



Per-Tunnel QoS for DMVPN

First Published: October 10, 2008

Last Updated: April 30, 2009

The Per-Tunnel QoS for DMVPN feature introduces per-tunnel quality of service (QoS) support for Dynamic Multipoint VPN (DMVPN) tunnel interfaces and increases QoS performance for IP Security (IPSec) Virtual Tunnel Interfaces (VTIs).

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 Per-Tunnel QoS for DMVPN” section on page 16](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Per-Tunnel QoS for DMVPN, page 2](#)
- [Restrictions for Per-Tunnel QoS for DMVPN, page 2](#)
- [Information About Per-Tunnel QoS for DMVPN, page 2](#)
- [How to Configure Per-Tunnel QoS for DMVPN, page 3](#)
- [Configuration Examples for Per-Tunnel QoS for DMVPN, page 7](#)
- [Additional References, page 14](#)
- [Feature Information for Per-Tunnel QoS for DMVPN, page 16](#)



Americas Headquarters:

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

Prerequisites for Per-Tunnel QoS for DMVPN

Before you can configure per-tunnel QoS for DMVPN, you must configure Cisco Express Forwarding (CEF) switching.

Restrictions for Per-Tunnel QoS for DMVPN

- You cannot configure a per-tunnel QoS policy on a tunnel interface *and* a separate QoS policy on the outbound physical interface at the same time.
- You can attach a per-tunnel QoS policy on the tunnel only in the egress direction.

Information About Per-Tunnel QoS for DMVPN

This feature lets you apply a QoS policy on a DMVPN hub on a per-tunnel-instance (per-spoke) basis in the egress direction for DMVPN hub-to-spoke tunnels. This lets you shape the tunnel traffic to individual spokes (a parent policy) and differentiate individual data flows going through the tunnel for policing (a child policy). The QoS policy that the hub uses for a specific spoke is selected according to the specific Next Hop Resolution Protocol (NHRP) group into which that spoke is configured. Although you can configure many spokes into the same NHRP group, the tunnel traffic for each spoke is measured individually for shaping and policing.

For IPsec VTIs, per-tunnel QoS support existed before this feature was introduced. But this feature does improve performance (because HQF performs the queuing at the egress physical interface instead of in the switching path).

You can use this feature with DMVPN with or without IPsec.

With Per-Tunnel QoS for DMVPN, the queuing and shaping is performed at the outbound physical interface for the GRE/IPsec tunnel packets. This means that the GRE header, the IPsec header and the L2 (for the physical interface) header are included in the packet-size calculations for shaping and bandwidth queuing of packets under QoS.

To configure the Per-Tunnel QoS for DMVPN feature, you should understand the following concepts:

- [Benefits of Per-Tunnel QoS for DMVPN, page 2](#)
- [NHRP QoS Provisioning for DMVPN, page 3](#)

Benefits of Per-Tunnel QoS for DMVPN

Without this feature, QoS on a DMVPN hub could only be configured to either measure outbound traffic in the aggregate (over all spokes) or (with extensive manual configuration) the DMVPN hub could measure outbound traffic on a per-spoke basis.

Per-Tunnel QoS for DMVPN provides the following benefits:

- The QoS policy is attached to the DMVPN hub, and criteria for matching the tunnel traffic are set up automatically as each spoke registers with the hub (which means that extensive manual configuration is not needed).
- Traffic can be regulated from the hub to spokes on a per-spoke basis.

- The hub cannot send excessive traffic to (and overrun) a small spoke.
- The amount of outbound hub bandwidth that a “greedy” spoke can consume can be limited, and therefore it cannot monopolize a hub's resources and starve other spokes.

NHRP QoS Provisioning for DMVPN

NHRP performs the provisioning for Per-Tunnel QoS for DMVPN by using NHRP groups.

An NHRP group, which is the new concept introduced by this feature, is the group identity information signaled by a DMVPN node (a spoke) to the DMVPN hub. The hub uses this information to select a locally-defined QoS policy instance for the remote node.

You configure the NHRP group name on the spoke router on the DMVPN GRE tunnel interface. The NHRP group name is communicated to the hub in each of the periodic NHRP registration requests sent from the spoke to the hub. A new Cisco vendor-private NHRP extension **nhrp-group** is defined to carry the NHRP group string in the NHRP registration request.

The NHRP-group-to-QoS-policy mappings are configured on the hub DMVPN GRE tunnel interface. The NHRP group string received from a spoke is mapped to a QoS policy, which is applied for that hub-to-spoke tunnel in the egress direction.

When the NHRP group is configured on the spoke, the group is not immediately sent to the *hub*, but is sent in the next periodic registration request. The spoke can be in only one NHRP group per GRE tunnel interface. If a spoke is configured as a part of two or more DMVPN networks (multiple GRE tunnel interfaces), then the spoke can have a different NHRP group name on each of the GRE tunnel interfaces.

If an NHRP group is not received from the spoke, then a QoS policy is *not* applied, and any existing QoS policy applied for that spoke is removed. If an NHRP group is received from the spoke when previous NHRP registrations did not have an NHRP group, then the corresponding QoS policy is applied. If the same NHRP group name is received from a spoke as was received in the previous NHRP registration request, then no action is taken (because a QoS policy would have already been applied for that spoke). If a different NHRP group is received from the spoke than what was received in the previous NHRP registration request, any applied QoS policy is removed, and the QoS policy corresponding to the new NHRP group is applied.

How to Configure Per-Tunnel QoS for DMVPN

To configure the Per-Tunnel QoS for DMVPN feature, you define an NHRP group on the spokes and then map the NHRP group to a QoS policy on the hub.

This section contains the following procedures:

- [Configuring an NHRP Group on a Spoke, page 4](#) (required)
- [Mapping an NHRP Group to a QoS Policy on the Hub, page 5](#) (required)
- [Verifying Per-Tunnel QoS for DMVPN, page 6](#) (optional)

Configuring an NHRP Group on a Spoke

To configure an NHRP group on a spoke, perform the steps in this section.

Prerequisites

The spoke and the hub must already be configured for DMVPN without the Per-Tunnel QoS feature.

SUMMARY STEPS

1. **enable**
2. **configure** { **terminal** | **memory** | **network** }
3. **interface tunnel** *number*
4. **ip nhrp group** *group-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels (such as privileged EXEC mode). <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure { terminal memory network } Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 1	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 interface that you want to create or configure. • There is no limit on the number of tunnel interfaces that you can create.
Step 4	ip nhrp group <i>group-name</i> Example: Router(config-if# ip nhrp group spoke_group1	Configures an NHRP group on the spoke.
Step 5	end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Mapping an NHRP Group to a QoS Policy on the Hub

To configure an NHRP-group-to-QoS-policy mapping on a hub, perform the steps in this section.



Note

The **qos pre-classify** command is not required with this feature, because classification is performed before encapsulation.

Prerequisites

The spoke and the hub must already be configured for DMVPN without the Per-Tunnel QoS feature.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface tunnel** *number*
4. **ip nhrp map group** *group-name* **service-policy output** *qos-policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels (such as privileged EXEC mode). <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure { terminal memory network }	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 1	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 interface that you want to create or configure. • There is no limit on the number of tunnel interfaces that you can create.

	Command or Action	Purpose
Step 4	<pre>ip nhrp map group <i>group-name</i> service-policy output <i>qos-policy-map-name</i></pre> <p>Example: Router(config-if)# ip nhrp map group spoke_group1 service-policy output group1_parent</p>	Adds the NHRP group to the QoS policy mapping on the hub.
Step 5	<pre>end</pre> <p>Example: Router(config-if)# end</p>	Returns to privileged EXEC mode.

Verifying Per-Tunnel QoS for DMVPN

To verify the configuration of Per-Tunnel QoS for DMVPN, perform the steps in this section.

SUMMARY STEPS

1. `enable`
2. `show dmvpn detail`
3. `show ip nhrp`
4. `show ip nhrp group-map [group-name]`
5. `show policy-map multipoint [tunnel tunnel-interface-number]`
6. `show tunnel endpoints`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	Enables higher privilege levels (such as privileged EXEC mode). <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<pre>show dmvpn detail</pre> <p>Example: Router# show dmvpn detail</p>	Displays detailed DMVPN information for each session, including the Next Hop Server (NHS) and NHS status, crypto session information, and socket details. Also displays the NHRP group received from the spoke and the QoS policy applied to the spoke tunnel.
Step 3	<pre>show ip nhrp</pre> <p>Example: Router# show ip nhrp</p>	Displays the NHRP cache and the NHRP group received from the spoke.

	Command or Action	Purpose
Step 4	<pre>show ip nhrp group-map [group-name]</pre> <p>Example: Router# show ip nhrp group-map Router# show ip nhrp group-map group1-parent</p>	Displays the group-to-policy maps configured on the hub. Also displays the tunnels on which the QoS policy is applied.
Step 5	<pre>show policy-map multipoint [tunnel tunnel-interface-number]</pre> <p>Example: Router# show policy-map multipoint Router# show policy-map multipoint tunnel 1</p>	Displays QoS policy details applied to multipoint tunnels.
Step 6	<pre>show tunnel endpoints</pre> <p>Example: Router# show tunnel endpoints</p>	Displays information about the source and destination endpoints for multipoint tunnels. Also displays the QoS policy applied on the spoke tunnel.

Configuration Examples for Per-Tunnel QoS for DMVPN

This section provides the following configuration examples:

- [Configuring an NHRP Group on a Spoke: Example, page 7](#)
- [Mapping an NHRP Group to a QoS Policy on the Hub: Example, page 8](#)
- [Verifying Per-Tunnel QoS for DMVPN: Examples, page 9](#)

Configuring an NHRP Group on a Spoke: Example

The following example shows how to configure two NHRP groups on three spokes.

Configuring the First Spoke

```
interface Tunnel 1
 ip address 20.1.1.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp group spoke_group1
 ip nhrp map 20.1.1.1 200.0.0.1
 ip nhrp map multicast 200.0.0.1
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
 ip tcp adjust-mss 1360
 ip nhrp nhs 20.1.1.1
 tunnel source Ethernet 0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN

interface Ethernet 0/0
 ip address 200.0.0.2 255.255.255.0
```

Configuring the Second Spoke

```

interface Tunnel 1
 ip address 20.1.1.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp group spoke_group1
 ip nhrp map 20.1.1.1 200.0.0.1
 ip nhrp map multicast 200.0.0.1
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
 ip tcp adjust-mss 1360
 ip nhrp nhs 20.1.1.1
 tunnel source Ethernet 0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN

interface Ethernet 0/0
 ip address 200.0.0.3 255.255.255.0

```

Configuring the Third Spoke

```

interface Tunnel 1
 ip address 20.1.1.4 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication testing
 ip nhrp group spoke_group2
 ip nhrp map 20.1.1.1 200.0.0.1
 ip nhrp map multicast 200.0.0.1
 ip nhrp network-id 172176366
 ip nhrp holdtime 300
 ip tcp adjust-mss 1360
 ip nhrp nhs 20.1.1.1
 tunnel source Ethernet 0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN

interface Ethernet 0/0
 ip address 200.0.0.4 255.255.255.0

```

Mapping an NHRP Group to a QoS Policy on the Hub: Example

The following example shows how to map NHRP groups to a QoS policy on the hub. The example shows a hierarchical QoS policy (parent: group1_parent/group2_parent, child: group1/group2) that will be used for Per-Tunnel QoS for DMVPN. The example also shows how to map the NHRP group spoke_group1 to the QoS policy group1_parent and map the NHRP group spoke_group2 to the QoS policy group2_parent on the hub:

```

class-map match-all group1_Routing
 match ip precedence 6

class-map match-all group2_Routing
 match ip precedence 6

class-map match-all group2_voice
 match access-group 100

class-map match-all group1_voice

```

```

match access-group 100

policy-map group1
  class group1_voice
    priority 1000
  class group1_Routing
    bandwidth percent 20

policy-map group1_parent
  class class-default
    shape average 3000000
  service-policy group1

policy-map group2
  class group2_voice
    priority percent 20
  class group2_Routing
    bandwidth percent 10

policy-map group2_parent
  class class-default
    shape average 2000000
  service-policy group2

interface Tunnel 1
  ip address 20.1.1.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication testing
  ip nhrp map multicast dynamic
  ip nhrp map group spoke_group1 service-policy output group1_parent
  ip nhrp map group spoke_group2 service-policy output group2_parent
  ip nhrp network-id 172176366
  ip nhrp holdtime 300
  ip nhrp registration no-unique
  tunnel source Ethernet0/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile DMVPN

interface Ethernet 0/0
  ip address 200.0.0.1 255.255.255.0

```

Verifying Per-Tunnel QoS for DMVPN: Examples

The following example shows how to display the information about NHRP groups received from the spokes as well as the QoS policy that is applied to each spoke tunnel. You enter this command on the hub:

```
Router# show dmvpn 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 20.1.1.1, VRF ""
  Tunnel Src./Dest. addr: 200.0.0.1/MGRE, Tunnel VRF ""
  Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
Type:Hub, Total NBMA Peers (v4/v6): 3

```

```

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
  1      200.0.0.2          20.1.1.2    UP 00:19:20    D      20.1.1.2/32
NHRP group: spoke_group1
Output QoS service-policy applied: group1_parent

  1      200.0.0.3          20.1.1.3    UP 00:19:20    D      20.1.1.3/32
NHRP group: spoke_group1
Output QoS service-policy applied: group1_parent

  1      200.0.0.4          20.1.1.4    UP 00:19:23    D      20.1.1.4/32
NHRP group: spoke_group2
Output QoS service-policy applied: group2_parent

```

Crypto Session Details:

```

-----
Interface: Tunnell
Session: [0x04AC1D00]
IKE SA: local 200.0.0.1/500 remote 200.0.0.2/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 200.0.0.2
IPSEC FLOW: permit 47 host 200.0.0.1 host 200.0.0.2
Active SAs: 2, origin: crypto map
Outbound SPI : 0x9B264329, transform : ah-md5-hmac
Socket State: Open

```

```

Interface: Tunnell
Session: [0x04AC1C08]
IKE SA: local 200.0.0.1/500 remote 200.0.0.3/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 200.0.0.3
IPSEC FLOW: permit 47 host 200.0.0.1 host 200.0.0.3
Active SAs: 2, origin: crypto map
Outbound SPI : 0x36FD56E2, transform : ah-md5-hmac
Socket State: Open

```

```

Interface: Tunnell
Session: [0x04AC1B10]
IKE SA: local 200.0.0.1/500 remote 200.0.0.4/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 200.0.0.4
IPSEC FLOW: permit 47 host 200.0.0.1 host 200.0.0.4
Active SAs: 2, origin: crypto map
Outbound SPI : 0xAC96818F, transform : ah-md5-hmac
Socket State: Open

```

Pending DMVPN Sessions:

The following example shows how to display information about the NHRP groups that are received from the spokes. You enter this command on the hub:

```

Router# show ip nhrp
20.1.1.2/32 via 20.1.1.2
  Tunnell created 00:22:49, expire 00:01:40
  Type: dynamic, Flags: registered
  NBMA address: 200.0.0.2
  Group: spoke_group1
20.1.1.3/32 via 20.1.1.3
  Tunnell created 00:22:48, expire 00:01:41
  Type: dynamic, Flags: registered
  NBMA address: 200.0.0.3

```

```

Group: spoke_group1
20.1.1.4/32 via 20.1.1.4
Tunnel1 created 00:22:52, expire 00:03:27
Type: dynamic, Flags: registered
NBMA address: 200.0.0.4
Group: spoke_group2

```

The following example shows how to display the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings. You enter this command on the hub:

```

Router# show ip nhrp group-map
Interface: Tunnel1
NHRP group: spoke_group1
QoS policy: group1_parent
Tunnels using the QoS policy:
Tunnel destination overlay/transport address
20.1.1.2/200.0.0.2
20.1.1.3/200.0.0.3

NHRP group: spoke_group2
QoS policy: group2_parent
Tunnels using the QoS policy:
Tunnel destination overlay/transport address
20.1.1.4/200.0.0.4

```

The following example shows how to display statistics about a specific QoS policy as it is applied to a tunnel endpoint. You enter this command on the hub:

```

Router# show policy-map multipoint

Interface Tunnel1 <--> 200.0.0.2

Service-policy output: group1_parent

Class-map: class-default (match-any)
 29 packets, 4988 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
Queueing
queue limit 750 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 3000000, bc 12000, be 12000
target shape rate 3000000

Service-policy : group1

  queue stats for all priority classes:

    queue limit 250 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0

Class-map: group1_voice (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 100
Priority: 1000 kbps, burst bytes 25000, b/w exceed drops: 0

Class-map: group1_Routing (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 6

```

```

Queueing
queue limit 150 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 20% (600 kbps)

Class-map: class-default (match-any)
 29 packets, 4988 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any

queue limit 350 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0

Interface Tunnel1 <--> 200.0.0.3

Service-policy output: group1_parent

Class-map: class-default (match-any)
 29 packets, 4988 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
Queueing
queue limit 750 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 3000000, bc 12000, be 12000
target shape rate 3000000

Service-policy : group1

queue stats for all priority classes:

queue limit 250 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0

Class-map: group1_voice (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: access-group 100
Priority: 1000 kbps, burst bytes 25000, b/w exceed drops: 0

Class-map: group1_Routing (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 6
Queueing
queue limit 150 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 20% (600 kbps)

Class-map: class-default (match-any)
 29 packets, 4988 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any

queue limit 350 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0

```

```
Interface Tunnel1 <--> 200.0.0.4
```

```
Service-policy output: group2_parent
```

```
Class-map: class-default (match-any)
  14 packets, 2408 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  Queueing
  queue limit 500 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  shape (average) cir 2000000, bc 8000, be 8000
  target shape rate 2000000
```

```
Service-policy : group2
```

```
queue stats for all priority classes:
```

```
queue limit 100 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

```
Class-map: group2_voice (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group 100
  Priority: 20% (400 kbps), burst bytes 10000, b/w exceed drops: 0
```

```
Class-map: group2_Routing (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 6
  Queueing
  queue limit 50 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth 10% (200 kbps)
```

```
Class-map: class-default (match-any)
  14 packets, 2408 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

  queue limit 350 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```

Additional References

The following sections provide references related to the Per-Tunnel QoS for DMVPN feature.

Related Documents

Related Topic	Document Title
General information about QoS	“ <i>Quality of Service Overview</i> ” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
Configuring hierarchical queuing	<ul style="list-style-type: none"> “<i>QoS—Hierarchical Queueing Framework (HQF)</i>” module in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i>. <i>Cisco IOS Quality of Service Solutions Command Reference</i>
Configuring NHRP	<ul style="list-style-type: none"> “<i>Configuring NHRP</i>” module in the <i>Cisco IOS IP Addressing Services Configuration Guide</i>. <i>Cisco IOS IP Addressing Services Command Reference</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Per-Tunnel QoS for DMVPN

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1), 12.0(3)S, 12.2(33)SRA, 12.2(33)SXH, or later releases appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.


Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Per-Tunnel QoS for DMVPN

Feature Name	Releases	Feature Information
Per-Tunnel QoS for DMVPN	12.4(22)T	<p>The Per-Tunnel QoS for DMVPN feature introduces per-tunnel QoS support for DMVPN and increases per-tunnel QoS performance for IPsec VTIs.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Benefits of Per-Tunnel QoS for DMVPN, page 2 • Configuring an NHRP Group on a Spoke, page 4 • Mapping an NHRP Group to a QoS Policy on the Hub, page 5 • Verifying Per-Tunnel QoS for DMVPN, page 6 <p>The following commands were introduced or modified: ip nhrp group, ip nhrp map, ip nhrp map group, show dmvpn, show ip nhrp, show ip nhrp group-map, show policy-map multipoint tunnel.</p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

Any Internet Protocol (IP) addresses 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.

© 2008–2009 Cisco Systems, Inc. All rights reserved.

