



# DF Bit Override Functionality with IPSec Tunnels

---

This feature module describes the DF Bit Override Functionality with IPSec Tunnels feature and contains the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 4
- Command Reference, page 5

## Feature Overview

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to specify whether their router can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether a router is allowed to fragment a packet.

Some customer configurations have hosts that perform the following functions:

- Set the DF bit in packets they send
- Use firewalls that block Internet Control Message Protocol (ICMP) errors from outside the firewall, preventing hosts from learning about the maximum transmission unit (MTU) size outside the firewall
- Use IP Security (IPSec) to encapsulate packets, reducing the available MTU size

Customers whose configurations have hosts that prevent them from learning about their available MTU size can configure their router to clear the DF bit and fragment the packet.



**Note**

---

In compliance with RFC 2401, this feature can be configured globally or per interface. If both levels are configured, the interface configuration will override the global configuration.

---

## Benefits

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPSec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting.

## Restrictions

### Performance Impact

Because each packet is reassembled at the process level, a significant performance impact occurs at a high data rate. Two major caveats are as follows:

- The reassemble queue can fill up and force fragments to be dropped.
- The traffic is slower because of the process switching.

### DF Bit Setting Requirement

If several interfaces share the same crypto map using the local address feature, these interfaces must share the same DF bit setting.

### Feature Availability

This feature is available only for IPSec tunnel mode. (IPSec transport mode is not affected because it does not provide an encapsulating IP header.)

## Related Documents

The following documents provide information related to the DF Bit Override Functionality with IPSec Tunnels feature:

- “Configuring IPSec Network Security” chapter, *Cisco IOS Security Configuration Guide*, Release 12.2
- “IPSec Network Security Commands” chapter, *Cisco IOS Security Command Reference*, Release 12.2

## Supported Platforms

This feature is supported on the following platforms:

- Cisco 800
- Cisco 827
- Cisco 1600
- Cisco 1600R
- Cisco 1700
- Cisco 2600
- Cisco 3620
- Cisco 3640

- Cisco 3660
- Cisco 4000
- Cisco 4500
- Cisco 5200
- Cisco 5300
- Cisco 5400
- Cisco 6400
- Cisco 7100
- Cisco 7200
- Cisco 7500
- Cisco uBR7200
- Cisco uBR900
- Cisco uBR905
- Cisco uBR910

This feature runs on all platforms that support IPSec.

## Supported Standards, MIBs, and RFCs

### Standards

No new or modified standards are supported by this feature.

### MIBs

No new or modified MIBS are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### RFCs

- RFC 2401, *Security Architecture for the Internet Protocol*

## Prerequisites

IPSec must be enabled on your router.


## Configuration Tasks

See the following section for configuration tasks for the DF-Bit Override Functionality with IPSec Tunnels feature:

- Configuring the DF Bit for the Encapsulating Header in Tunnel Mode

## Configuring the DF Bit for the Encapsulating Header in Tunnel Mode

To set the DF bit for the encapsulating header in tunnel mode, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>crypto ipsec df-bit</b> [ <b>clear</b>   <b>set</b>   <b>copy</b> ]	<p>Sets the DF bit for the encapsulating header in tunnel mode for all interfaces.</p> <p>To set the DF bit for a specified interface, use the <b>crypto ipsec df-bit</b> command in interface configuration mode.</p>
	<p> <b>Note</b> DF bit interface configuration settings override all DF bit global configuration settings.</p>

## Verifying DF Bit Setting

To verify the current DF Bit settings on your router, use the **show running-config** command in EXEC mode.

## Configuration Examples

This section provides the following configuration example:

- DF Bit Setting Configuration Example

## DF Bit Setting Configuration Example

In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces *except* Ethernet0 will allow the router to send packets larger than the available MTU size; Ethernet0 will allow the router to fragment the packet.

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des

crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102

!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```

## Command Reference

This section documents the following new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **crypto ipsec df-bit (global)**
- **crypto ipsec df-bit (interface)**

## crypto ipsec df-bit (global)

To set the DF bit for the encapsulating header in tunnel mode to all interfaces, use the **crypto ipsec df-bit** command in global configuration mode.

**crypto ipsec df-bit** [**clear** | **set** | **copy**]

Syntax Description	clear	set	copy
	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.	The router will look in the original packet for the outer DF bit setting. The <b>copy</b> keyword is the default setting.

**Defaults** The default is **copy**.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

**Usage Guidelines** Use the **crypto ipsec df-bit** command in global configuration mode to configure your router to specify the DF bit in an encapsulated header.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as the default.

**Examples** The following example shows how to clear the DF bit on all interfaces:

```
crypto ipsec df-bit clear
```

# crypto ipsec df-bit (interface)

To set the DF bit for the encapsulating header in tunnel mode to a specific interface, use the **crypto ipsec df-bit** command in interface configuration mode.

**crypto ipsec df-bit** [**clear** | **set** | **copy**]

Syntax Description	clear	set	copy
	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.	The router will look in the original packet for the outer DF bit setting. The <b>copy</b> keyword is the default setting.

**Defaults** The default is **copy**.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

**Usage Guidelines** Use the **crypto ipsec df-bit** command in interface configuration mode to configure your router to specify the DF bit in an encapsulated header. This command overrides any existing DF bit global settings.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPsec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as default.

**Examples** In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces *except* Ethernet0 will allow the router to send packets larger than the available MTU size; Ethernet0 will allow the router to fragment the packet.

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des

crypto ipsec df-bit clear
!
!
```

```
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102

!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```