



CHAPTER 6

Configuring IP Tunnels

This chapter describes how to configure IP tunnels using Generic Route Encapsulation (GRE) on the device.

This chapter includes the following sections:

- [Information About IP Tunnels, page 6-1](#)
- [Licensing Requirements for IP Tunnels, page 6-3](#)
- [Prerequisites for IP Tunnels, page 6-3](#)
- [Guidelines and Limitations, page 6-3](#)
- [Configuring IP Tunnels, page 6-4](#)
- [Displaying Tunnel Interface Statistics, page 6-6](#)
- [Field Descriptions for Tunnel Interfaces, page 6-6](#)
- [Additional References, page 6-7](#)

Information About IP Tunnels

IP tunnels can encapsulate a same-layer or higher layer protocol and transport the result over IP through a tunnel created between two devices.

This section includes the following topics:

- [Overview of IP Tunnels, page 6-1](#)
- [GRE Tunnels, page 6-2](#)
- [Path MTU Discovery, page 6-2](#)
- [Virtualization Support, page 6-3](#)
- [High Availability, page 6-3](#)

Overview of IP Tunnels

IP tunnels consists of the following three main components:

- **Passenger protocol**—The protocol that needs to be encapsulated. IPv4 is an example of a passenger protocol.

Send document comments to nexus7k-docfeedback@cisco.com

- Carrier protocol—The protocol that is used to encapsulate passenger protocol. Cisco NX-OS supports GRE as a carrier protocol.
- Transport protocol—The protocol that is used to carry the encapsulated protocol. IPv4 is an example of a transport protocol.

An IP tunnel takes a passenger protocol, such as IPv4, and encapsulates that protocol within a carrier protocol, such as GRE. The device then transmits this carrier protocol over a transport protocol, such as IPv4.

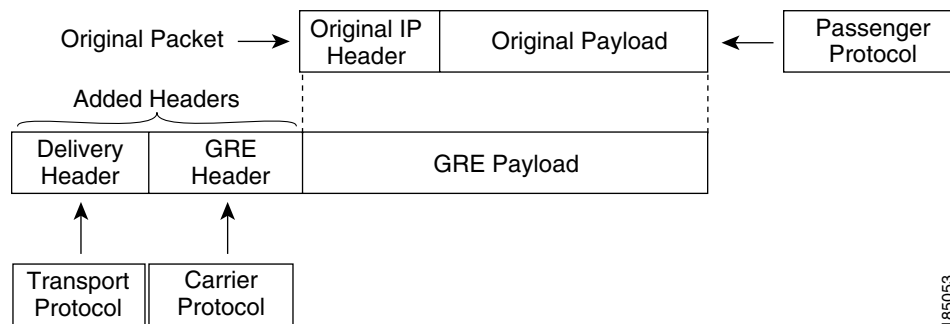
You configure a tunnel interface with matching characteristics on each end of the tunnel. For more information, see the “[Configuring IP Tunnels](#)” section on page 6-4.

GRE Tunnels

You can use GRE as the carrier protocol for a variety of passenger protocols.

[Figure 6-1](#) shows the IP tunnel components for a GRE tunnel. The original passenger protocol packet becomes the GRE payload and the device adds a GRE header to the packet. The device then adds the transport protocol header to the packet and transmits it.

Figure 6-1 GRE PDU



Path MTU Discovery

Path maximum transmission unit (MTU) discovery (PMTUD) prevents fragmentation in the path between two endpoints by dynamically determining the lowest MTU along the path from the packet's source to its destination. PMTUD reduces the send MTU value for the connection if the interface receives information that the packet would require fragmentation.

When you enable PMTUD, the interface sets the Don't Fragment (DF) bit on all packets that traverse the tunnel. If a packet that enters the tunnel encounters a link with a smaller MTU than the MTU value for the packet, the remote link drops the packet and sends an ICMP message back to the sender of the packet. This message indicates that fragmentation was required (but not permitted) and provides the MTU of the link that dropped the packet.



Note

PMTUD on a tunnel interface requires that the tunnel endpoint can receive ICMP messages generated by devices in the path of the tunnel. Check that ICMP messages can be received before using PMTUD over firewall connections.

Send document comments to nexus7k-docfeedback@cisco.com

Virtualization Support

You can configure IP tunnels only in the default virtual device context (VDC).

You can configure a tunnel interface as a member of a Virtual Routing and Forwarding (VRF) instance. By default, Cisco NX-OS places you in the default VDC and default VRF unless you specifically configure another VDC and VRF.

See the *Cisco DCNM Virtual Device Context Configuration Guide, Release 4.0* for information about VDCs and see the *Cisco DCNM Unicast Routing Configuration Guide, Release 4.0* for information about configuring an interface as a member of a VRF.



Note

You must assign a tunnel interface to a VRF before you configure the IP address for that tunnel interface.

High Availability

IP tunnels support stateful restarts. A stateful restart occurs on a supervisor switchover. After the switchover, Cisco NX-OS applies the runtime configuration after the switchover.

Licensing Requirements for IP Tunnels

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	IP tunnels require a LAN Enterprise license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the <i>Cisco DCNM Licensing Guide</i> .
NX-OS	IP tunnels require an Enterprise Services license. For a complete explanation of the NX-OS licensing scheme and how to obtain and apply licenses, see the <i>Cisco NX-OS Licensing Guide</i> .

Prerequisites for IP Tunnels

IP tunnels have the following prerequisites:

- You must be familiar with TCP/IP fundamentals to configure IP tunnels.
- You are logged on to the switch.
- You have installed the Enterprise Services license for Cisco NX-OS.
- You have installed the LAN Enterprise license for DCNM.
- You must enable the tunneling feature in a device before you can configure and enable any IP tunnels.

Guidelines and Limitations

IP tunnels have the following guidelines and limitations:

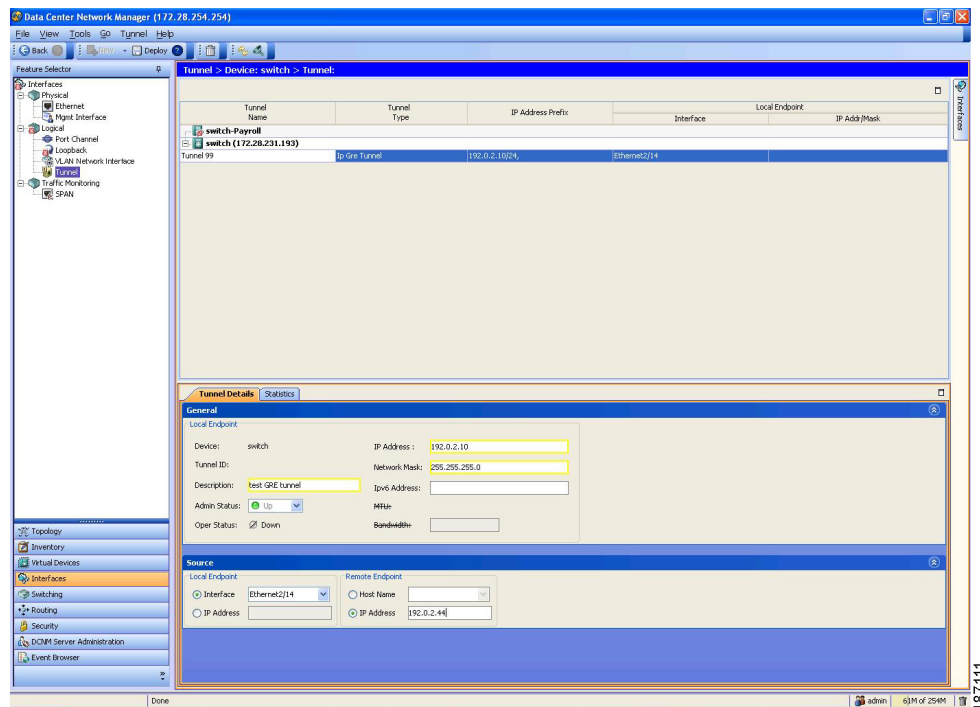
Send document comments to nexus7k-docfeedback@cisco.com

- Cisco NX-OS supports the GRE Header defined in IETF RFC 2784. Cisco NX-OS does not support tunnel keys and other options from IETF RFC 1701.

Configuring IP Tunnels

You can access IP tunnels from the Interfaces feature selection. [Figure 6-2](#) shows how to configure IP tunnels.

Figure 6-2 Configuring Tunnel Interfaces



For more information about the Data Center Network Manager (DCNM) features, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0*

This section includes the following topics:

- [Enabling Tunneling, page 6-4](#)
- [Creating a Tunnel Interface, page 6-5](#)
- [Displaying Tunnel Interface Statistics, page 6-6](#)

Enabling Tunneling

You must enable the tunneling feature before you can configure any IP tunnels.

DETAILED STEPS

To enable the tunneling feature, follow these steps:

Send document comments to nexus7k-docfeedback@cisco.com

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Logical > Tunnel**.
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device that you want to enable IP tunneling on.
- Step 3** From the menu bar, choose **Tunnel > Enable Tunnel Service**.
- Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Creating a Tunnel Interface

You can create a tunnel interface and then configure this logical interface for your IP tunnel.

BEFORE YOU BEGIN

Ensure that you have enabled the tunneling feature.

DETAILED STEPS

To create a tunnel interface, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Logical > Tunnel**.
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device to display a list of existing tunnels.
- Step 3** From the menu bar, choose **Tunnel > New Tunnel**.
The system highlights the new tunnel in the Summary pane, and tabs update in the Details pane.
- Step 4** From the highlighted tunnel field, enter the tunnel number.
The number range is from 0 to 32767.
- Step 5** From the Details pane, click the **Tunnel Details** tab.
The Tunnel Details tab appears.
- Step 6** From the Tunnel Details tab, expand the **General** section.
The general tunnel information appears in the Details pane.
- Step 7** (Optional) From the General section, set the IP Address field to the IPv4 address for this tunnel interface.
- Step 8** (Optional) In the Network Mask field, set the network mask for this IPv4 address in dotted decimal notation.
- Step 9** (Optional) In the IPv6 Address field, set the Primary/prefix length field to the IPv6 address and prefix length for this tunnel interface.
The length range is from 1 to 128.
- Step 10** (Optional) From the Description field, enter a string to describe this tunnel.
The string should be from 1 to 97 alphanumeric characters.
- Step 11** From the Details tab, expand the **Source** section.
The tunnel source and destination appears in the Details pane.

Send document comments to nexus7k-docfeedback@cisco.com

- Step 12** From the local endpoint area, select either an interface or an IP address to act as the tunnel source.
- Step 13** From the Remote endpoint area, select either a host or an IP address to act as the tunnel destination.
- Step 14** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Deleting a Tunnel Interface

You can delete tunnel interfaces.

DETAILED STEPS

To delete a tunnel interface, follow these steps:

- Step 1** From the Feature Selector pane, choose **Interfaces > Logical > Tunnel**.
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device to display a list of existing tunnels.
- Step 3** Click on the tunnel that you want to delete.
- Step 4** From the menu bar, choose **Tunnel > Delete Tunnel**.
- Step 5** Click **Yes** in the confirmation popup window to apply your changes to the device.
-

Displaying Tunnel Interface Statistics

You can configure DCNM to collect tunnel interface statistics. Choose **Interfaces > Logical > Tunnel** from the Feature Selector and navigate to the interface that you want to collect statistics on.

You see the Port Traffic Statistics window. You can collect statistics on input and output (packet and byte) counters, broadcast, multicast, and unicast traffic.

See the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0* for more information on collecting statistics for layer 3 interfaces.

Field Descriptions for Tunnel Interfaces

This section includes the following field descriptions for tunnel interfaces:

- [Tunnel: Details Tab: Tunnel Details Section, page 6-7](#)
- [Tunnels: Details Tab: Source Section, page 6-7](#)
- [Tunnel: Statistics Tab, page 6-7](#)

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Tunnel: Details Tab: Tunnel Details Section

Table 6-1 Tunnel: Details: Tunnel

Field	Description
Device	<i>Display only.</i> Name of device where tunnel interface exists.
Tunnel ID	<i>Display only.</i> Tunnel interface number.
Description	String that describes the tunnel interface.
Admin Status	Administrative status of the tunnel interface. The default is down.
Oper Status	Operational status of the tunnel interface.
IP Address	IPv4 address in dotted decimal notation.
Net mask	Network mask for the IPv4 address, in dotted decimal notation.
IPv6 Address	IPv6 prefix in x:x:x::x/length format.

Tunnels: Details Tab: Source Section

Table 6-2 Tunnels: Details: Source

Field	Description
Local Endpoint	
Interface	Interface for the tunnel source address.
IP Address	IPv4 address, in dotted decimal notation for the tunnel source address.
Remote Endpoint	
Host Name	Device name for tunnel destination.
IP Address	IPv4 address, in dotted decimal notation for the tunnel destination address.

Tunnel: Statistics Tab

Table 6-3 Tunnel: Statistics Tab

Field	Description
Status	Status of statistics collection. Roll over Status to get a popup tip.
Select Parameters	List of statistics that can be gathered on tunnel interfaces.
Show Overview Chart	Overview popup of statistics.

Additional References

For additional information related to implementing IP tunnels, see the following sections:

- [Related Documents, page 6-8](#)

Send document comments to nexus7k-docfeedback@cisco.com

- [Standards, page 6-8](#)

Related Documents

Related Topic	Document Title
IP Tunnel commands	<i>Cisco NX-OS Interfaces Command Reference, Release 4.0</i>
IP Fragmentation and Path MTU discovery	<i>Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC</i>

Standards

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