



# DF Bit Override Functionality with IPsec Tunnels

---

**First Published: July 30, 2002**

**Last Updated: March 24, 2011**

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.

## 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 DF Bit Override Functionality with IPsec Tunnels](#)” section on [page 7](#).

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for DF Bit Override Functionality with IPsec Tunnels, page 2](#)
- [Restrictions for DF Bit Override Functionality with IPsec Tunnels, page 2](#)
- [Information About DF Bit Override Functionality with IPsec Tunnels, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [How to Configure DF Bit Override Functionality with IPsec Tunnels, page 3](#)
- [Configuration Example for DF Bit Override Functionality with IPsec Tunnels, page 4](#)
- [Additional References, page 6](#)
- [Feature Information for DF Bit Override Functionality with IPsec Tunnels, page 7](#)



---

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

# Prerequisites for DF Bit Override Functionality with IPsec Tunnels

IPsec must be enabled on your router.

## Restrictions for DF Bit Override Functionality with IPsec Tunnels

### 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.)

## Information About DF Bit Override Functionality with IPsec Tunnels

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.

---

# How to Configure DF Bit Override Functionality with IPsec Tunnels

This section contains the following task:

- [Configuring the DF Bit for the Encapsulating Header in Tunnel Mode, page 3](#)

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

The following task sets the DF bit for the encapsulating header in tunnel mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec df-bit [clear | set | copy]**
4. **interface *type number***
5. **crypto ipsec df-bit [clear | set | copy]** (Optional)
6. **exit**
7. **show running-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto ipsec df-bit [clear   set   copy]</b>  <b>Example:</b> Router(config)# crypto ipsec df-bit set	Sets the DF bit for the encapsulating header in tunnel mode for all interfaces. <ul style="list-style-type: none"> <li>• The <b>clear</b> keyword clears the DF bit in the outer IP header, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.</li> <li>• The <b>set</b> keyword sets the DF bit in the outer IP header, however, the router may fragment the packet if the original packet had the DF bit cleared.</li> <li>• The <b>copy</b> keyword has the router look in the original packet for the outer DF bit setting. The copy keyword is the default setting.</li> </ul>

	Command or Action	Purpose
Step 4	<code>interface type number</code>  <b>Example:</b> Router(config-if)# interface Ethernet0/0	Specifies the interface on which the DF bit is configured and enters interface configuration mode.
Step 5	<code>crypto ipsec df-bit [clear   set   copy]</code>  <b>Example:</b> Router(config-if)# crypto ipsec df-bit clear	(Optional) Sets the DF bit for a specified interface, <b>Note</b> DF bit interface configuration settings override all DF bit global configuration settings.
Step 6	<code>exit</code>  <b>Example:</b> Router(config)# exit	Exits interface configuration mode and enters EXEC mode.
Step 7	<code>show running-config</code>  <b>Example:</b> Router# show running-config	Verifies the current DF Bit settings on your router.

## Configuration Example for DF Bit Override Functionality with IPsec Tunnels

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
```

# Additional References

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Security commands	<a href="#">Cisco IOS Security Command Reference</a>

## MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2401	<a href="#">Security Architecture for the Internet Protocol</a>

## Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for DF Bit Override Functionality with IPsec Tunnels

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

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

**Table 1** Feature Information for DF Bit Override Functionality with IPsec Tunnels

Feature Name	Releases	Feature Information
DF Bit Override Functionality with IPsec Tunnels	12.2(11)T	<p>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.</p> <p>This feature was introduced in Cisco IOS Release 12.2(11)T.</p> <p>The following commands were introduced or modified:  <b>crypto ipsec df-bit (global configuration), crypto ipsec df-bit (interface configuration).</b></p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2002–2011 Cisco Systems, Inc. All rights reserved.

