CHAPTER 5

Configuring IPsec VPN Fragmentation and MTU

This chapter provides information about configuring IPsec VPN fragmentation and the maximum transmission unit (MTU). It includes the following sections:

For more information about the commands used in this chapter, see the *Catalyst 6500 Series Cisco IOS Command Reference, 12.2SX* publication. Also refer to the related Cisco IOS Release 12.2 software command reference and master index publications. For more information about accessing these publications, see the "Related Documentation" section on page xvi.

Note Some illustrations in this chapter refer to the IPsec VPN SPA. In these instances, the VSPA performs the equivalent function.

Understanding IPsec VPN Fragmentation and MTU

This section includes the following topics:

Overview of Fragmentation and MTU

When a packet is nearly the size of the maximum transmission unit (MTU) of the physical egress port of the encrypting switch, and it is encapsulated with IPsec headers, it probably will exceed the MTU of the egress port. This situation causes the packet to be fragmented after encryption (post-fragmentation), which requires the IPsec peer to perform reassembly before decryption, degrading its performance. To minimize post-fragmentation, you can set the MTU in the upstream data path to ensure that most fragmentation occurs before encryption (prefragmentation). Prefragmentation for IPsec VPNs avoids performance degradation by shifting the reassembly task from the receiving IPsec peer to the receiving end hosts.

Note In this document, prefragmentation refers to fragmentation prior to any type of encapsulation, such as IPsec or GRE. IPsec prefragmentation refers to fragmentation prior to IPsec encryption.

To ensure prefragmentation in most cases, we recommend the following MTU settings:

- The crypto interface VLAN MTU associated with the VSPA should be set to be equal or less than the egress interface MTU.
- For GRE over IPsec, the IP MTU of the GRE tunnel interface should be set below the egress interface MTU by at least the overhead of IPsec encryption and the 24-byte GRE+IP header (20-byte IP header plus 4-byte GRE header). Because options such as tunnel key (RFC 2890) are not supported, the GRE+IP IP header will always be 24 bytes.

Note The crypto interface VLAN MTU, the egress interface MTU, and the IP MTU of the GRE tunnel interface are all Layer 3 parameters.

The following are additional guidelines for IPsec prefragmentation and MTU in crypto-connect mode:

- If a packet's DF (Don't Fragment) bit is set and the packet exceeds the MTU at any point in the data path, the packet will be dropped. To prevent a packet drop, clear the DF bit by using either policy-based routing (PBR) or the **crypto df-bit clear** command.
- If GRE encapsulation is not taken over by the VSPA, and if the packets exceed the IP MTU of the GRE tunnel interface, the route processor will fragment and encapsulate the packets.

Note If the supervisor engine performs GRE encapsulation, the encapsulated packets will have the DF bit set.

For general information on fragmentation and MTU issues, see "Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec" at this URL:

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml

IPsec Prefragmentation

In the IPsec prefragmentation process (also called Look-Ahead Fragmentation, or LAF), the encrypting switch can predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPsec security association (SA). IPsec prefragmentation avoids reassembly by the receiving switch before decryption and helps improve overall IPsec traffic throughput by shifting the reassembly task to the end hosts.

A packet will be fragmented before encryption if either of the following conditions is met:

- The encrypted packet will exceed the MTU of the crypto interface VLAN.
- The clear packet exceeds the tunnel MTU.

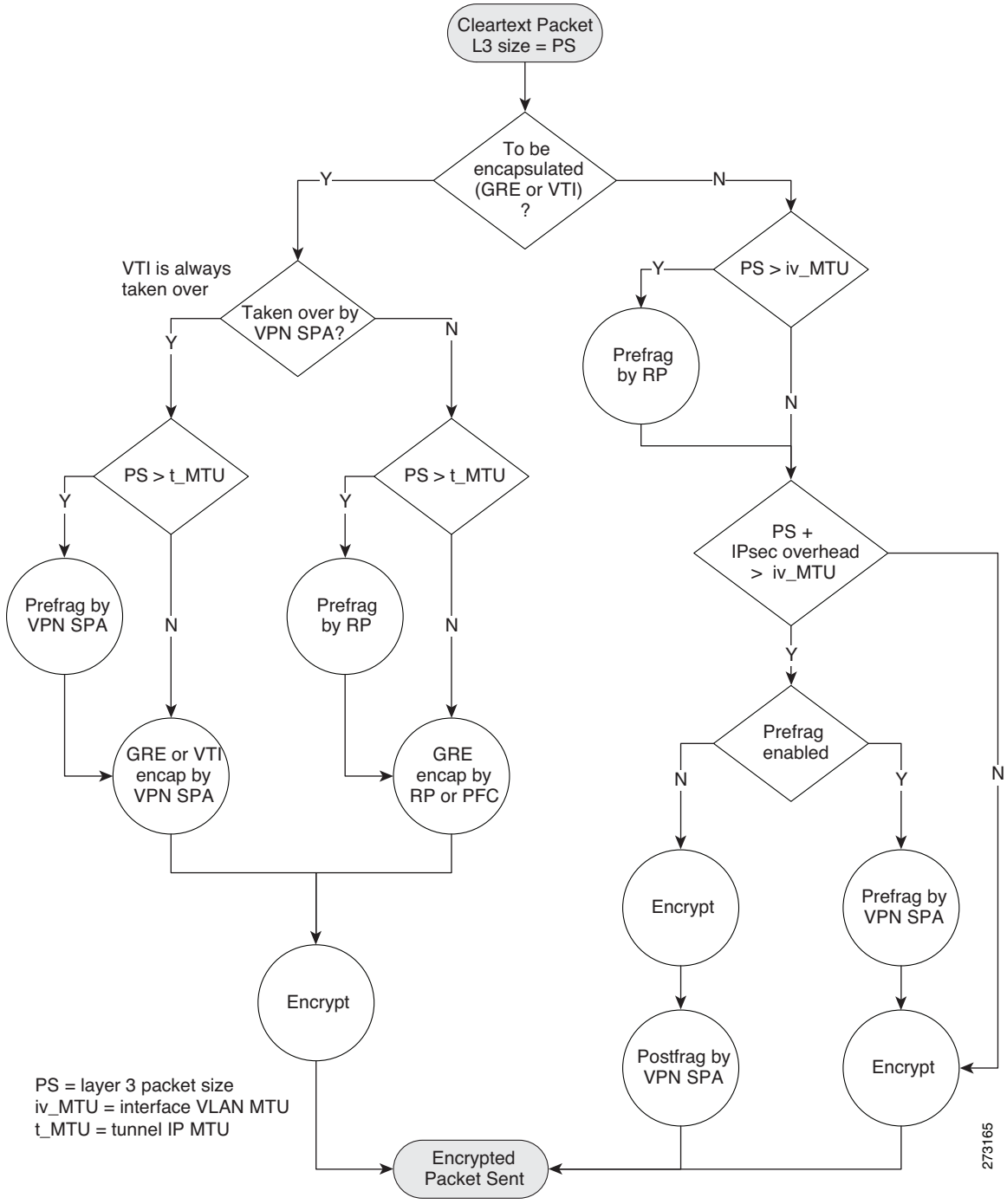
Fragmentation in Different Modes

The fragmentation process differs depending on the IPsec VPN mode and whether GRE or virtual tunnel interface (VTI) is used. The process is described in the following sections:

Overview of the Fragmentation Process

Figure 5-1 shows the fragmentation process for IPsec packets in all VPN modes.

Figure 5-1 Fragmentation of IPsec Packets in All VPN Modes



These notes apply to the fragmentation process:

- The fragmentation process described in Figure 5-1 applies only when the DF (Don't Fragment) bit is not set for cleartext packets entering the flowchart. If a packet requires fragmentation and the DF bit is set, the packet will be dropped.
- VTI encapsulation is always taken over by the VSPA.
- GRE encapsulation of RP-generated packets is never taken over by the VSPA.
- GRE encapsulation of mGRE packets is never taken over by the VSPA.
- The VSPA will perform only a single fragmentation operation, either prefragmentation or postfragmentation, but not both.
- Fragmentation is based on the IP MTU of the tunnel or of the crypto interface VLAN, not the egress interface.
- Path MTU discovery (PMTUD) is supported in both crypto-connect and VRF modes.
- The **ip tcp adjust-mss** command is supported in all modes.

Fragmentation of IPsec Packets in Crypto-Connect Mode

For fragmentation of packets in crypto-connect mode, the following are the MTU setting requirements and recommendations:

- The configured IP MTU of the interface VLAN
  - Prefragmentation of traffic by the VSPA is based on this MTU.
  - You must configure this MTU to be less than or equal to the minimum MTU of the physical egress interfaces configured on the port VLAN, or packets will be dropped.
- The configured MTU of the LAN interface
  - To avoid fragmentation by the RP, we recommend that you configure the MTU of the LAN interface to be less than or equal to the configured IP MTU of the interface VLAN.

In the following example, a 1500-byte cleartext packet will not be fragmented by the RP, because it is within the MTU of the interface VLAN. The cleartext packet will be fragmented by the VSPA, because the IPsec overhead would cause the encrypted packet to exceed the MTU of the interface VLAN.

A 1600-byte cleartext packet will first be fragmented by the RP, because the packet exceeds the MTU of the interface VLAN. The packet will then be fragmented again by the VSPA, because the IPsec overhead added by the encryption process would cause the encrypted packet to exceed the MTU of the interface VLAN.

```
interface GigabitEthernet1/1
  ! switch inside port
  mtu 9216
  ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
  ! switch outside port
  ! mtu 1500 by default
  switchport
  switchport access vlan 502
  switchport mode access
!
interface Vlan2
  ! interface vlan
  ! mtu 1500 by default
  ip address 11.0.0.2 255.255.255.0
  crypto map testtag
```

```
  crypto engine slot 4/0
!
interface Vlan502
  ! port vlan
  no ip address
  crypto connect vlan 2
!
```

Fragmentation of GRE Packets in Crypto-Connect Mode

For fragmentation of packets in crypto-connect mode, the following are the MTU setting requirements and recommendations:

- The configured IP MTU of the crypto interface VLAN
  - You must configure this MTU to be less than or equal to the minimum MTU of the physical egress interfaces configured on the port VLAN, or packets will be dropped.
- The configured MTU of the LAN interface
  - To avoid fragmentation by the RP, we recommend that you configure the MTU of the LAN interface to be less than or equal to the configured IP MTU of the crypto interface VLAN.
- The configured IP MTU of the GRE tunnel interface
  - Prefragmentation of traffic by the VSPA is based on this MTU.
  - You must set this MTU so that IPsec-encrypted GRE packets will not exceed the IP MTU of the crypto interface VLAN, or packets will be dropped. This requirement applies regardless of whether the GRE tunnel is taken over by the VSPA.

In the following example, if the tunnel is taken over by the VSPA, a 1600-byte cleartext packet will be fragmented by the VSPA, because the packet exceeds the IP MTU of the tunnel interface. The fragmented packet will then be GRE-encapsulated and IPsec-encrypted by the VSPA.

If the tunnel is not taken over by the VSPA, a 1600-byte cleartext packet will be fragmented by the RP, because the packet exceeds the IP MTU of the tunnel interface. The fragmented packet will then be GRE-encapsulated by the PFC and IPsec-encrypted by the VSPA.

```
interface Tunnel1
  ip mtu 1400
  ip address 1.0.0.1 255.255.255.0
  tunnel source Vlan2
  tunnel destination 11.0.0.2
!
interface GigabitEthernet1/1
  ! switch inside port
  mtu 9216
  ip address 12.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
  ! switch outside port
  ! mtu 1500 by default
  switchport
  switchport access vlan 502
  switchport mode access
!
interface Vlan2
  ! mtu 1500 by default
  ip address 11.0.0.1 255.255.255.0
  no mop enabled
  crypto map testtag
  crypto engine slot 4/0
```

```
!
interface Vlan502
  no ip address
  crypto connect vlan 2
!
```

Fragmentation of IPsec Packets in VRF Mode

For fragmentation of packets in VRF mode, the following are the MTU setting requirements and recommendations:

- The MTU of the crypto interface VLAN.
  - Prefragmentation by the VSPA will be based on this MTU.
  - You must configure this MTU to be less than or equal to the minimum MTU of the physical egress interfaces, or packets will be dropped.
- The configured MTU of the LAN interface
  - To avoid fragmentation by the RP, we recommend that you configure the MTU of the LAN interface to be less than or equal to the configured IP MTU of the crypto interface VLAN.

In the following example, a 1500-byte cleartext packet will not be fragmented by the RP, because it is within the MTU of the interface VLAN. The cleartext packet will be fragmented by the VSPA, because the IPsec overhead would cause the encrypted packet to exceed the MTU of the interface VLAN.

A 1600-byte cleartext packet will first be fragmented by the RP, because the packet exceeds the MTU of the interface VLAN. The packet will then be fragmented again by the VSPA, because the IPsec overhead added by the encryption process would cause the encrypted packet to exceed the MTU of the interface VLAN.

```
interface GigabitEthernet1/1
  ! switch inside port
  mtu 9216
  ip vrf forwarding ivrf
  ip address 12.0.0.1 255.255.255.0
!
!
interface GigabitEthernet1/2
  ! switch outside port
  ! mtu 1500 by default
  ip address 11.0.0.1 255.255.255.0
  crypto engine slot 4/0 outside
!
interface Vlan2
  ! mtu 1500 by default
  ip vrf forwarding ivrf
  ip address 13.0.0.252 255.255.255.0
  crypto map testtag
  crypto engine slot 4/0 inside
!
```

Fragmentation of GRE Packets in VRF Mode

For fragmentation of packets in VRF mode, the following are the MTU setting requirements and recommendations:

- The MTU of the crypto interface VLAN.
  - You must configure this MTU to be less than or equal to the minimum MTU of the physical egress interfaces configured on the port VLAN, or packets will be dropped.

- The configured MTU of the LAN interface
  - To avoid fragmentation by the RP, we recommend that you configure the MTU of the LAN interface to be less than or equal to the configured IP MTU of the crypto interface VLAN.
- The configured IP MTU of the GRE tunnel interface
  - Prefragmentation by the VSPA will be based on this MTU.
  - You must set this MTU so that IPsec-encrypted GRE packets will not exceed the minimum MTU of the physical egress interfaces, or packets will be dropped. This requirement applies regardless of whether the GRE tunnel is taken over by the VSPA.

In the following example, if the tunnel is taken over by the VSPA, a 1600-byte cleartext packet will be fragmented by the VSPA, because the packet exceeds the IP MTU of the tunnel interface. The fragmented packet will then be GRE-encapsulated and IPsec-encrypted by the VSPA.

If the tunnel is not taken over by the VSPA, a 1600-byte cleartext packet will be fragmented by the RP, because the packet exceeds the IP MTU of the tunnel interface. The fragmented packet will then be GRE-encapsulated by the PFC and IPsec-encrypted by the VSPA.

```
interface Tunnel1
  ip mtu 1400
  ip vrf forwarding coke
  ip address 10.1.1.254 255.255.255.0
  tunnel source 172.1.1.1
  tunnel destination 100.1.1.1
  tunnel protection ipsec profile tp
  crypto engine slot 4/0 inside
!
interface GigabitEthernet6/1
  ! switch outside port
  ! mtu 1500 by default
  ip address 172.1.1.1 255.255.255.0
  crypto engine slot 4/0 outside
!
interface FastEthernet7/13
  ! switch inside port
  mtu 9216
  ip vrf forwarding coke
  ip address 13.1.1.2 255.255.255.0
!
```

Fragmentation of IPsec Packets Using VTI

The following are the relevant MTU settings for fragmentation of static virtual tunnel interface (sVTI) packets:

- The IP MTU of the VTI tunnel interface.
  - Prefragmentation by the VSPA will be based on this MTU.
  - Configuring this MTU is unnecessary because it is automatically adjusted to accommodate the IPsec overhead.

Note We recommend that the IP MTU of the VTI tunnel interface be left at its default value. If you change it, be sure that it does not exceed the MTU of the physical egress interface minus the IPsec overhead.

The fragmentation behavior using VTI is the same as the behavior shown in the "Fragmentation of GRE Packets in VRF Mode" section on page 5-7 for the case in which the tunnel is taken over by the VSPA.

Configuring IPsec Prefragmentation

IPsec prefragmentation can be configured globally or at the interface level. By default, IPsec prefragmentation is enabled globally. Enabling or disabling IPsec prefragmentation at the interface will override the global configuration.

IPsec Prefragmentation Configuration Guidelines

Note Tunnels support only IPsec prefragmentation; postfragmentation is not supported. The guidelines in this section apply only to an interface to which a crypto map is applied.

When configuring IPsec prefragmentation, follow these guidelines:

- To configure IPsec prefragmentation at the interface level, apply it on the interface to which the crypto map is applied.
- If an IPsec peer is experiencing high CPU utilization with large packet flows, verify that IPsec prefragmentation is enabled (the peer may be reassembling large packets).
- IPsec prefragmentation for IPsec VPNs operates in IPsec tunnel mode. It does not apply in IPsec transport mode.
- IPsec prefragmentation for IPsec VPNs functionality depends on the **crypto ipsec df-bit** configuration of the interface to which the crypto map is applied, and on the incoming packet "do not fragment" (DF) bit state. For general information about IPsec prefragmentation, see the following URL:

  http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftprefrg.html
- GRE+IP encapsulation adds 24 bytes to the packet size. When configuring for prefragmentation based on anticipated GRE overhead, use this value.
- IPsec encryption adds a number of bytes to the packet size depending on the configured IPsec transform set. When configuring for prefragmentation based on anticipated IPsec overhead, use the following table of worst-case IPsec overhead bytes for various IPsec transform sets:

IPsec Transform Set	IPsec Overhead, Maximum Bytes
esp-aes-(256 or 192 or 128) esp-sha-hmac or md5	73
esp-aes (256 or 192 or 128)	61
esp-3des, esp-des	45
esp-(des or 3des) esp-sha-hmac or md5	57
esp-null esp-sha-hmac or md5	45
ah-sha-hmac or md5	44

Configuring IPsec Prefragmentation Globally

IPsec prefragmentation is globally enabled by default. To enable or disable prefragmentation for IPsec VPNs at the global level, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto ipsec fragmentation before-encryption`	Enables prefragmentation for IPsec VPNs globally.
Step 2	`Router(config)# crypto ipsec fragmentation after-encryption`	Disables prefragmentation for IPsec VPNs globally.

Configuring IPsec Prefragmentation at the Interface

IPsec prefragmentation is globally enabled by default. To enable or disable prefragmentation for IPsec VPNs at the interface level, perform this task beginning in interface configuration mode for the interface to which the crypto map is attached:

	Command	Purpose
Step 1	`Router(config-if)# crypto ipsec fragmentation before-encryption`	Enables prefragmentation for IPsec VPNs on the interface.
Step 2	`Router(config-if)# crypto ipsec fragmentation after-encryption`	Disables prefragmentation for IPsec VPNs on the interface.

Note Enabling or disabling IPsec prefragmentation at the interface will override the global configuration.

Verifying the IPsec Prefragmentation Configuration

To verify that IPsec prefragmentation is enabled, consult the interface statistics on the encrypting switch and the decrypting switch. If fragmentation occurs on the encrypting switch, and no reassembly occurs on the decrypting switch, fragmentation is occurring before encryption, which means that the packets are not being reassembled before decryption and the feature is enabled.

To verify that the IPsec prefragmentation feature is enabled, enter the **show running-configuration** command on the encrypting switch. If the feature is enabled, no fragmentation feature will appear in the command output:

```
Router# show running-configuration

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!!! the postfragmentation feature appears here if IPsec prefragmentation is disabled
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

If IPsec prefragmentation has been disabled, the postfragmentation feature will appear in the command output:

```
Router# show running-configuration

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
crypto ipsec fragmentation after-encryption
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

To display the configuration of the encrypting switch interface VLAN, enter the **show running-configuration interface** command. If the IPsec prefragmentation feature is enabled, a prefragmentation statement will appear in the command output:

```
Router# show running-configuration interface vlan2

interface Vlan2
 ip address 15.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 1/0
 crypto ipsec fragmentation before-encryption
```

If the IPsec prefragmentation feature has been disabled at the interface VLAN, a postfragmentation statement will appear in the command output:

```
Router# show running-configuration interface vlan2

interface Vlan2
 ip address 15.0.0.2 255.255.255.0
 crypto map testtag
 crypto engine slot 1/0
 crypto ipsec fragmentation after-encryption
end
```

Configuring MTU Settings

The Cisco IOS software supports several types of configurable maximum transmission unit (MTU) options at various levels of the protocol stack. You should ensure that all MTU values are consistent to avoid unnecessary fragmentation of packets.

MTU Settings Configuration Guidelines and Restrictions

When configuring MTU settings for a VSPA, follow these guidelines and note these restrictions:

- The MTU value used by the VSPA for fragmentation decisions is based on the IP MTU of the tunnel or of the crypto interface VLAN, not the egress interface. For information on the recommended MTU settings, see the "Fragmentation in Different Modes" section on page 5-3.
- If you have GRE tunneling configured, see the "Fragmentation in Different Modes" section on page 5-3 for information on the recommended MTU settings.

Note For additional information on fragmentation of packets, see the "Configuring IPsec Prefragmentation" section on page 5-9.

Changing the Physical Egress Interface MTU

You can configure either the Layer 3 MTU or the IP MTU of the physical egress interface. To change the MTU value on a physical egress interface, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Enters interface configuration mode for the interface.
Step 2	`Router(config-if)# mtu` *bytes*	Configures the maximum transmission unit (MTU) size for the interface. • *bytes*—The range is 1500 to 9216; the default is 1500.

1. *type* = **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

Changing the Tunnel Interface IP MTU

You can configure the IP MTU of the tunnel interface, but you cannot configure the Layer 3 MTU. To change the IP MTU value on a tunnel, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *tunnel_name*	Enters interface configuration mode for the tunnel.
Step 2	`Router(config-if)# ip mtu` *bytes*	Configures the IP MTU size for the tunnel. • *bytes*—The minimum is 68; the maximum and the default depend on the interface medium.

Changing the Interface VLAN MTU

You can configure the Layer 3 MTU of the interface VLAN. To change the MTU value on an interface VLAN, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface` *vlan_ID*	Enters interface configuration mode for the VLAN.
Step 2	`Router(config-if)# mtu` *bytes*	Configures the MTU size for the interface VLAN. • *bytes*—The range is 64 to 9216; the default is 1500.

Verifying the MTU Size

To verify the MTU size for an interface, enter the **show interface** command or the **show ip interface** command, as shown in the following examples:

To display the MTU value for a secure port, enter the **show interface** command:

```
Router# show interface g1/1

GigabitEthernet1/1 is up, line protocol is up (connected)
Hardware is C6k 1000Mb 802.3, address is 000a.8ad8.1c4a (bia 000a.8ad8.1c4a)
MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
...
```

To display the MTU size for an interface VLAN, enter the **show interface** command:

```
Router# show interface vlan2
Vlan2 is up, line protocol is up
  Hardware is EtherSVI, address is 000e.39ad.e700 (bia 000e.39ad.e700)
  Internet address is 192.168.1.1/16
  MTU 1000 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
...
```

To display the IP MTU value for a GRE tunnel, enter the **show ip interface** command:

```
Router# show ip interface tunnel 2

Tunnel2 is up, line protocol is up
Internet address is 11.1.0.2/16
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1450 bytes
...
```

Configuration Examples

The following sections provide examples of IPsec prefragmentation configurations:

- Crypto-Connect Mode IPsec Prefragmentation Configuration Example, page 5-13
- VRF Mode with GRE using Tunnel Protection IPsec Prefragmentation Configuration Example, page 5-15

Crypto-Connect Mode IPsec Prefragmentation Configuration Example

The following example shows an IPsec prefragmentation configuration using crypto-connect mode:

```
!
hostname router-1
!
vlan 2,502
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key 12345 address 11.0.0.1
```

```
!
!
crypto ipsec transform-set proposal1 esp-3des esp-md5-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 11.0.0.1
 set transform-set proposal1
 match address 101
!
!
interface GigabitEthernet1/1
  !switch inside port
  ! mtu 1500 by default
  ip address 13.0.0.1 255.255.255.0
!
interface GigabitEthernet1/2
 !switch outside port
  mtu 1000
  switchport
  switchport access vlan 502
  switchport mode access
!
interface GigabitEthernet4/0/1
  !VSPA inside port
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,2,1002-1005
  switchport mode trunk
  mtu 9216
  flowcontrol receive on
  flowcontrol send off
  spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
  !VSPA outside port
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,502,1002-1005
  switchport mode trunk
  mtu 9216
  flowcontrol receive on
  flowcontrol send off
  spanning-tree portfast trunk
!
interface Vlan2
 !interface vlan
  mtu 1000
  ip address 11.0.0.2 255.255.255.0
  crypto map testtag
  crypto engine slot 4/0
!
interface Vlan502
  !port vlan
  no ip address
  crypto connect vlan 2
!
ip classless
ip route 12.0.0.0 255.0.0.0 11.0.0.1
!
access-list 101 permit ip host 13.0.0.2 host 12.0.0.2
!
end
```

VRF Mode with GRE using Tunnel Protection IPsec Prefragmentation Configuration Example

The following example shows an IPsec prefragmentation configuration using VRF mode with GRE and tunnel protection:

```
!
hostname router-1
!
ip vrf coke
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
crypto keyring key1
 pre-shared-key address 100.1.1.1 key happy-eddie
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp profile prof1
 keyring key1
 match identity address 100.1.1.1 255.255.255.255
!
crypto ipsec transform-set TR esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile tp
 set transform-set TR
 set isakmp-profile prof1
!
!
crypto engine mode vrf
!
interface Tunnel1
  ip mtu 1400
  ip vrf forwarding coke
  ip address 10.1.1.254 255.255.255.0
  tunnel source 172.1.1.1
  tunnel destination 100.1.1.1
  tunnel protection ipsec profile tp
  crypto engine slot 4/0 inside
!
interface GigabitEthernet4/0/1
  !VSPA inside port
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,1002-1005
  switchport mode trunk
  cdp enable
  spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
  !VSPA outside port
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,1002-1005
  switchport mode trunk
```

```
  cdp enable
  spanning-tree portfast trunk
!
interface GigabitEthernet6/1
  ! mtu 1500 by default
  ip address 172.1.1.1 255.255.255.0
  crypto engine slot 4/0 outside
!
interface FastEthernet7/13
  ip vrf forwarding coke
  ip address 13.1.1.2 255.255.255.0
!
ip route 100.1.1.1 255.255.255.255 Tunnel1
end
```