

tunnel bandwidth

To set the transmit bandwidth used by the tunnel interface, use the **tunnel bandwidth** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

tunnel bandwidth {receive | transmit} *bandwidth*

no tunnel bandwidth

Syntax Description	receive	Specifies the bandwidth to be used to receive packets through the tunnel.
	Note	This keyword is no longer used and will be removed in future releases.
	transmit	Specifies the bandwidth to be used to send packets through the tunnel.
	<i>bandwidth</i>	Bandwidth, in kbps. Range is from 0 to 2147483647. Default is 8000.

Defaults	8000 kbps
----------	-----------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.3(7)T	This command was introduced.

Usage Guidelines	Use the tunnel bandwidth command to specify the capacity of the satellite link.
------------------	--

Examples	The following example shows how to set the satellite tunnel bandwidth to 1000 kbps for transmitting packets using Rate Based Satellite Control Protocol:
----------	--

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel bandwidth transmit 1000
```

Related Commands	Command	Description
	tunnel destination	Specifies the destination for a tunnel interface.
	tunnel mode	Sets the encapsulation mode for a tunnel interface.
	tunnel source	Sets the source address of a tunnel interface.

tunnel checksum

To enable encapsulator-to-decapsulator checksumming of packets on a tunnel interface, use the **tunnel checksum** command in interface configuration mode. To disable checksumming, use the **no** form of this command.

tunnel checksum

no tunnel checksum

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command currently applies to generic routing encapsulation (GRE) only. Some passenger protocols rely on media checksums to provide data integrity. By default, the tunnel does not guarantee packet integrity. By enabling end-to-end checksums, the routers will drop corrupted packets.

Examples

The following example shows how to enable encapsulator-to-decapsulator checksumming of packets for all protocols on the tunnel interface:

```
Router(config-if)# tunnel checksum
```

tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

```
tunnel destination {host-name | ip-address | ipv6-address}
```

```
no tunnel destination
```

Syntax Description

<i>host-name</i>	Name of the host destination.
<i>ip-address</i>	IP address of the host destination expressed in dotted decimal notation.
<i>ipv6-address</i>	IPv6 address of the host destination expressed in IPv6 address format.

Command Default

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The address field was modified to accept an <i>ipv6-address</i> argument to allow IPv6 nodes to be configured as a tunnel destination.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and configure the packet source off of the loopback interface. Refer to the *Cisco IOS AppleTalk, DECnet, ISO CLNS, and Novell IPX Configuration Guide* for more information on AppleTalk Cayman tunneling.

Examples

Tunnel Destination Address for Cayman Tunnel Example

The following example shows how to configure the tunnel destination address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

Tunnel Destination Address for GRE Tunneling Example

The following generic routing encapsulation (GRE) example shows how to configure the tunnel destination address for GRE tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

Tunnel Destination Address for IPv6 Tunnel Example

The following GRE example shows how to configure the tunnel destination address for GRE tunneling of IPv6 packets:

```
Router(config)# interface Tunnel0
Router(config-if)# no ip address
Router(config-if)# ipv6 router isis
Router(config-if)# tunnel source Ethernet0/0
Router(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64
Router(config-if)# tunnel mode gre ipv6
Router(config-if)# exit
!
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
!
Router(config)# ipv6 unicast-routing

Router(config)# router isis
Router(config)# net 49.0000.0000.000a.00
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

tunnel key

To enable an ID key for a tunnel interface, use the **tunnel key** command in interface configuration mode. To remove the ID key, use the **no** form of this command.

tunnel key *key-number*

no tunnel key

Syntax Description

<i>key-number</i>	Number from 0 to 4294967295 that identifies the tunnel key.
-------------------	---

Defaults

No tunnel ID keys are enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command currently applies to generic route encapsulation (GRE) only. Tunnel ID keys can be used as a form of *weak* security to prevent improper configuration or injection of packets from a foreign source.



Note

IP multicast traffic is not supported when a tunnel ID key is configured unless the traffic is process-switched. You must configure the **no ip mroute-cache** command in interface configuration mode on the interface if an ID key is configured. This note applies only to Cisco IOS Release 12.0 and earlier releases.



Note

When GRE is used, the ID key is carried in each packet. We do *not* recommend relying on this key for security purposes.

Examples

The following example shows how to set the tunnel ID key to 3:

```
Router(config-if)# tunnel key 3
```

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the **no** form of this command.

```
tunnel mode { aurp | cayman | dvmrp | eon | gre | gre multipoint | gre ipv6 | ipip
  [decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | ipsec ipv6 | mpls | nos | rbscp }
```

```
no tunnel mode
```

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible Connectionless Network Protocol (CLNS) tunnel.
gre	Generic routing encapsulation (GRE) protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
gre ipv6	GRE tunneling using IPv6 as the delivery protocol.
ipip	IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Tunnel mode is IPsec, and the transport is IPv4.
iptalk	Apple IPTalk encapsulation.
ipv6	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
ipsec ipv6	Tunnel mode is IPsec, and the transport is IPv6.
mpls	Multiprotocol Label Switching (MPLS) encapsulation.
nos	KA9Q/NOS compatible IP over IP.
rbscp	Rate Based Satellite Control Protocol (RBSCP).

Command Default

GRE tunneling

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The aurp , dvmrp , and ipip keywords were added.
11.2	The optional decapsulate-any keyword was added.
12.2(13)T	The gre multipoint keyword was added.

Release	Modification
12.3(7)T	The following keywords were added: <ul style="list-style-type: none"> • gre ipv6 to support GRE tunneling using IPv6 as the delivery protocol. • ipv6 to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • rbscp to support RBSCP.
12.3(14)T	The ipsec ipv4 keyword was added.
12.2(18)SXE	The gre multipoint keyword added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The ipsec ipv6 keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mrouter (multicast) router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPsec profile. Combining mGRE tunnels and IPsec encryption allows a single mGRE interface to support multiple IPsec tunnels, thereby simplifying the size and complexity of the configuration.



Note

GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPsec, over satellite links without breaking the end-to-end model.

IPSec in IPv6 Transport

IPv6 IPsec encapsulation provides site-to-site IPsec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 routers to work as a security gateway, establishes IPsec tunnels between another security gateway router, and provides crypto IPsec protection for traffic from an internal network when being transmitting across the public IPv6 Internet. IPv6 IPsec is very similar to the security gateway model using IPv4 IPsec protection.

Examples**Cayman Tunneling**

The following example shows how to enable Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre
```

IPSec in IPv4 Transport

The following example shows how to configure a tunnel using IPsec encapsulation with IPv4 as the transport mechanism:

```
Router(config)# crypto ipsec profile PROF
Router(config)# set transform tset
Router(config)# interface Tunnel0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel source Loopback0
Router(config-if)# tunnel destination 172.16.1.1
Router(config-if)# tunnel protection ipsec profile PROF
```

IPSec in IPv6 Transport

The following example shows how to configure an IPv6 IPsec tunnel interface:

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Router(config-if)# tunnel destination 10.0.0.1
Router(config-if)# tunnel source Ethernet 0/0
Router(config-if)# tunnel mode ipsec ipv6
Router(config-if)# tunnel protection ipsec profile profile1
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ! Ensures longer packets are fragmented before they are encrypted; otherwise, the
  ! receiving router would have to do the reassembly.
  ip mtu 1416
  ! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
  ! advertise routes that are learned via the mGRE interface back out that interface.
  no ip split-horizon eigrp 1
  no ip next-hop-self eigrp 1
  delay 1000
  ! Sets IPsec peer address to Ethernet interface's public address.
  tunnel source Ethernet0
  tunnel mode gre multipoint
  ! The following line must match on all nodes that want to use this mGRE tunnel.
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
```

RBSCP Tunneling

The following example shows how to enable RBSCP tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a generic routing encapsulation (GRE) or IP-in-IP tunnel interface, use the **tunnel path-mtu-discovery** command in interface configuration mode. To disable PMTUD on a tunnel interface, use the **no** form of this command.

tunnel path-mtu-discovery [**age-timer** {*aging-mins* | **infinite**} | **min-mtu** *mtu-bytes*]

no tunnel path-mtu-discovery

Syntax Description

age-timer	(Optional) Sets a timer to run for a specified interval, in minutes, after which the tunnel interface resets the maximum transmission unit (MTU) of the path to the default tunnel MTU minus 24 bytes for GRE tunnels or minus 20 bytes for IP-in-IP tunnels. <ul style="list-style-type: none"> <i>aging-mins</i>—Number of minutes. Range is from 10 to 30. Default is 10. infinite—Disables the age timer.
min-mtu	(Optional) Specifies the minimum Path MTU across GRE tunnels. <ul style="list-style-type: none"> <i>mtu-bytes</i>—Number of bytes. Range is from 92 to 65535. Default is 92.

Defaults

Path MTU Discovery is disabled for a tunnel interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC5	This command was introduced.
12.0(7)T3	This command was integrated into Cisco IOS Release 12.0(7)T3.
12.2(13)T	The min-mtu keyword and <i>mtu-bytes</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the GRE (or IP-in-IP) tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, no packet fragmentation occurs on the encapsulated packets that travel through the tunnel. Without packet fragmentation, there is a better throughput of TCP connections, and this makes PMTUD a method for maximizing the use of available bandwidth in the network between the endpoints of a tunnel interface.

After PMTUD is enabled, the Don't Fragment (DF) bit of the IP packet header that is forwarded into the tunnel is copied to the IP header of the external IP packets. The external IP packet is the encapsulating IP packet. Adding the DF bit allows the PMTUD mechanism to work on the tunnel path of the tunnel. The tunnel endpoint listens for Internet Control Message Protocol (ICMP) unreachable too-big messages and modifies the IP MTU of the tunnel interface, if required.

When the aging timer is configured, the tunnel code resets the tunnel MTU after the aging timer expires. After the tunnel MTU is reset, a set of full-size packets with the DF bit set is required to trigger the tunnel PMTUD and lower the tunnel MTU. At least two packets are dropped each time the tunnel MTU changes.

When PMTUD is disabled, the DF bit of an external (encapsulated) IP packet is set to zero even if the encapsulated packet has a DF bit set to one.

The *min-mtu* argument sets a low limit on the MTU that can be learned via the PMTUD process. Any ICMP signaling received specifying an MTU less than the minimum MTU configured will be ignored. This feature can be used to prevent a denial of service attack from any node that can send a specially crafted ICMP message to the router, specifying a very small MTU. For more information, see “*Crafted ICMP Messages Can Cause Denial of Service*” at the following URL:

http://www.cisco.com/en/US/products/products_security_advisory09186a0080436587.shtml



Note

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

PMTUD works only on GRE and IP-in-IP tunnel interfaces.

Use the **show interfaces tunnel** command to verify the tunnel PMTUD parameters.

Examples

The following example shows how to enable tunnel PMTUD:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interfaces tunnel	Displays information about the specified tunnel interface.

tunnel rbscp ack_split

To enable TCP acknowledgement (ACK) splitting for Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **tunnel rbscp ack_split** command in interface configuration mode. To disable TCP acknowledgement splitting for RBSCP tunnels, use the **no** form of this command.

tunnel rbscp ack_split *split-size*

no tunnel rbscp ack_split *split-size*

Syntax Description

<i>split-size</i>	Number of ACKs to send for every ACK received. Range is from 1 to 32. Default is 4.
-------------------	---

Defaults

TCP acknowledgement splitting for RBSCP tunnels is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Performance improvements can be made for clear-text TCP traffic using ACK splitting where a number of additional TCP ACKs are generated for each TCP ACK received. TCP will open a congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Use the **tunnel rbscp ack_split** command only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use ACK splitting.

Examples

The following example shows how to enable RBSCP tunnel TCP ACK splitting and configure three ACK packets to be sent for each ACK packet received:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp ack_split 3
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel rbscp delay

To enable the Rate Based Satellite Control Protocol (RBSCP) tunnel delay, use the **tunnel rbscp delay** command in interface configuration mode. To disable RBSCP tunnel delay, use the **no** form of this command.

tunnel rbscp delay

no tunnel rbscp delay

Syntax Description This command has no arguments or keywords.

Defaults RBSCP tunnel delay is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.

Usage Guidelines Use the **tunnel rbscp delay** command only if the RBSCP tunnel has a round-trip time (RTT) over 700 milliseconds.

Examples The following example shows how to enable the RBSCP tunnel delay:

```
Router(config)# interface tunnel 0  
Router(config-if)# tunnel rbscp delay
```

Related Commands	Command	Description
	show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel rbscp input_drop

To configure the input queue size on a Rate Based Satellite Control Protocol (RBSCP) tunnel, use the **tunnel rbscp input_drop** command in interface configuration mode. To restore the default input queue size, use the **no** form of this command.

tunnel rbscp input_drop *bw-delay-products*

no tunnel rbscp input_drop

Syntax Description	<i>bw-delay-products</i>	Number of bandwidth delay products (BDP) bytes that can be queued before packets are dropped on the input side. Range from 1 to 10. Default is 2.
---------------------------	--------------------------	---

Defaults	Input queue size is 2 BDP bytes.
-----------------	----------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.3(7)T	This command was introduced.

Usage Guidelines	<p>Use the tunnel rbscp input_drop command to restrict the amount of data queued by the router. After the configured byte limit is reached, packets that would be encapsulated and sent via the tunnel are dropped on the input side. Congestion control of the satellite link is also provided by this command because the dropped packets will force the end hosts to reduce their sending rate of packets.</p> <p>Use this command in conjunction with the tunnel rbscp long_drop command which allows packets that are waiting in an RBSCP tunnel encapsulation queue to be dropped after a period of time.</p>
-------------------------	---

Examples	The following example shows how to set the RBSCP tunnel queue size to 5 BDP bytes:
-----------------	--

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp input_drop 5
```

Related Commands	Command	Description
	show rbscp	Displays state and statistical information about RBSCP tunnels.
	tunnel rbscp long_drop	Allows packets to be dropped after waiting in the RBSCP tunnel encapsulation queue for too long.

tunnel rbscp long_drop

To allow packets to be dropped that have been queued too long for Rate Based Satellite Control Protocol (RBSCP) tunnel encapsulation, use the **tunnel rbscp long_drop** command in interface configuration mode. To disable the dropping of queued packets, use the **no** form of this command.

tunnel rbscp long_drop

no tunnel rbscp long_drop

Syntax Description This command has no arguments or keywords.

Defaults No queued packets are dropped.

Command Modes Interface configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.

Usage Guidelines The **tunnel rbscp long_drop** command allows the transmitting router to drop packets that have been waiting in the queue for RBSCP tunnel encapsulation for a long time. The period of time after which packets are dropped is determined using the round-trip time (RTT) estimate of the tunnel.

Use this command in conjunction with the **tunnel rbscp input_drop** command which configures the size of the input queue. After the configured byte limit of the input queue is reached, packets are dropped.

Examples The following example shows how to allow packets to be dropped when they have been queued for RBSCP tunnel encapsulation too long:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp long_drop
```

Related Commands	Command	Description
	show rbscp	Displays state and statistical information about RBSCP tunnels.
	tunnel rbscp input_drop	Configures the input queue size on an RBSCP tunnel.

tunnel rbscp report

To report dropped Rate Based Satellite Control Protocol (RBSCP) packets to the Stream Control Transmission Protocol (SCTP), use the **tunnel rbscp report** command in interface configuration mode. To disable dropped-packet reporting to SCTP, use the **no** form of this command.

tunnel rbscp report

no tunnel rbscp report

Syntax Description This command has no arguments or keywords.

Defaults RBSCP dropped-packet reporting is enabled.

Command Modes Interface configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.

Usage Guidelines Use the **tunnel rbscp report** command to provide early reporting of dropped RBSCP packets to SCTP instead of attempting retransmission of the packets at the router. SCTP will inform the end hosts of the dropped packets and allow the end hosts to retransmit the packets. Reporting dropped packets through SCTP provides better throughput because the packet dropping is not assumed to be caused by congestion.

Examples The following example shows how to disable the SCTP drop reporting (reporting is enabled by default):

```
Router(config)# interface tunnel 0
Router(config-if)# no tunnel rbscp report
```

Related Commands	Command	Description
	show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel rbscp window_stuff

To enable TCP window stuffing by increasing the value of the TCP window scale for Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **tunnel rbscp window_stuff** command in interface configuration mode. To restore the default TCP window scale value, use the **no** form of this command.

```
tunnel rbscp window_stuff step-size
```

```
no tunnel rbscp window_stuff
```

Syntax Description	<i>step-size</i>	Increment step size for the TCP window scale. Range is from 1 to 20. Default is 1.
---------------------------	------------------	--

Defaults	TCP window stuffing is disabled.
-----------------	----------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.3(7)T	This command was introduced.

Usage Guidelines	Use the tunnel rbscp window_stuff command to make the sending host believe that the receiving host has a larger window by artificially increasing the TCP window size. RBSCP buffers the additional window and which be configured up to the satellite link bandwidth or the memory available on the router.
-------------------------	---



Note

The actual TCP window size value that is used by the router may be smaller than the configured value because of the available bandwidth.

Examples	The following example shows how to enable TCP window stuffing on the RBSCP tunnel and configure a window size of 2:
-----------------	---

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp window_stuff 2
```

Related Commands	Command	Description
	show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel route-via

To specify the outgoing interface of the tunnel transport, use the **tunnel route-via** command in interface configuration mode. To disable the source address selection, use the **no** form of this command.

tunnel route-via *interface-type interface-number* {**mandatory** | **preferred**}

no tunnel route-via

Syntax Description

<i>interface-type</i>	Indicates the type of interface.
<i>interface-number</i>	Indicates the interface number of the interface configured as the tunnel transport.
mandatory	Drops the traffic if the route is not available.
preferred	If the route is not available, forwards the traffic using any available route.

Command Default

This command is disabled by default. The tunnel transport cannot be routed using a subset of the routing table.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If the **tunnel route-via** *interface-type interface-number* **mandatory** command is configured, and there is no route to the tunnel destination using that interface, a point-to-point tunnel interface will go into a down state.

Examples

The following example shows the options that are available to configure the interfaces of the tunnel transport and route the tunnel transport using a subset of the routing table:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel 0
Router(config-if)# tunnel route-via ethernet0 mandatory
```

Related Commands

Command	Description
debug tunnel route-via	Displays information about the source address selection.
show interfaces tunnel	Displays information about the physical output tunnel interface.

tunnel sequence-datagrams

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnel sequence-datagrams** command in interface configuration mode. To disable this function, use the **no** form of this command.

tunnel sequence-datagrams

no tunnel sequence-datagrams

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command currently applies to generic routing encapsulation (GRE) only. This command is useful when carrying passenger protocols that behave poorly when they receive packets out of order (for example, LLC2-based protocols).

Examples The following example shows how to configure the tunnel to drop datagrams that arrive out of order:

```
Router(config-if)# tunnel sequence-datagrams
```

tunnel source

To set the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source { *ip-address* | *ipv6-address* | *interface-type interface-number* }

no tunnel source

Syntax Description		
<i>ip-address</i>	IP address to use as the source address for packets in the tunnel.	<ul style="list-style-type: none"> In the case of traffic engineering (TE) tunnels it is the control packets that are affected.
<i>ipv6-address</i>	IPv6 address to use as the source address for packets in the tunnel.	
<i>interface-type</i>	Interface type.	
<i>interface-number</i>	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the show interfaces command.	

Command Default No tunnel interface source address is set.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	10.0	This command was introduced.
	12.3(7)T	The address field has been updated to accept IPv6 addresses as the source address to allow an IPv6 node to be used as a tunnel source.
	12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines The source address is either an explicitly defined IP address or the IP address assigned to the specified interface.

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface. This restriction is applicable only for generic routing encapsulation (GRE) tunnels. You can have more than one TE tunnel with the same source and destination address.

When using tunnels to Cayman boxes, you must set the **tunnel source** command to an explicit IP address on the same subnet as the Cayman box, not the tunnel itself.

GRE tunnel encapsulation and deencapsulation for multicast packets are handled by the hardware in PFC3 and 12.2(18)SXF and later releases. Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. You should use secondary addresses on loopback interfaces or create multiple loopback interfaces to ensure the hardware-assisted tunnels do not share a source.

Examples

Cayman Tunnel Example

The following example shows how to set a tunnel source address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.32.164.19
Router(config-if)# tunnel mode cisco1
```

GRE Tunneling Example

The following example shows how to set a tunnel source address for GRE tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.32.164.19
Router(config-if)# tunnel mode gre ip
```

MPLS TE Tunnel Example

The following example shows how to set a tunnel source for a Multiprotocol Label Switching (MPLS) TE tunnel:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel source loopback1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# end
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.

tunnel tos

To configure the type of service (ToS) byte value for a tunnel interface, use the **tunnel tos** command in interface configuration mode. To use the payload ToS byte value (if payload protocol is IP) or 0, use the **no** form of this command.

tunnel tos *tos-bytes*

no tunnel tos

Syntax Description

<i>tos-bytes</i>	ToS byte value from 0 to 255 specified in the encapsulating IP header of a tunneled packet. The default value is 0.
------------------	---

Defaults

The default ToS byte value is the payload ToS byte value (if payload protocol is IP); otherwise, 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **tunnel tos** command is not configured and the packet to be encapsulated is not an IP packet, the tunnel interface will use a default value of 0. If the **tunnel tos** command is not configured and the packet to be encapsulated is an IP packet, the tunnel interface will use the ToS byte value of the inner IP packet header.

Examples

The following example shows how to configure a ToS byte value of 55 on tunnel interface 1:

```
interface tunnel 1
 tunnel tos 55
```

Related Commands

Command	Description
show interfaces tunnel	Lists tunnel interface information.
tunnel ttl	Configures the TTL hop-count value for a tunnel interface.

tunnel ttl

To configure the Time-to-Live (TTL) hop-count value for a tunnel interface, use the **tunnel ttl** command in interface configuration command. To use the payload TTL value (if payload protocol is IP) or 255, use the **no** form of this command.

tunnel ttl *hop-count*

no tunnel ttl

Syntax Description

<i>hop-count</i>	TTL hop-count value from 1 to 255 to be used in the encapsulating IP header of a tunneled packet. The default is 255.
------------------	---

Defaults

The TTL default hop-count value is 255.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure a TTL hop-count value of 200 on tunnel interface 1:

```
interface tunnel 1
 tunnel ttl 200
```

Related Commands

Command	Description
show interfaces tunnel	Lists tunnel interface information.
tunnel tos	Configures the ToS byte value for a tunnel interface.

tunnel vrf

To associate a VPN routing and forwarding (VRF) instance with a specific tunnel destination, interface or subinterface, use the **tunnel vrf** command in global configuration mode or interface configuration mode. To disassociate a VRF from the tunnel destination, use the **no** form of this command.

tunnel vrf *vrf-name*

no tunnel vrf *vrf-name*

Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

Defaults

The default destination is determined by the global routing table.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(33)SRA	Support was added for the Cisco 10000 Series Router. This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB5	This command was integrated into Cisco IOS Release 12.2(31)SB5.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The tunnel source and destination must be in the same VRF.

Either the IP VRF or the tunnel VRF can be set to the global routing table (using the **no ip vrf forwarding** *vrf* command or the **no tunnel vrf** *vrf* command).

The tunnel will be disabled if no route to the tunnel destination is defined. If the tunnel VRF is set, there must be a route to that destination in the VRF.

Cisco 10000 Series Router

The VRF associated with the tunnel through the tunnel vrf command is the same as the VRF associated with the physical interface over which the tunnel sends packets (outer IP packet routing).

Examples

The following example shows how to associate a VRF with a tunnel destination. The tunnel endpoint, 10.5.5.5 will be looked up in the blue VRF.

```
interface tunnel0
 ip vrf forwarding green
 ip address 10.3.3.3 255.255.255.0
 tunnel source loop 0
```

```
tunnel destination 10.5.5.5
tunnel vrf blue
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.
ip vrf forwarding	Associates a VPN VRF instance with an interface or subinterface.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tx-queue-limit

To control the number of transmit buffers available to a specified interface on the multiport communications interface (MCI) and serial communications interface (SCI) cards, use the **tx-queue-limit** command in interface configuration mode.

tx-queue-limit *number*

Syntax Description

<i>number</i>	Maximum number of transmit buffers that the specified interface can subscribe.
---------------	--

Defaults

Defaults depend on the total transmit buffer pool size and the traffic patterns of all the interfaces on the card. Defaults and specified limits are displayed with the **show controllers mci** command.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command should be used only under the guidance of a technical support representative. This command does not have a **no** form.

Examples

The following example shows how to set the maximum number of transmit buffers on the interface to 5:

```
Router(config)# interface ethernet 0
Router(config-if)# tx-queue-limit 5
```

Related Commands

Command	Description
show controllers mci	Displays all information under the MCI card or the SCI.

ubr+

To configure unspecified bit rate (UBR) quality of service (QoS) and specify the output peak cell rate and output minimum guaranteed cell rate for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle member, use the **ubr+** command in the appropriate command mode. To remove the UBR+ parameters, use the **no** form of this command.

```
ubr+ output-pcr output-mcr [input-pcr] [input-mcr]
```

```
no ubr+ output-pcr output-mcr [input-pcr] [input-mcr]
```

Syntax Description

<i>output-pcr</i>	The output peak cell rate (PCR) in kbps.
<i>output-mcr</i>	The output minimum guaranteed cell rate in kbps.
<i>input-pcr</i>	(Optional for SVCs only) The input PCR in kbps. If this value is omitted, the <i>input-pcr</i> equals the <i>output-pcr</i> .
<i>input-mcr</i>	(Optional for SVCs only) The input minimum guaranteed cell rate in kbps. If this value is omitted, the <i>input-mcr</i> equals the <i>output-mcr</i> .

Command Default

UBR QoS is at the maximum line rate of the physical interface.

Command Modes

Interface-ATM-VC configuration (for an ATM PVC on non-DSL interfaces only or an ATM SVC on non-DSL interfaces only)
 VC-class configuration (for a VC class)
 Bundle-VC configuration (for ATM VC bundle members)
 PVC range configuration (for an ATM PVC range)
 PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(3)T	This command was enhanced to support selection of UBR+ QoS and configuration of output PCR and output minimum guaranteed cell rate for ATM VC bundles and VC bundle members.
12.1(5)T	This command was made available in PVC range and PVC-in-range configuration modes.
12.4(2)XA	This command was enabled on DSL ATM interfaces.
12.4(6)T	This command was enabled on DSL ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(1)T	This command was enhanced to support the use of UBR+ on previous generation products.

Usage Guidelines

To configure ATM SVCs with an output PCR and an input PCR that differ from each other, you must expressly configure an output value and an input value using the *output-pcr*, *output-mcr*, *input-pcr*, and *input-mcr* arguments.

Configure QoS parameters using the **ubr**, **ubr+**, or **vbr-nrt** command. The last command that you enter applies to the PVC or SVC that you are configuring.

If the **ubr+** command is not explicitly configured on an ATM PVC or SVC, the VC inherits the following default configuration (in order of precedence):

- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC or SVC itself
- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC ATM subinterface or SVC ATM subinterface
- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC main interface or SVC ATM main interface
- Global default: UBR QoS at the maximum line rate of the PVC or SVC

To use this command in VC-class configuration mode, enter the **vc-class atm** global configuration command before you enter the **ubr+** command. This command has no effect if the VC class that contains the command is attached to a standalone VC (meaning a VC that is not a bundle member).

To use this command in bundle-VC configuration mode, enter the **bundle** command to specify the bundle to which the VC member belongs, then enter bundle configuration mode. Finally, enter the **pvc-bundle** bundle configuration command to add the VC to the bundle as a member.

VCs in a VC bundle use the following configuration inheritance rules (in order of next-highest precedence):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode (with effect of assigned VC-class configuration)
- Subinterface configuration in subinterface mode

DSL ATM interfaces do not support switched virtual circuits (SVCs).

Examples

The following example configures UBR+ PVC on a DSL line:

```
interface atm 0/0
 pvc 4/100
  ubr+ 2304 2304
```

The following example specifies the *output-pcr* argument for an ATM PVC to be 100000 kbps and the *output-mcr* to be 3000 kbps:

```
pvc 1/32
 ubr+ 100000 3000
```

The following example specifies the *output-pcr*, *output-mcr*, *input-pcr*, and *input-mcr* arguments for an ATM SVC to be 10000 kbps, 3000 kbps, 9000 kbps, and 1000 kbps, respectively:

```
svc lion nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 ubr+ 10000 3000 9000 1000
```

Related Commands	Command	Description
	abr	Selects ABR QoS and configures the output peak cell rate and the output minimum guaranteed cell rate for an ATM PVC or VC class.
	broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
	bump	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
	bundle	Creates a bundle or enters bundle configuration mode to modify an existing bundle.
	class	Assigns a VC class to an ATM main interface, subinterface, PVC, SVC, VC bundle, or VC bundle member.
	encapsulation	Sets the encapsulation method used by the interface.
	inarp	Configures the InARP time period for an ATM PVC, VC class, or VC bundle.
	oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a VC class that can be applied to a VC bundle.
	oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
	precedence	Configures precedence levels for a VC class that can be assigned to a VC bundle and thus applied to all VC members of that bundle.
	protect	Configures a VC class with protected group or protected VC status for application to a VC bundle member.
	protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle.
	pvc-bundle	Adds a PVC to a bundle as a member of the bundle and enters bundle-VC configuration mode to configure that PVC bundle member.
	ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
	vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.
	vbr-rt	Configures variable bit rate real-time for VoATM voice connections.

unidirectional

To configure the software-based UDE, use the **unidirectional** command in interface configuration mode. To remove the software-based UDE configuration, use the **no** form of this command.

unidirectional { **send-only** | **receive-only** }

no unidirectional

Syntax Description

send-only	Specifies that the unidirectional transceiver transmits traffic only.
receive-only	Specifies that the unidirectional transceiver receives traffic only.

Defaults

UDE is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

UDE is supported on the interfaces of these switching modules:

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

You do not need to configure software-based UDE on ports where you implement hardware-based UDE.

If an interface is configured with Unidirectional Ethernet or has a receive-only transceiver, UDLD is operationally disabled. Use the **show udld** command to display the configured and operational states of this interface.

When you apply the UDE configuration to an interface, the following warning message is displayed:

Warning!

Enable port unidirectional mode will automatically disable port udld. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

Examples

This example shows how to configure 10-Gigabit Ethernet port 1/1 as a UDE send-only port:

```
Router(config-if)# unidirectional send-only
```

Warning!

Enable port unidirectional mode will automatically disable port udd. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

This example shows how to configure 10-Gigabit Ethernet port 1/2 as a UDE receive-only port:

```
Router(config-if)# unidirectional receive-only
```

Warning!

Enable port unidirectional mode will automatically disable port udd. You must manually ensure that the unidirectional link does not create a spanning tree loop in the network.

Enable 13 port unidirectional mode will automatically disable ip routing on the port. You must manually configure static ip route and arp entry in order to route ip traffic.

Related Commands

Command	Description
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
show interfaces unidirectional	Displays the operational state of an interface with a receive-only transceiver.

upgrade fpd auto

To configure the router to automatically upgrade the current FPD images on a SPA or any FPD-capable cards when an FPD version incompatibly is detected, enter the **upgrade fpd auto** global configuration command. To disable automatic FPD image upgrades, use the **no** form of this command.

upgrade fpd auto

no upgrade fpd auto

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default if your router has any installed SPAs or FPD-capable cards. The router checks the FPD image during bootup or after an insertion of a SPA or FPD-capable card. If the router detects an incompatibility between an FPD image and a SPA or FPD-capable card, an automatic FPD upgrade attempt occurs unless the user has disabled automatic FPD upgrades by entering the **no upgrade fpd auto** command. The **upgrade fpd path** command can be used to direct the router to search for the FPD image package at another location (such as an FTP or TFTP server) when an FPD incompatibility is detected.

Cisco 7200 VXR

The router searches the disk2: Flash Disk for the FPD image package file when an FPD incompatibility is detected and **upgrade fpd auto** is enabled.

Cisco 7304

The router searches the primary Flash file system (disk0:) for the FPD image package file when an FPD incompatibility is detected and **upgrade fpd auto** is enabled.

Cisco 7600 Series, Cisco 12000 Series

The router searches all of its Flash file systems for the FPD image package when an FPD incompatibility is detected and **upgrade fpd auto** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD3	This command was integrated into Cisco IOS Release 12.4(4)XD3.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

This command is enabled by default. In most cases, this default configuration should be retained.

If this command is disabled but an FPD upgrade is required for a SPA, the **upgrade hw-module subslot** command can be used to upgrade the SPA FPD image manually after the SPA is disabled because of the existing FPD incompatibility.

If this command is disabled but an FPD upgrade is required for an FPD-capable card on the Cisco 7200 VXR router, you cannot upgrade the card manually. Select the FPD image package and download it to the disk2: Flash Disk, enable the automatic FPD upgrade by using the **upgrade fpd auto** command, and reboot the router.

Upgrading the FPD image on a SPA or FPD-capable card places the SPA or card offline while the upgrade is taking place. The time required to complete an FPD image upgrade can be lengthy. The **show upgrade fpd progress** command can be used to gather more information about estimated FPD download times for a particular SPA.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), refer to the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*.

Examples**Cisco 7200 VXR**

The following example shows the output that is displayed when a VSA in slot 0 requires an FPD image upgrade and the **upgrade fpd auto** command is enabled. The required FPD image is automatically upgraded.

```
*Apr 10 00:37:42.859: %FPD_MGMT-3-INCOMP_IMG_VER: Incompatible VSA (FPD ID=1) image
version detected for VSA card in slot 0. Detected version = 0.9, minimum required version
= 0.10. Current HW version = 0.0.
*Apr 10 00:37:42.859: %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically upgrade the
FPD image(s) for VSA card in slot 0. Use 'show upgrade fpd progress' command to view the
upgrade progress ...
*Apr 10 00:37:43.023: %FPD_MGMT-6-BUNDLE_DOWNLOAD: Downloading FPD image bundle for VSA
card in slot 0 ...
*Apr 10 00:37:44.543: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
VSA card in slot 0 = 00:03:00.
*Apr 10 00:37:44.639: %FPD_MGMT-6-UPGRADE_START: VSA (FPD ID=1) image upgrade in progress
for VSA card in slot 0. Updating to version 0.10. PLEASE DO NOT INTERRUPT DURING THE
UPGRADE PROCESS (estimated upgrade completion time = 00:03:00) ..*****
*Apr 10 00:38:57.483: %FPD_MGMT-6-UPGRADE_PASSED: VSA (FPD ID=1) image in the VSA card in
slot 0 has been successfully updated from version 0.9 to version 0.10. Upgrading time =
00:01:12.844
*Apr 10 00:38:57.483: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the
required FPD images have been completed for VSA card in slot 0. Number of
successful/failure upgrade(s): 1/0.
*Apr 10 00:38:57.483: %FPD_MGMT-5-CARD_POWER_CYCLE: VSA card in slot 0 is being power
cycled for the FPD image upgrade to take effect.
```

Cisco 7304

The following example shows the output displayed when a SPA requires an FPD image upgrade and the **upgrade fpd auto** command is enabled. The incompatible FPD image is automatically upgraded.

```
% Uncompressing the bundle ... [OK]
*Jan 13 22:38:47:%FPD_MGMT-3-INCOMP_FPD_VER:Incompatible 4FE/2GE FPGA (FPD ID=1) image
version detected for SPA-4FE-7304 card in subslot 2/0. Detected version = 4.12, minimal
required version = 4.13. Current HW version = 0.32.
*Jan 13 22:38:47:%FPD_MGMT-5-FPD_UPGRADE_ATTEMPT:Attempting to automatically upgrade the
FPD image(s) for SPA-4FE-7304 card in subslot 2/0 ...

*Jan 13 22:38:47:%FPD_MGMT-6-BUNDLE_DOWNLOAD:Downloading FPD image bundle for SPA-4FE-7304
card in subslot 2/0 ...
```

■ upgrade fpd auto

```
*Jan 13 22:38:49:%FPD_MGMT-6-FPD_UPGRADE_TIME:Estimated total FPD image upgrade time for
SPA-4FE-7304 card in subslot 2/0 = 00:06:00.
*Jan 13 22:38:49:%FPD_MGMT-6-FPD_UPGRADE_START:4FE/2GE FPGA (FPD ID=1) image upgrade in
progress for SPA-4FE-7304 card in subslot 2/0. Updating to version 4.13. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:06:00)
...[.....]
(part of the output has been removed for brevity)
.....]
.....]
SUCCESS - Completed XSVF execution.

*Jan 13 22:44:33:%FPD_MGMT-6-FPD_UPGRADE_PASSED:4FE/2GE FPGA (FPD ID=1) image upgrade for
SPA-4FE-7304 card in subslot 2/0 has PASSED. Upgrading time = 00:05:44.108
*Jan 13 22:44:33:%FPD_MGMT-6-OVERALL_FPD_UPGRADE:All the attempts to upgrade the required
FPD images have been completed for SPA-4FE-7304 card in subslot 2/0. Number of
successful/failure upgrade(s):1/0.
*Jan 13 22:44:33:%FPD_MGMT-5-CARD_POWER_CYCLE:SPA-4FE-7304 card in subslot 2/0 is being
power cycled for the FPD image upgrade to take effect.
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

upgrade fpd path

To configure the router to search for an FPD image package file in a location other than the default router Flash file system during an automatic FPD upgrade, enter the **upgrade fpd path** command in global configuration mode. To return to the default setting of the router searching for the FPD image package file in the router Flash file systems when an automatic FPD upgrade is triggered, use the **no** form of this command.

upgrade fpd path *fpd-pkg-dir-url*

no upgrade fpd path *fpd-pkg-dir-url*

Syntax Description

fpd-pkg-dir-url Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include **disk0**, **slot0**, **tftp**, or **ftp**) and followed by the path to the FPD image package file. It is important to note that the name of the FPD image package file should not be specified as part of *fpd-pkg-dir-url*; Cisco IOS will automatically download the correct FPD image package file once directed to the proper location.

It is important to note that the last character of the *fpd-pkg-dir-url* is always a “/”.

Defaults

The **upgrade fpd path** command is used to specify a new location for a router to locate the FPD image package file, if you want to store the FPD image package file in a location other than the default router Flash file system for automatic FPD upgrades. The default locations the router searches are as follows:

Cisco 7200 VXR

The router searches the disk2: Flash Disk for the FPD image package file when an FPD incompatibility is detected and **upgrade fpd auto** is enabled.

Cisco 7304

The router searches the primary Flash file system (disk0:) for the FPD image package file when an FPD incompatibility is detected and **upgrade fpd auto** is enabled.

Cisco 7600 Series, Cisco 12000 Series

The router searches all of its Flash file systems for the FPD image package when an FPD incompatibility is detected and **upgrade fpd auto** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(4)XD3	This command was integrated into Cisco IOS Release 12.4(4)XD3.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

It is important to note that the last character of the *fpd-pkg-dir-url* is always a “/”. This path points users to the directory that stores the file, but not the file itself.

When specifying the path to the location of the new FPD image package file, do not include the file name in the path. The Cisco IOS will automatically download the correct FPD image package file once directed to the proper location, even if multiple FPD image package files of different versions are stored in the same location.

If the **upgrade fpd path** command is not entered, the router searches the default router Flash file system for the FPD image.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), refer to the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*.

Examples

In the following example, the FPD image package file that is stored on the TFTP server using the path *johnstftpserver/fpdfiles* is scanned for the latest FPD image package file when an automatic FPD upgrade occurs:

```
upgrade fpd path tftp://johnstftpserver/fpdfiles/
```

In the following example, the FPD package file that is stored on the FTP server using the path *johnsftpserver/fpdfiles* is scanned for the latest FPD image package when an automatic FPD upgrade occurs. In this example, *john* is the username and *XXXXXXXX* is the FTP password:

```
upgrade fpd path ftp://john:XXXXXXXX@johnsftpserver/fpdfiles/
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.

Command	Description
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

upgrade fpga

To set router behavior regarding handling of FPGA mismatches after FPGA mismatches are detected, use the **upgrade fpga** command in privileged EXEC mode.

upgrade fpga [**force** | **prompt**]

no upgrade fpga

Syntax Description

force	If the force option is entered, an FPGA upgrade will be forced on the system if an FPGA mismatch is detected.
prompt	If the prompt option is entered, the user will be prompted to upgrade the FPGA when an FPGA mismatch is detected.

Defaults

Before Cisco IOS Release 12.2(20)S6, users were automatically prompted for an FPGA upgrade when an FPGA version mismatch was detected.

In Cisco IOS Release 12.2(20)S6, the default setting became **no upgrade fpga**. By default, FPGA is not upgraded when an FPGA version mismatch is detected and the user is not prompted to upgrade the FPGA, although it is important to note that a message indicating the FPGA mismatch is displayed on the console. Users who want to upgrade FPGA must use the **upgrade fpga all** command to manually perform the upgrade when the default settings are set.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S4	The upgrade fpga prompt command was introduced.
12.2(20)S6	The no upgrade fpga command was introduced and became the default setting. The force option was introduced. The no upgrade fpga prompt command behavior was changed. The no upgrade fpga prompt configuration no longer automatically begins an FPGA upgrade when an FPGA mismatch is detected.

Usage Guidelines

Note that **no upgrade fpga** is the default setting starting in Cisco IOS Release 12.2(20)S6. See the Defaults section of this command reference for additional information on the changes to the default setting in Cisco IOS Release 12.2(20)S6.

This command can be used to upgrade all of the FPGAs in a Cisco 7304 router except for the SPA FPGA. The SPA FPGA is upgraded using an FPD image package.

An FPGA match check is automatically run by the Cisco 7304 router during system bootup or after a piece of hardware with FPGA is installed into an operating Cisco 7304 router. This command defines the behavior for a router after an FPGA mismatch is detected during one of these FPGA match checks. When the default setting of **no upgrade fpga** is maintained, FPGA is not upgraded when an FPGA


```
00:00:08:%PLATFORM-4-FPGA_MISMATCH:FPGA image in slot 5 (name = 6T3, hardware version = 03.03, current fpga version = 00.20) does not match the FPGA image in Cisco IOS software (version 00.21). Approximate time to update the FPGA image is 12 minutes.
```

Related Commands

Command	Description
show c7300	Displays the types of hardware installed in a Cisco 7304 router, including the current FPGA version and the bundled FPGA version.
show diag	Displays hardware information for any slot or the chassis.
show upgrade fpga progress	Displays the progress of an FPGA upgrade.
upgrade fpga all	Manually upgrades all of the FPGAs for all of the installed hardware on the Cisco 7304 router.

upgrade fpga all

To manually start the Field-Programmable Gate Array (FPGA) image update process, use the **upgrade fpga all** command in privileged EXEC mode.

upgrade fpga all

Syntax Description This command has no arguments or keywords.

Defaults No default behaviors or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(10)EX	This command was introduced.
	12.2(11)YZ	Support was added for the 7300-CC-PA.
	12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2 S.
	12.2(20)S6	The prompt asking users if they would like to reload the line card to complete the FPGA upgrade process was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Use this command to manually start the FPGA image update process. Automatic FPGA version checking is performed during every system startup for all line cards, processors, and jacket cards in the system. Automatic FPGA version checking is also performed for hardware after insertion of that hardware during an online insertion and removal (OIR).

Traffic disruption for traffic on the hardware upgrading FPGA usually occurs during FPGA upgrades. If you are going to upgrade FPGA using this command, keep this fact in mind.

Before Cisco IOS Release 12.2(20)S6, the hardware that had the FPGA upgrade would automatically be reloaded as the final procedure of the FPGA upgrade. In Cisco IOS Release 12.2(20)S6 onward, the user sees a prompt asking if the hardware should be reloaded to complete the FPGA upgrade. The user can choose to skip the hardware reload at the current time if desired, but the FPGA upgrade is not complete until the hardware is reloaded. If the user chooses not to reload the hardware that is getting the FPGA upgrade, the hardware will have to be reloaded using the **hw-module slot-number stop** command followed by the **hw-module slot-number start** command if the hardware is not a processor. If the hardware is a processor, the router must be reloaded.

In cases where the FPGA upgrade is performed but the hardware is not reloaded, users should note that the bundled FPGA version will be transferred to Flash memory but not to the hardware. Therefore, if the **show c7300** command is entered to see FPGA versions after an FPGA upgrade has been performed but


```

Slot 4 LC FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM

FPGA flash update in progress
Erasing (this may take a while)...
Programming...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone
  Comparing with the source file...Passed

Slot 4 LC FPGA successfully updated from version 0.13 to version 0.12

Slot 4 linecard reset after FPGA update...

Slot 4 linecard successfully reset
00:11:37:%PLATFORM-6-FPGAUPDSUCCESS:Slot 4 LC FPGA successfully update from version 0.13
to 0.12.

```

Related Commands

Command	Description
show c7300	Displays the types of hardware (processors, line cards, jacket cards, and so on) installed in the Cisco 7304 router slots, including the bundled, Flash, and current FPGA versions.
show diag	Displays hardware information for any slot or the chassis.
upgrade rom-monitor default	Configures a particular ROM monitor image as the default ROMmon image.
upgrade rom-monitor file	Upgrades the ROM monitor.

upgrade hw-module slot

**Note**

The **upgrade hw-module slot** command is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the **upgrade hw-module slot fpd file** command.

**Note**

The **upgrade hw-module slot** command is not available in Cisco IOS Release 12.4(15)T and later Cisco IOS 12.4T releases. It is replaced by the **upgrade hw-module slot fpd file** command.

To manually upgrade the current FPD image package on a SIP or any FPD-capable cards, enter the **upgrade hw-module slot** command in privileged EXEC mode.

Cisco 7200 VXR

```
upgrade hw-module slot {slot | npe} file file-url
```

Cisco 7600 Series

```
upgrade hw-module slot slot file file-url [force]
```

Syntax Description

<i>slot</i>	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide. For slot numbering in the Cisco 7200 VXR router, refer to refer to the <i>Cisco 7200 VXR Installation and Configuration Guide</i> .
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.
file	Specifies that a file will be downloaded.
<i>file-url</i>	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0 , slot0 , tftp , or ftp) and followed by the path to the FPD image package file.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package file on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Defaults**Cisco 7200 VXR**

No default behavior or values.

Cisco 7600 Series

No default behavior or values, although it is important to note that the router containing the SIP is configured, by default, to upgrade the FPD images when it detects a version incompatibility between the FPD image on the SIP and the FPD image required to run the SPA with the running Cisco IOS image. The **upgrade hw-module slot** command is used to manually upgrade the FPD images; therefore, the

upgrade hw-module slot command should only be used when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs or when the automatic upgrade default configuration has been manually disabled. The **no upgrade fpd auto** command can be entered to disable automatic FPD upgrades.

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD, and the npe keyword was added.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the upgrade hw-module slot fpd file command.
12.4(15)T	This command was removed. It is not available in Cisco IOS Release 12.4(15)T and later Cisco IOS 12.4T releases. It is replaced by the upgrade hw-module slot fpd file command.

Usage Guidelines

Cisco 7200 VXR

This command is used to manually upgrade FPD images. Note that for a manual FPD upgrade to take effect on the NPE-G2, you must power cycle the router. The router will *not* use the new version of the NPE-G2 FPD image if you reload the router without a power cycle. Other FPD-capable cards require only a router reload after a manual FPD upgrade, not a router power cycle.

Cisco 7600 Series

This command is used to manually upgrade the FPD images on a SIP. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade detects and automatically upgrades all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SIP was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SIP and all the SPAs in the SIP offline. The time required to complete an FPD image upgrade can be lengthy. The **show upgrade fpd progress** command can be used to gather more information about estimated FPD image download times for a particular SIP.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*. For FPD upgrades on the Cisco 7200 VXR router, see the *Field-Programmable Device Upgrades* feature guide.

Examples

Cisco 7200 VXR

The following example shows a sample manual FPD upgrade of the FPD image package for the NPE-G2:

```
Router# upgrade hw-module slot npe file
tftp://mytftpserver/myname/myfpdpkg/c7200-fpd-pkg.124-4.XD.pkg
% The following FPD(s) will be updated for NPE-G2 (H/W ver = 0.0) in NPE slot:

=====
Field Programmable   Current      Upgrade     Estimated
Device: "ID-Name"   Version      Version      Upgrade Time
=====
1-NPEG2 I/O FPGA      0.7          0.8          00:01:00
=====

% NOTES:
- Use 'show upgrade fpd progress' command to view the progress of the FPD
  upgrade.
- The target card will be automatically reload after the upgrade
  operation. This reload will interrupt normal operation of the card. If
  necessary, ensure that appropriate actions have been taken to redirect
  card traffic before starting the FPD upgrade.

% Are you sure that you want to perform this operation? [no]: yes
% Initiating the upgrade operation on the target card ...

Router#
*Jan 1 00:33:41.611: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
NPE-G2 card in NPE slot = 00:01:00.
*Jan 1 00:33:41.615: %FPD_MGMT-6-UPGRADE_START: NPEG2 I/O FPGA (FPD ID=1) image upgrade
in progress for NPE-G2 card in NPE slot. Updating to version 0.8. PLEASE DO NOT INTERRUPT
DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...

*Jan 1 00:34:14.279: %FPD_MGMT-6-UPGRADE_PASSED: NPEG2 I/O FPGA (FPD ID=1) image in the
NPE-G2 card in NPE slot has been successfully updated from version 0.7 to version 0.8.
Upgrading time = 00:00:32.664
*Jan 1 00:34:14.279: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the
required FPD images have been completed for NPE-G2 card in NPE slot. Number of
successful/failure upgrade(s): 1/0.
*Jan 1 00:34:14.279: %FPD_MGMT-5-CARD_POWER_CYCLE: NPE-G2 card in NPE slot is being power
cycled for the FPD image upgrade to take effect.
```

Cisco 7600 Series

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module slot 4 file disk0:c7600-fpd-pkg.122-18.SXE.pkg

% The following FPD(s) will be upgraded for 7600-SIP-200 (H/W ver = 0.550) in slot 4:

=====
Field Programmable   Current      Upgrade     Estimated
Device:"ID-Name"   Version      Version      Upgrade Time
=====
5-ROMMON              1.1          1.2          00:02:00
=====
```

```

% Are you sure that you want to perform this operation? [no]:y
% Restarting the target card in slot 4 for FPD image upgrade. Please wait ...

Router#
Mar 25 16:39:37:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:39:40:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_TIME:Estimated total FPD image upgrade time for
7600-SIP-200 card in slot 4 = 00:02:00.
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_START:ROMMON (FPD ID=5) image upgrade in progress for
7600-SIP-200 card in slot 4. Updating to version 1.2. PLEASE DO NOT INTERRUPT DURING THE
UPGRADE PROCESS (estimated upgrade completion time = 00:02:00) ...
Mar 25 16:39:39:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:39:40:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:39:40:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:39:40:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
Mar 25 16:39:46:%FPD_MGMT-6-UPGRADE_PASSED:ROMMON (FPD ID=5) image in the 7600-SIP-200
card in slot 4 has been successfully updated from version 1.1 to version 1.2. Upgrading
time = 00:00:06.000
Mar 25 16:39:46:%FPD_MGMT-6-OVERALL_UPGRADE:All the attempts to upgrade the required FPD
images have been completed for 7600-SIP-200 card in slot 4. Number of successful/failure
upgrade(s):1/0.
Mar 25 16:39:47:%FPD_MGMT-5-CARD_POWER_CYCLE:7600-SIP-200 card in slot 4 is being power
cycled for the FPD image upgrade to take effect.
Mar 25 16:39:47:%OIR-6-REMCARD:Card removed from slot 4, interfaces disabled
Mar 25 16:39:47:%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
Mar 25 16:40:38:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
Mar 25 16:40:40:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:40:41:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:40:41:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online

```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.

Command	Description
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-module slot fpd file

To manually upgrade the current FPD image package on a SIP or any FPD-capable cards, use the **upgrade hw-module slot fpd file** command in privileged EXEC mode.

Cisco 7200 VXR

```
upgrade hw-module slot {slot | npe} fpd file file-url
```

Cisco 7600 Series

```
upgrade hw-module slot slot fpd file file-url [force]
```

Syntax Description

<i>slot</i>	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide. For slot numbering in the Cisco 7200 VXR router, refer to refer to the <i>Cisco 7200 VXR Installation and Configuration Guide</i> .
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.
<i>file-url</i>	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0 , slot0 , tftp , or ftp) and followed by the path to the FPD image package file.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package file on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Defaults

Cisco 7200 VXR

No default behavior or values.

Cisco 7600 Series

No default behavior or values, although it is important to note that the router containing the SIP is configured, by default, to upgrade the FPD images when it detects a version incompatibility between the FPD image on the SIP and the FPD image required to run the SPA with the running Cisco IOS image. Manual upgrade of FPD images is recommended only when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs, or when the automatic upgrade default configuration has been manually disabled. The **no upgrade fpd auto** command can be entered to disable automatic FPD upgrades.

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced. This command replaces the upgrade hw-module slot command.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines**Cisco 7200 VXR**

This command is used to manually upgrade FPD images. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. Note that for a manual FPD upgrade to take effect on the NPE-G2, you must power cycle the router. The router will *not* use the new version of the NPE-G2 FPD image if you reload the router without a power cycle. Other FPD-capable cards require only a router reload after a manual FPD upgrade, not a router power cycle.

Cisco 7600 Series

This command is used to manually upgrade the FPD images on a SIP. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade detects and automatically upgrades all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SIP was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SIP and all the SPAs in the SIP offline. The time required to complete an FPD image upgrade can be lengthy. The **show upgrade fpd progress** command can be used to gather more information about estimated FPD image download times for a particular SIP.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*. For FPD upgrades on the Cisco 7200 VXR router, see the *Field-Programmable Device Upgrades* feature guide.

Examples**Cisco 7200 VXR**

The following example shows a sample manual FPD upgrade of the FPD image package for the NPE-G2:

```
Router# upgrade hw-module slot npe fpd file
tftp://mytftpserver/myname/myfpd/pkg/c7200-fpd-pkg.124-4.XD.pkg

% The following FPD(s) will be updated for NPE-G2 (H/W ver = 0.0) in NPE slot:

=====
Field Programmable   Current   Upgrade   Estimated
Device: "ID-Name"   Version   Version   Upgrade Time
=====
1-NPEG2 I/O FPGA    0.7       0.8       00:01:00
=====

% NOTES:
- Use 'show upgrade fpd progress' command to view the progress of the FPD
  upgrade.
```

- The target card will be automatically reload after the upgrade operation. This reload will interrupt normal operation of the card. If necessary, ensure that appropriate actions have been taken to redirect card traffic before starting the FPD upgrade.

```
% Are you sure that you want to perform this operation? [no]: yes
% Initiating the upgrade operation on the target card ...
```

```
Router#
```

```
*Jan 1 00:33:41.611: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for NPE-G2 card in NPE slot = 00:01:00.
```

```
*Jan 1 00:33:41.615: %FPD_MGMT-6-UPGRADE_START: NPEG2 I/O FPGA (FPD ID=1) image upgrade in progress for NPE-G2 card in NPE slot. Updating to version 0.8. PLEASE DO NOT INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...
```

```
*Jan 1 00:34:14.279: %FPD_MGMT-6-UPGRADE_PASSED: NPEG2 I/O FPGA (FPD ID=1) image in the NPE-G2 card in NPE slot has been successfully updated from version 0.7 to version 0.8. Upgrading time = 00:00:32.664
```

```
*Jan 1 00:34:14.279: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the required FPD images have been completed for NPE-G2 card in NPE slot. Number of successful/failure upgrade(s): 1/0.
```

```
*Jan 1 00:34:14.279: %FPD_MGMT-5-CARD_POWER_CYCLE: NPE-G2 card in NPE slot is being power cycled for the FPD image upgrade to take effect.
```

Cisco 7600 Series

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module slot 4 fpd file disk0:c7600-fpd-pkg.122-18.SXE.pkg
```

```
% The following FPD(s) will be upgraded for 7600-SIP-200 (H/W ver = 0.550) in slot 4:
```

```
=====
Field Programmable   Current      Upgrade      Estimated
Device:"ID-Name"    Version      Version      Upgrade Time
=====
5-ROMMON             1.1          1.2          00:02:00
=====
```

```
% Are you sure that you want to perform this operation? [no]:y
```

```
% Restarting the target card in slot 4 for FPD image upgrade. Please wait ...
```

```
Router#
```

```
Mar 25 16:39:37:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
```

```
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
```

```
Mar 25 16:39:40:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
```

```
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_TIME:Estimated total FPD image upgrade time for 7600-SIP-200 card in slot 4 = 00:02:00.
```

```
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_START:ROMMON (FPD ID=5) image upgrade in progress for 7600-SIP-200 card in slot 4. Updating to version 1.2. PLEASE DO NOT INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:02:00) ...
```

```
Mar 25 16:39:39:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
```

```
Mar 25 16:39:40:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
```

```
SLOT 1:Mar 26 00:39:40:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
```

```
Mar 25 16:39:40:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

```
Mar 25 16:39:46:%FPD_MGMT-6-UPGRADE_PASSED:ROMMON (FPD ID=5) image in the 7600-SIP-200 card in slot 4 has been successfully updated from version 1.1 to version 1.2. Upgrading time = 00:00:06.000
```

```
Mar 25 16:39:46:%FPD_MGMT-6-OVERALL_UPGRADE:All the attempts to upgrade the required FPD images have been completed for 7600-SIP-200 card in slot 4. Number of successful/failure upgrade(s):1/0.
```

upgrade hw-module slot fpd file

```

Mar 25 16:39:47:%FPD_MGMT-5-CARD_POWER_CYCLE:7600-SIP-200 card in slot 4 is being power
cycled for the FPD image upgrade to take effect.
Mar 25 16:39:47:%OIR-6-REMCARD:Card removed from slot 4, interfaces disabled
Mar 25 16:39:47:%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
Mar 25 16:40:38:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
Mar 25 16:40:40:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:40:41:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:40:41:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online

```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module subslot fpd file	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-module subslot


Note

The **upgradehw-module subslot** command is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the **upgrade hw-module subslot fpd file** command.


Note

The **upgrade hw-module subslot** command is not available in Cisco IOS Release 12.2(33)SB and later Cisco IOS 12.2SB releases. It is replaced by the **upgrade hw-module subslot fpd file** command.

To manually upgrade the current FPD image package on a SPA, use the **upgrade hw-module subslot** command in privileged EXEC mode.

Cisco 7304

```
upgrade hw-module subslot slot/subslot file file-url [reload]
```

Cisco 7600 Series, Cisco 12000 Series

```
upgrade hw-module subslot slot/subslot file file-url [force]
```

Syntax Description

<i>slot</i>	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
<i>subslot</i>	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
file	Specifies that a file will be downloaded.
<i>file-url</i>	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0, slot0, tftp, or ftp) and followed by the path to the FPD image package file.
reload	(Optional) Reloads the SPA to complete the FPD upgrade.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Defaults

No default behavior or values, although it is important to note that the router containing the SPA is configured, by default, to upgrade the FPD images when it detects a version incompatibility between a the FPD image on the SPA and the FPD image required to run the SPA with the running Cisco IOS image. The **upgrade hw-module subslot** command is used to manually upgrade the FPD images; therefore, the

upgrade hw-module subslot command should only be used when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs or when the automatic upgrade default configuration has been manually disabled. The **no upgrade fpd auto** command can be entered to disable automatic FPD upgrades.

Cisco 7304

By default the SPA is not reloaded to complete the FPD upgrade unless the **reload** option is entered. Reloading the SPA drops all traffic traversing that SPA's interfaces. If you want to reload the SPA later to complete the upgrade, do not enter the **reload** option and perform OIR of the SPA later to complete the FPD upgrade.

Cisco 7600 Series, Cisco 12000 Series

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(25)S3	The force option was removed and replaced by the reload option (Cisco 7304 router).
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the upgrade hw-module subslot fpd file command.
12.2(33)SB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SB and later Cisco IOS 12.2SB releases. It is replaced by the upgrade hw-module slot fpd file command.

Usage Guidelines

This command is used to manually upgrade the FPD images on a SPA. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade will detect and automatically upgrade all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SPA was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SPA offline. The time required to complete an FPD image upgrade can be lengthy. The **show upgrade progress** command can be used to gather more information about estimated FPD download times for a particular SPA.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Configuration Guide*, the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*, or the *Cisco 12000 Series Router SIP and SPA Software Configuration Guide*.

Examples

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module subslot 2/0 file disk0:spa_fpd.122-20.S2.pkg

% Uncompressing the bundle ... [OK]

% The following FPD(s) will be upgraded for card in subslot 2/0 :

=====
Field Programmable   Current   Upgrade   Estimated
Device:"ID-Name"     Version   Version   Upgrade Time
=====
1-Data & I/O FPGA    4.12     4.13     00:06:00
=====

% Are you sure that you want to perform this operation? [no]:y
% Restarting the target card (subslot 2/0) for FPD image upgrade. Please wait ...

Router#
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_TIME:Estimated total FPD image upgrade time for
SPA-4FE-7304 card in subslot 2/0 = 00:06:00.
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_START:4FE/2GE FPGA (FPD ID=1) image upgrade in
progress for SPA-4FE-7304 card in subslot 2/0. Updating to version 4.13. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:06:00)
...[.....(part of the output has been removed for brevity)....]
.....]
SUCCESS - Completed XSVF execution.

*Jan 14 00:42:59:%FPD_MGMT-6-FPD_UPGRADE_PASSED:4FE/2GE FPGA (FPD ID=1) image upgrade for
SPA-4FE-7304 card in subslot 2/0 has PASSED. Upgrading time = 00:05:42.596
*Jan 14 00:42:59:%FPD_MGMT-6-OVERALL_FPD_UPGRADE:All the attempts to upgrade the required
FPD images have been completed for SPA-4FE-7304 card in subslot 2/0. Number of
successful/failure upgrade(s):1/0.
*Jan 14 00:42:59:%FPD_MGMT-5-CARD_POWER_CYCLE:SPA-4FE-7304 card in subslot 2/0 is being
power cycled for the FPD image upgrade to take effect.
```

Related Commands

Command	Description
show hw-module slot fpd	Displays the current versions of FPD image files for all of the active SIPs on a router.
show hw-module subslot fpd	Displays the FPD version on each SPA in the router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.

Command	Description
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-module subslot fpd file

To manually upgrade the current FPD image package on a SPA, use the **upgrade hw-module subslot fpd file** command in privileged EXEC mode.

Cisco 7304

```
upgrade hw-module subslot slot/subslot fpd file file-url [reload]
```

Cisco 7600 Series

```
upgrade hw-module subslot slot/subslot fpd file file-url [force]
```

Syntax Description

<i>slot</i>	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
<i>subslot</i>	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
<i>file-url</i>	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0 , slot0 , tftp , or ftp) and followed by the path to the FPD image package file.
reload	(Optional) Reloads the SPA to complete the FPD upgrade.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Defaults

No default behavior or values, although it is important to note that the router containing the SPA is configured, by default, to upgrade the FPD images when it detects a version incompatibility between a the FPD image on the SPA and the FPD image required to run the SPA with the running Cisco IOS image. Manual upgrade of FPD images is recommended only when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs, or when the automatic upgrade default configuration has been manually disabled. The **no upgrade fpd auto** command can be entered to disable automatic FPD upgrades.

Cisco 7304

By default the SPA is not reloaded to complete the FPD upgrade unless the **reload** option is entered. Reloading the SPA drops all traffic traversing that SPA’s interfaces. If you want to reload the SPA later to complete the upgrade, do not enter the **reload** option and perform OIR of the SPA later to complete the FPD upgrade.

Cisco 7600 Series

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced. This command replaces the upgrade hw-module subslot command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to manually upgrade the FPD images on a SPA. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade will detect and automatically upgrade all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SPA was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SPA offline. The time required to complete an FPD image upgrade can be lengthy. The **show upgrade progress** command can be used to gather more information about estimated FPD download times for a particular SPA.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Configuration Guide* or the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*.

Examples

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module subslot 2/0 fpd file disk0:spa_fpd.122-20.S2.pkg

% Uncompressing the bundle ... [OK]

% The following FPD(s) will be upgraded for card in subslot 2/0 :

=====
Field Programmable   Current   Upgrade   Estimated
Device:"ID-Name"     Version   Version   Upgrade Time
=====
1-Data & I/O FPGA    4.12     4.13     00:06:00
=====

% Are you sure that you want to perform this operation? [no]:y
% Restarting the target card (subslot 2/0) for FPD image upgrade. Please wait ...

Router#
```

```
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_TIME:Estimated total FPD image upgrade time for
SPA-4FE-7304 card in subslot 2/0 = 00:06:00.
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_START:4FE/2GE FPGA (FPD ID=1) image upgrade in
progress for SPA-4FE-7304 card in subslot 2/0. Updating to version 4.13. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:06:00)
...[.....(part of the output has been removed for brevity)....
.....]
SUCCESS - Completed XSVF execution.

*Jan 14 00:42:59:%FPD_MGMT-6-FPD_UPGRADE_PASSED:4FE/2GE FPGA (FPD ID=1) image upgrade for
SPA-4FE-7304 card in subslot 2/0 has PASSED. Upgrading time = 00:05:42.596
*Jan 14 00:42:59:%FPD_MGMT-6-OVERALL_FPD_UPGRADE:All the attempts to upgrade the required
FPD images have been completed for SPA-4FE-7304 card in subslot 2/0. Number of
successful/failure upgrade(s):1/0.
*Jan 14 00:42:59:%FPD_MGMT-5-CARD_POWER_CYCLE:SPA-4FE-7304 card in subslot 2/0 is being
power cycled for the FPD image upgrade to take effect.
```

Related Commands

Command	Description
show hw-module slot fpd	Displays the current versions of FPD image files for all of the active SIPs on a router.
show hw-module subslot fpd	Displays the FPD version on each SPA in the router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot fpd file	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-programmable

To perform a Complex Programmable Logic Device (CPLD) or Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router, use the **upgrade hw-programmable** command in Privileged EXEC configuration mode.

```
upgrade hw-programmable [all | CPLD | FPGA] {filename filename} {R0 | R1 | F0 | F1 | 0..5}
```

Syntax Description	
all	Select to perform both a CPLD and FPGA upgrades on a Cisco ASR 1000 Series Router. Note This option is not supported in Cisco IOS XE Release 3.1.0S.
CPLD	Select to perform a Complex Programmable Logic Device (CPLD) upgrade on the Cisco ASR1000-SIP10, standby or active Cisco ASR1000-RP in a Cisco ASR 1013 Router.
FPGA	Select to perform a Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router. Note This option is not supported in Cisco IOS XE Release 3.1.0S.
filename	Specifies the hw-programmable upgrade package file.
<i>filename</i>	Specifies the hw-programmable upgrade package file and its file system location. For <i>filename</i> , specify one of the following system locations and a package file name: <ul style="list-style-type: none"> • bootflash: RP-relative HW programmable package name • flash: RP-relative HW programmable package name • harddisk: RP-relative HW programmable package name This is the hw-programmable upgrade package file that contains a new version of the CPLD and FPGA code, used for performing the CPLD on a Cisco ASR 1013 Router or FPGA upgrade on a Cisco ASR 1000 Series Router. The package file name is typically named <code>asr1000-hw-programmables.<release_name>.pkg</code> .
R0	RP slot 0. In the Cisco ASR 1006 Routers and Cisco ASR 1013 Routers, it is the lower RP slot. In the Cisco ASR 1002 and Cisco ASR 1004 Routers, it is the only slot.
R1	RP slot 1. This is only in the Cisco ASR 1006 and Cisco ASR 1013 Routers. It is the higher RP slot.
F0	This is the embedded services processor (ESP) slot 0. In the Cisco ASR 1006 Routers and Cisco ASR 1013 Routers, it is the lower ESP slot. In the Cisco ASR 1002 and Cisco ASR 1004 Routers, it is the only slot.

F1	This is the embedded services processor (ESP) slot 2. This is only in the Cisco ASR 1006 and Cisco ASR 1013 Routers. It is the higher ESP slot.
0..5	This is one of the SIP carrier card slots. Select a slot number zero through five.
Note	A CPLD upgrade cannot be performed in Slot 5 in the ASR100-SIP10. Move the card to another slot.

Command Default CPLD or FPGA is not upgraded.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced in Cisco IOS XE Release 3.1S.

Usage Guidelines For procedures on performing a CPLD upgrade, see the [Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers](#) document.

Examples The following example upgrades the Cisco ASR1000-RP2 CPLD with the following command:

```
Router# upgrade hw-programmable cpld filename harddisk:
asr1000-hw-programmables.15.01s.pkg R0
```

```
Upgrade CPLD on Route-Processor 0 from current version 08103002 to 10021901 [confirm] This
command could take up to 10 minutes, please wait and do not power cycle the box or the
card (hardware may be unrecoverable). This command also issues a reset to the linecard at
the end of upgrade.[confirm]
```

Related Commands	Command	Description
	show hw-programmable	Displays the current CPLD and FPGA versions on a Cisco ASR 1000 Series Router.
	show upgrade hw-programmable progress	Displays the upgrade progress of the line card-field upgradeable device (LC-FPD) on a Cisco ASR 1000 Series Router.
	show upgrade hw-programmable	Displays the names and versions of individual files in the hw_programmable package file.

upgrade rom-monitor default

To configure a particular ROM monitor image as the default ROMmon image, use the **upgrade rom-monitor default** command in privileged EXEC mode.

upgrade rom-monitor {rom0 | rom1 | rom2} default

Syntax Description

rom0	One-time programmable, always-there “golden” ROMmon.
rom1	Upgradable ROM monitor 1.
rom2	Upgradable ROM monitor 2.

Defaults

ROM 0, the one-time programmable, always there “golden” ROMmon is the default ROM monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(18)S	This command was implemented on Cisco 7304 routers running Cisco IOS Release 12.2 S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set a ROMmon image as the default ROMmon image. If this command is not configured, the system uses ROM 0 as the default ROMmon image.

There are three ROMmon images. ROM 0 is a one-time programmable, always-there ROMmon image, referred to as the “golden” ROMmon. ROM 1 and ROM 2 are upgradeable ROMmon images. At bootup, the system uses the golden ROMmon by default. If either ROM 1 or ROM 2 are configured, the system still begins bootup with the golden ROMmon, then switches to the configured ROMmon. If a new configured ROMmon image fails to boot up Cisco IOS, the router marks this ROMmon image as invalid and reverts to the golden image for the next Cisco IOS bootup.

After downloading a new ROMmon image to the writeable ROMmon, you must reload Cisco IOS for the new ROMmon to take effect. The first time a new ROMmon image is loaded, you must allow the system to boot up Cisco IOS before doing any resets or power cycling. If the ROMmon loading process is interrupted, the system interprets this as a bootup failure of the new ROMmon image and reverts the ROMmon back to the golden ROMmon image in ROM 0.

Examples

The following example configures ROM 2 as the default ROMmon image:

```
Router# upgrade rom-monitor rom2 default  
  
done!  
Will take effect on next reload/reset
```

Related Commands

Command	Description
show c7300	Displays the types of hardware installed in a Cisco 7304 router.
show platform	Displays the platform.
show diag	Displays hardware information for any slot or the chassis.
upgrade rom-monitor file	Upgrades the ROM monitor.

upgrade satellite satellite

To upgrade the firmware of an NM-1VSAT-GILAT network module through TFTP, use the **upgrade satellite satellite** command in privileged EXEC mode.

upgrade satellite satellite *slot/unit tftp-server-address firmware-filename*

Syntax Description

<i>slot/</i>	Router chassis slot in which the network module is installed. The / must be typed in between <i>slot</i> and <i>unit</i> .
<i>unit</i>	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
<i>tftp-server-address</i>	The IP address of the TFTP server that contains the firmware upgrade.
<i>firmware-filename</i>	The name of the file with the upgraded firmware.

Command Default

Firmware will not be upgraded through TFTP.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XJ2	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The **upgrade satellite satellite** command is used to provide a firmware upgrade of VSATs locally at remote sites through TFTP. This method reduces dependency on a central hub, and allows for ease of update when connected to a service provider who uses third-party hubs.

When the TFTP server is configured on the router, the VSAT firmware is copied to the router flash memory. The TFTP server configuration would be as follows:

```
tftp-server flash:< <firmware filename>
```

This configuration would be within the overall router configuration.

When this configuration is done, the upgrade is accomplished by pointing the VSAT to the router IP address in the **upgrade satellite satellite** command. The upgrade process will take several minutes.

Examples

The following example shows the response of the NM-1VSAT-GILAT network module to a firmware upgrade command.

```
Router# upgrade satellite satellite 1/0 9.1.0.1 VSAT_99.06.01.26_Bin.bin
Download of new firmware will proceed after a reboot of
the satellite network module. This could take up to two minutes.
Please wait...
```

```
*Mar 4 03:18:15.006: %LINEPROTO-5-UPDOWN: Line protocol on Interface Satellite1/0, changed
state to up
```

The upgrade process will complete in several minutes.
It will take place in the background.
Please monitor the console for errors.

```
*Mar 4 03:21:16.006: %LINEPROTO-5-UPDOWN: Line protocol on Interface Satellite1/0, changed
state to down
*Mar 4 03:27:20.842: %LINEPROTO-5-UPDOWN: Line protocol on Interface Satellite1/0, changed
state to up
```

Related Commands

Command	Description
service-module satellite status	Verifies the image version of the downloaded firmware.

wanphy flag j1 transmit

To configure the J1 byte values on the local SPA and to check the connectivity to the remotely connected SPA by passing the J1 byte values, use the **wanphy flag j1 transmit** *byte-value* command in the Controller configuration mode. To deconfigure the J1 byte value and stop the J1 byte value from being sent to the remote end, use the **no** form of this command.

wanphy flag j1 transmit *byte-value*

no wanphy flag j1 transmit

Syntax Description	byte-value	J1 byte value that is sent from the local SPA to the remote SPA. Length of string in bytes. The range is from 0 to 16 bytes.
	j1	Specifies that the J1 byte value is passed from the local SPA to the remote SPA.
	transmit	Transmits the specified byte value passed from the local SPA to the remote SPA.

Command Default No default behavior or values are available.

Command Modes Controller configuration (config-controller)

Command History	Release	Modification
	Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines The **wanphy flag j1 transmit** command has been introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.3.0S. The main purpose of this command is to pass a J1 string value from the local Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter to the remote SPA in order to check the connectivity between the two SPAs.



Note

Both the local and remotely connected Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter must operate in the WAN mode.

Examples The following example shows how to pass a J1 byte value string from locally installed SPA to a remote SPA:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy flag j1 transmit messagefromlocalspa
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

wanphy report-alarm

To enable selective alarm reporting for line-level, path-level, or section-level alarms, use the **wanphy report-alarm** command in Controller configuration mode. To reset the alarm reporting to its default, use the **no** form of this command.

wanphy report-alarm {*default* | *line* | *path* | *section* | *wis*}

no wanphy report-alarm

Syntax Description

<i>default</i>	Alarm reporting of line, section, and path to their default configured values.
<i>line</i>	The line-level alarm reporting status.
<i>path</i>	The path-level alarm reporting status.
<i>section</i>	The section-level alarm reporting status.
<i>wis</i>	The WIS-level alarm reporting status.

Command Default

No default values are available.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The **wanphy report-alarm** command has been introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.3.0S. The main purpose of this command is to selectively add more line-level, section-level, WIS-level, and path-level alarms over and above the default configured alarms. To set alarm reporting to its default value, use the **no wanphy report-alarm** command.

The wanphy delay triggers command is not supported on the WANPHY SPA, because upon executing this command, the hardware brings down the link when critical alarms are detected. An error message is displayed as in the following example:

```
Router(config-controller)# wanphy delay triggers line
%'delay triggers' is not supported on Wanphy SPA since the hardware brings down
the link when critical alarms are detected.
```

Examples

The following example shows how to configure the line-level alarms:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy report-alarm line
```

The following example shows how to configure the path-level alarms:

```
Router# config  
Router(config)# controller wanphy 2/1/0  
Router(config-controller)# wanphy report-alarm path
```

The following example shows how to configure the section-level alarms:

```
Router# config  
Router(config)# controller wanphy 2/1/0  
Router(config-controller)# wanphy report-alarm section
```

The following example shows how to configure the WIS-level alarms:

```
Router# config  
Router(config)# controller wanphy 2/1/0  
Router(config-controller)# wanphy report-alarm wis
```

The following example shows how to reconfigure the alarms to their default values:

```
Router# config  
Router(config)# controller wanphy 2/1/0  
Router(config-controller)# wanphy report-alarm default
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

wanphy threshold

To configure the physical layer threshold values for b1-tca, b2-tca, the Signal Degrade (SD) Bit Error Rate (BER), and Signal Failure (SF) BER, use the **wanphy threshold** command in the Controller configuration mode. To reset the threshold alarm values to its default values, use the **no** form of the command.

wanphy threshold {*b1-tca* | *b2-tca* | *sd-ber* | *sf-ber*}

no wanphy threshold

Syntax Description		
<i>b1-tca</i>	The B1 BER threshold-crossing alarm value. The default b1-tca value is 10e-6. The valid range is 4 to 9.	
<i>b2-tca</i>	The B2 BER threshold-crossing alarm values. The default b2-tca value is 10e-6. The valid range is 3 to 9.	
<i>sd-ber</i>	The SD BER threshold-crossing alarm value. The range value is expressed exponentially as 10e-n. The default sd-ber value is 6 (10e-6). The valid range is 3 to 9.	
<i>sf-ber</i>	The SF BER threshold-crossing alarm value. The range value is expressed exponentially as 10e-n. The default sf-ber value is 3 (10e-3). The valid range is 3 to 9.	

Command Default By default, SF-BER, SD-BER, B1-tca, and B2-tca are enabled. However, alarm logging is enabled only for SF-BER.

Command Modes Controller configuration (config-controller)

Command History	Release	Modification
	Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines The **wanphy threshold** command has been introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.3.0S. The main purpose of this command is to configure the threshold values for SF-BER and SD-BER.

Examples The following example shows how to configure the B1 TCA value:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold b1-tca 4
```

The following example shows how to configure the B2 TCA value:

```
Router# config
```

```
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold b2-tca 5
```

The following example shows how to configure the SD-BER threshold value:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold sd-ber 8
```

The following example shows how to configure the SF-BER threshold value:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold sf-ber 9
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

xconnect (CEM)

To build one end of a circuit emulation (CEM) connection and to enter CEM xconnect configuration mode, use the **xconnect** command in CEM configuration mode. To remove any existing CEM connections from this CEM channel, use the **no** form of this command.

xconnect *remote-ip-address* *virtual-connect-ID* **encapsulation** *encapsulation-type*

no xconnect

Syntax Description

<i>remote-ip-address</i>	IP address of an interface—physical or loopback—on the destination router.
<i>virtual-connect-ID</i>	Virtual connect ID (VCID). For CEM over IP (CEoIP), you must enter a value of 0.
encapsulation	Sets the encapsulation type.
<i>encapsulation-type</i>	Encapsulation type. You must set the encapsulation type to UDP.

Command Default

No CEM connections are built.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example shows how to build one end of a CEoIP connection and to enter CEM xconnect configuration mode.

```
Router(config-cem)# xconnect 10.0.5.1 0 encapsulation udp
Router(config-cem-xconnect)#
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
local ip address	Defines the IP address of the local router.
local udp port	Defines the local UDP port.
remote udp port	Defines the UDP port of a remote endpoint.
show cem	Displays CEM channel statistics.

yellow

To enable generation and detection of yellow alarms, use the **yellow** command in interface configuration mode.

yellow {generation | detection}

Syntax Description

generation	Enables or disables generation of yellow alarms.
detection	Enables or disables detection of yellow alarms.

Defaults

Yellow alarm generation and detection are enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7100 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to generate and detect yellow alarms. If the received signal is lost the yellow alarm can be generated to indicate a frame loss event. Generation of a yellow alarm will ensure that the alarm is sent to the remote end of the link. When the remote end is transmitting a yellow alarm, detection must be enabled to detect the alarm condition.

Examples

The following example shows how to enable generation and detection of yellow alarms on a Cisco 7500 series router:

```
Router(config)# interface atm 3/1/0
Router(config-if)# yellow generation
Router(config-if)# yellow detection
```