Configuring IP Tunnels

This chapter describes how to configure IP tunnels.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

Feature History for Configuring IP Tunnels

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Release	Feature Information
GRE tunnels	7.3(0)DX(1)	Support for M3 Series modules was added.
GRE tunnels	6.2(10)	Support for F3 Series modules was added.
Support for tunnel and its transport in different VRFs	6.1(1)	This feature was introduced.

Feature Name	Release	Feature Information
IP tunnels in VDC and VRF other than default	4.2(1)	This feature was introduced.
IP tunnels	4.0(1)	This feature was introduced.

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.

IP Tunnel Overview

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.
- Carrier protocol—The protocol that is used to encapsulate the 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.

You must enable the tunnel feature before you can see configure it. From Cisco NX-OS Release 4.2, the system automatically takes a checkpoint prior to disabling the feature, and you can roll back to this checkpoint. See the Cisco Nexus 7000 Series NX-OS System Management Configuration Guide for information about rollbacks and checkpoints.

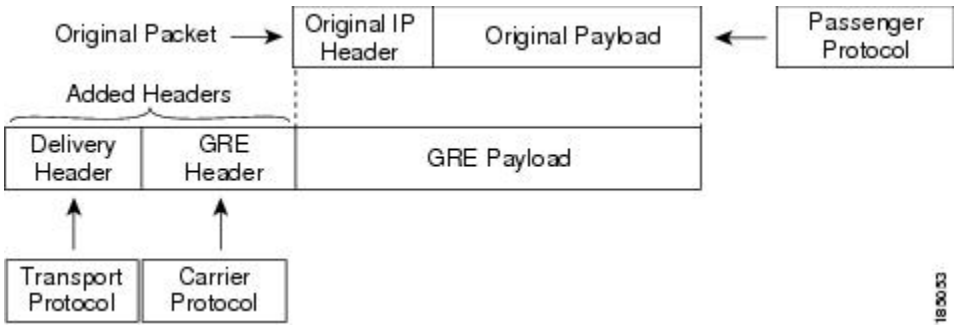
GRE Tunnels

Note From Cisco NX-OS Release 5.1(1), the software supports multicasting over GRE tunnels.

You can use generic routing encapsulation (GRE) as the carrier protocol for a variety of passenger protocols.

The figure below 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 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. Cisco NX-OS software disables ICMP unreachable messages by default. ICMP unreachable messages can be enabled in the Cisco NX-OS software using the **ip unreachables** interface command.

Virtualization Support

From Cisco NX-OS Release 4.2, you can configure tunnels in a nondefault VDC and a nondefault VRF. A tunnel configured in one VDC is isolated from a tunnel with the same number configured in another VDC. For example, Tunnel 0 in VDC 1 is independent of tunnel 0 in VDC 2.

Before Cisco NX-OS Release 6.1(1), a tunnel interface and tunnel transport should be in the same VRF. See the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide for information about VDCs and see the Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide for information about VRFs.

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.

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 must enable the tunneling feature in a device before you can configure and enable any IP tunnels.

Guidelines and Limitations for IP Tunnels

IP tunnels have the following configuration guidelines and limitations:

- 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.
- Tunnels are supported only on the M Series cards on Cisco Nexus 7000 Series platforms.
- Cisco NX-OS does not support the Web Cache Control Protocol (WCCP) on tunnel interfaces.
- Tunnel features are supported only on M series and F3 series modules on Cisco Nexus 7000 Series and Cisco Nexus 7700 Series platforms.
- Cisco NX-OS does not support GRE tunnel keepalives.
- When the tunnelled (encapsulated) traffic is forwarded to the same interface from where the traffic was originally received (unencapsulated), make ensure that the IP redirects are disabled using the **no ip redirects** command.
- IPv6 as a carrier or a passenger/transport protocol is not supported in GRE Tunnels.

Default Settings for IP Tunnels

Table 1: Default Settings for IP Tunnels

Parameter	Default
Path MTU discovery age timer	10 minutes
Path MTU discovery minimum MTU	64
Tunnel feature	Disabled

Configuring IP Tunnels

Enabling Tunneling

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature tunnel**	Allows the creation of a new tunnel interface. To disable the tunnel interface feature, use the **no** form of this command.
Step 3	(Optional) switch(config)# **show feature**	Displays information about the features enabled on the device.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Creating a Tunnel Interface

Before you begin

- From Cisco NX-OS Release 6.1 and later releases, you can configure the tunnel source and the tunnel destination in different VRFs. Ensure that you have enabled the tunneling feature.
- You can create a tunnel interface and then configure this logical interface for your IP tunnel.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)#**interface tunnel** *number*	Creates a new tunnel interface.
Step 3	switch(config-if)# **tunnel source** {*ip-address* | *interface-name*}	Configures the source address for this IP tunnel.
Step 4	switch(config-if)# **tunnel destination** {*ip-address* | *host-name*}	Configures the destination address for this IP tunnel.
Step 5	switch(config-if)# **tunnel use-vrf** *vrf-name*	Uses the configured VRF to look up the tunnel IP destination address.

	Command or Action	Purpose
Step 6	(Optional) switch(config-if)# **show interfaces tunnel** *number*	Displays the tunnel interface statistics.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Use the **no interface tunnel** command to remove the tunnel interface and all associated configuration.

Table 2: Removing the Tunnel Interface and its Associated Configuration

Command	Purpose
no interface tunnel *number*	Deletes the tunnel interface and the associated configuration.

You can configure the following optional parameters to tune the tunnel in interface configuration mode:

Table 3: Configuring Optional Parameters

Command	Purpose
description *string*	Configures a description for the tunnel.
mtu *value*	Sets the MTU of IP packets sent on an interface.
tunnel ttl *value*	Sets the tunnel time-to-live value. The range is from 1 to 255.

Example

This example shows how to create a tunnel interface:

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel source ethernet 1/2
switch(config-if)# tunnel destination 192.0.2.1
switch(config-if)# copy running-config startup-config
```

Configuring a GRE Tunnel

You can set a tunnel interface to GRE tunnel mode.

Before you begin

Ensure that you have enabled the tunneling feature.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface tunnel** *number*	Creates a new tunnel interface.
Step 3	switch(config-if)# **tunnel mode gre ip**	Sets this tunnel mode to GRE.
Step 4	(Optional) switch(config-if)# **show interfaces tunnel** *number*	Displays the tunnel interface statistics.
Step 5	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Enabling Path MTU Discovery

Use the **tunnel path-mtu discovery** command to enable path MTU discovery on a tunnel.

Command	Purpose
tunnel path-mtu-discovery [**age-timer** *min*] [**min-mtu** *bytes*]	Enables Path MTU Discovery (PMTUD) on a tunnel interface. The parameters are as follows: • *mins*—Number of minutes. The range is from 10 to 30. The default is 10. • *mtu-bytes*—Minimum MTU recognized. The range is from 92 to 65535. The default is 92.

Assigning VRF Membership to a Tunnel Interface

You can add a tunnel interface to a VRF.

Before you begin

- Ensure that you have enabled the tunneling feature.
- Before you configure this feature for the entire system, ensure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.
- Assign the IP address for a tunnel interface after you have configured the interface for a VRF.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface tunnel** *number*	Enters interface configuration mode.
Step 3	switch(config-if)# **vrf member** *vrf-name*	Adds this interface to a VRF.

	Command or Action	Purpose
Step 4	switch(config-vrf)# **ip address** *ip-prefix/length*	Configures an IP address for this interface. You must do this step after you assign this interface to a VRF.
Step 5	(Optional) switch(config-vrf)# **show vrf** [*vrf-name*] **interface** *interface-type number*	Displays VRF information.
Step 6	(Optional) switch(config-vrf)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to add a tunnel interface to the VRF:

```
switch# configure terminal
switch(config)# interface tunnel 0
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 209.0.2.1/16
switch(config-if)# copy running-config startup-config
```

Configuration Examples for IP Tunneling

These examples show a simple GRE tunnel. Ethernet 1/2 is the tunnel source for router A and the tunnel destination for router B. Ethernet interface 2/1 is the tunnel source for router B and the tunnel destination for router A.

Router A:

```
feature tunnel
interface tunnel 0
  ip address 209.165.20.2/8
  tunnel source ethernet 1/2
  tunnel destination 192.0.2.2
  tunnel mode gre ip
  tunnel path-mtu-discovery 25 1500
interface ethernet1/2
  ip address 192.0.2.55/8
```

Router B:

```
feature tunnel
interface tunnel 0
  ip address 209.165.20.1/8
  tunnel source ethernet2/1
  tunnel destination 192.0.2.55
  tunnel mode gre ip
interface ethernet 2/1
ip address 192.0.2.2/8
```

Verifying the IP Tunnel Configuration

Use one of the following commands to verify IP tunnel configuration information:

Table 4: Verifying the IP Tunnel Configuration

Command	Purpose
show interface tunnel *number*	Displays the configuration for the tunnel interface (MTU, protocol, transport, and VRF). Displays input and output packets, bytes, and packet rates.
show interface brief | include Tunnel	Displays the operational status, IP address, encapsulation type, and MTU of the tunnel interface.
show interface tunnel *number* **description**	Displays the configured description of the tunnel interface.
show interface tunnel *number* **status**	Displays the operational status of the tunnel interface.
show interface tunnel *number* **status err-disabled**	Displays the error disabled status of the tunnel interface.

Related Documents

Table 5: Related Documents

Related Topic
Cisco Nexus 7000 Series NX-OS Interfaces Command Reference
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide
Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide
Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 7000 Series Switches, Release 6.x
Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide
Cisco NX-OS Licensing Guide
VLANs, MAC address tables, private VLANs, and the Spanning Tree Protocol. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide
Cisco Nexus 7000 Series NX-OS FabricPath Command Reference
Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide
Cisco Nexus 7000 Series NX-OS Release Notes