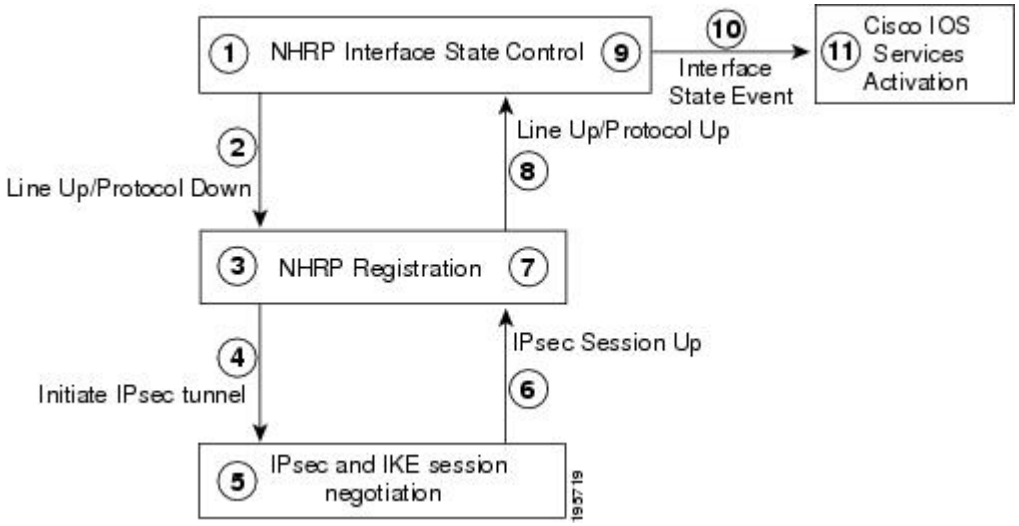
- If the interface state changes to down, the system clears any static routes that use the mGRE interface as the next hop. The Interface State Control feature provides a failover mechanism for routing when the mGRE interface is down.

The interface state control feature works on both point-to-point and mGRE interfaces.

Interface State Control Configuration Workflow

The diagram below illustrates how the system behaves when the Interface State Control feature is initialized.

Figure 1: Interface State Control Configuration Initialization Workflow



The Interface State Control initialization works as follows:

1. The Interface State Control feature is enabled on the GRE interface with NHRP configured.
2. The system reevaluates the protocol state and changes the state to line up and protocol down if none of the configured NHSs is responding.
3. The line up state change initiates the NHRP registration process.
4. The NHRP registration process initiates the IPsec tunnel.
5. The IPsec tunnel initiation starts the IPsec and IKE tunnel negotiation process.
6. On successful completion of the tunnel negotiation process, the system sends an IPsec Session Up message.
7. The NHRP registration process receives the IPsec Session Up message.
8. The NHRP registration process reports the line up and protocol up state to the GRE interface.
9. The GRE interface state changes to line up and protocol up.
10. The system reports the GRE interface state change to Cisco software.
11. The state change triggers Cisco services, such as interface event notifications, syslog events, DHCP renew, IP route refresh, and SNMP traps.

How to Configure DMVPN Tunnel Health Monitoring and Recovery

The DMVPN Tunnel Health Monitoring and Recovery feature allows you to configure SNMP NHRP notifications and interface states.

Configuring Interfaces to Generate SNMP NHRP Notifications

You can configure an interface so that SNMP NHRP traps are generated for NHRP events. In addition, you can configure the system to send the traps to particular trap receivers. To configure SNMP NHRP notifications on an interface, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* **rw**
4. **snmp-server enable traps nhrp nhs**
5. **snmp-server enable traps nhrp nhc**
6. **snmp-server enable traps nhrp nhp**
7. **snmp-server enable traps nhrp quota-exceeded**
8. **snmp-server host** *ip-address* **version** *snmpversion community-string*
9. **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	**snmp-server community** *string* **rw** **Example:** `Device(config)# snmp-server community public rw`	Configures the community access string to permit access to the SNMP.
Step 4	**snmp-server enable traps nhrp nhs** **Example:**	Enables NHRP NHS notifications.

	Command or Action	Purpose
	`Device(config)# snmp-server enable traps nhrp nhc`	
Step 5	**snmp-server enable traps nhrp nhc** **Example:** `Device(config)# snmp-server enable traps nhrp nhc`	Enables NHRP NHC notifications.
Step 6	**snmp-server enable traps nhrp nhp** **Example:** `Device(config)# snmp-server enable traps nhrp nhc`	Enables NHRP NHP notifications.
Step 7	**snmp-server enable traps nhrp quota-exceeded** **Example:** `Device(config)# snmp-server enable traps nhrp quota-exceeded`	Enables notifications for when the rate limit set on the NHRP packets is exceeded on the interface.
Step 8	**snmp-server host** *ip-address* **version** *snmpversion community-string* **Example:** `Device(config)# snmp-server host 192.40.3.130 version 2c public`	Specifies the recipient of an SNMP notification operation. • By default, SNMP notifications are sent as traps. • All NHRP traps are sent to the notification receiver with the IP address 192.40.3.130 using the community string public.
Step 9	**end** **Example:** `Device(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug snmp mib nhrp** command to troubleshoot SNMP NHRP notifications.

Configuring Interface State Control on an Interface

The Interface State Control feature enables the system to control the state of an interface based on whether the DMVPN tunnels connected to the interface are live or not. To configure interface state control on an interface, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **if-state nhrp**
5. **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** *type number* **Example:** `Device(config)# interface tunnel 1`	Configures an interface type and enters interface configuration mode.
Step 4	**if-state nhrp** **Example:** `Device(config-if)# if-state nhrp`	Enables NHRP to control the state of the tunnel interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuration Examples for DMVPN Tunnel Health Monitoring and Recovery

Example: Configuring SNMP NHRP Notifications

The following example shows how to configure SNMP NHRP notifications on a hub or spoke:

```
Device(config)# snmp-server community public rw
Device(config)# snmp-server enable traps nhrp nhs
Device(config)# snmp-server enable traps nhrp nhc
Device(config)# snmp-server enable traps nhrp nhp
Device(config)# snmp-server enable traps nhrp quota-exceeded
Device(config)# snmp-server host 209.165.200.226 version 2c public
```

Example: Configuring Interface State Control

The following example shows how to configure the Interface State Control feature for a spoke:

```
interface Tunnel 1
 ip address 209.165.200.228 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map 209.165.201.2 209.165.201.10
 ip nhrp map 209.165.201.3 209.165.201.11
 ip nhrp map multicast 209.165.201.10
 ip nhrp map multicast 209.165.201.11
 ip nhrp network-id 1
 ip nhrp holdtime 90
 ip nhrp nhs 209.165.201.3
 ip nhrp nhs 209.165.201.2
 ip nhrp shortcut
 if-state nhrp
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 !
end
```

Additional References for DMVPN Tunnel Health Monitoring and Recovery

Related Documents

Related Topic	Document Title
Dynamic Multipoint VPN information	"Dynamic Multipoint VPN (DMVPN)" module in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
IKE configuration tasks such as defining an IKE policy	"Configuring Internet Key Exchange for IPsec VPNs" module in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
IPsec configuration tasks	"Configuring Security for VPNs with IPsec" module in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
System messages	*System Messages Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2332	*NBMA Next Hop Resolution Protocol (NHRP)*
RFC 2677	*Definitions of Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)*

MIBs

MIB	MIBs Link
• CISCO-NHRP-EXT-MIB • NHRP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 DMVPN Tunnel Health Monitoring and Recovery

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 Tunnel Health Monitoring and Recovery

Feature Name	Releases	Feature Information
DMVPN—Tunnel Health Monitoring and Recovery (Interface Line Control)		The DMVPN—Tunnel Health Monitoring and Recovery (Interface Line Control) feature enables NHRP to control the state of the tunnel interface based on the health of the DMVPN tunnels. The following command was introduced: **if-state nhrp**.