

tunnel bandwidth through yellow

- tunnel bandwidth, on page 3
- tunnel checksum, on page 4
- tunnel mpls-ip-only, on page 5
- tunnel destination, on page 6
- tunnel endpoint service-policy output, on page 10
- tunnel entropy, on page 11
- tunnel key, on page 13
- tunnel mode, on page 14
- tunnel path-mtu-discovery, on page 20
- tunnel rbscp ack_split, on page 22
- tunnel rbscp delay, on page 23
- tunnel rbscp input_drop, on page 24
- tunnel rbscp long_drop, on page 25
- tunnel rbscp report, on page 26
- tunnel rbscp window_stuff, on page 27
- tunnel route-via, on page 28
- tunnel sequence-datagrams, on page 29
- tunnel source, on page 30
- tunnel tos, on page 34
- tunnel ttl, on page 35
- tunnel vrf, on page 36
- type STS48c, on page 38
- tx-queue-limit, on page 39
- ucse subslot imc password-reset, on page 40
- ucse subslot server, on page 41
- ucse subslot server password-reset, on page 43
- ucse subslot shutdown, on page 45
- ucse subslot statistics, on page 46
- ucse subslot status, on page 47
- ucse cmos-reset, on page 49
- ucse heartbeat-reset, on page 51
- ucse imc config, on page 52
- ucse imc file delete, on page 53

- ucse imc file download, on page 54
- ucse password-reset, on page 55
- ucse server boot, on page 57
- ucse server boot order, on page 59
- ucse server erase device hdd, on page 61
- ucse server raid level, on page 62
- ucse server reload boot, on page 64
- ucse server reset boot, on page 65
- ucse session, on page 66
- ucse shutdown, on page 68
- ucse server start boot, on page 70
- ucse statistics, on page 71
- ucse status, on page 73
- ucse stop, on page 75
- unidirectional, on page 77
- upgrade fpd auto, on page 79
- upgrade fpd path, on page 82
- upgrade fpga, on page 84
- upgrade fpga all, on page 88
- upgrade hw-module slot, on page 92
- upgrade hw-module slot fpd file, on page 97
- upgrade hw-module subslot, on page 101
- upgrade hw-module subslot fpd file, on page 105
- upgrade hw-programmable, on page 108
- upgrade rom-monitor default, on page 110
- upgrade satellite satellite, on page 112
- utc offset leap-second offset, on page 114
- vectoring, on page 115
- vtg, on page 116
- wanphy flag j1 transmit, on page 118
- wanphy report-alarm, on page 119
- wanphy threshold, on page 121
- xconnect (CEM), on page 123
- yellow, on page 125

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.
bandwidth	Bandwidth, in kbps. Range is from 0 to 2147483647. Default is 8000.

Command Default

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 **tunnelchecksum**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.

Command Default

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 mpls-ip-only

To copy the inner IP header's Do Not Fragment bit from the payload into the tunnel packet's IP header, use the **tunnel mpls-ip-only** command in the interface configuration mode.

tunnel mpls-ip-only
no tunnel mpls-ip-only

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
17.5.1	This command was introduced.

Usage Guidelines

If the Do Not Fragment bit is not set, the payload is fragmented when the IP packet exceeds the MTU set for the interface. When you enable the **tunnel mpls-ip-only** command, the **tunnel path-mtu-discovery** automatically gets enabled due to the dependency.

Examples

The following example shows how to enable this command:

```
Router(config-if)# tunnel mpls-ip-only
```

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-nameip-addressipv6-address* | **dynamic**}
no tunnel destination

Command Syntax for Cisco Catalyst 3850 Series Switches

tunnel destination *ip-address*
no tunnel destination

Syntax Description

host-name	Name of the host destination.
ip-address	IP address of the host destination expressed in dotted decimal notation.
ipv6-address	IPv6 address of the host destination expressed in IPv6 address format.
dynamic	Applies the tunnel destination address dynamically to the tunnel interface.

Command Default

No tunnel interface destination is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was modified. The address field was modified to accept an *ipv6-address* 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1SY	This command was integrated into Cisco IOS Release 15.1SY.
Cisco IOS XE Release 3.7S	This command was modified. The **dynamic** keyword was added.

Release	Modification
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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



Note **Only GRE tunneling is supported on Cisco Catalyst 3850 Series Switches.**

Tunnel Destination Address for Cayman Tunnel

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

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

Tunnel Destination Address for Dynamic Tunnel

The following example shows how to set the tunnel destination address dynamically:

```
Device(config)# interface tunnel0
Device(config-if)# tunnel destination dynamic
Device(config-if)# *Nov 22 19:38:28.271: Tunnel notified destination change: dynamic is set
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
 no ip address
 tunnel source dynamic
 tunnel destination dynamic
end
```

If the tunnel destination address is configured to be set dynamically, you cannot configure the tunnel destination address without removing the dynamic configuration.

```
Device(config)# interface tunnel0
Device(config-if)# tunnel destination ethernet 0/0
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
```

```
 no ip address
 tunnel destination dynamic
end
Device# configure terminal
Device(config)# interface tunnel0
Device(config-if)# no tunnel destination
```

Tunnel Destination Address for GRE Tunneling

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

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

Tunnel Destination Address for GRE Tunneling on Cisco Catalyst 3850 Series Switches

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in Global or non- VRF environment on Cisco Catalyst 3850 Series Switches:

```
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment on Cisco Catalyst 3850 Series Switches. Use the **vrf definition** *vrf-name* and the**vrf forwarding** *vrf-name* commands to configure and apply VRF.

```
Device(config)# vrf definition RED
Device(config-vrf)#  address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)#  exit
Device(config)# interface tunnel 2
Device(config)# vrf forwarding RED
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

Tunnel Destination Address for IPv6 Tunnel

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

```
Device(config)# interface Tunnel0
Device(config-if)# no ip address
Device(config-if)# ipv6 router isis
```

```
Device(config-if)# tunnel source Ethernet0/0
Device(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64
Device(config-if)# tunnel mode gre ipv6
Device(config-if)# exit
!
Device(config)# interface Ethernet0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# exit
!
Device(config)# ipv6 unicast-routing
Device(config)# router isis
Device(config)# net 49.0000.0000.000a.00
```



Note **IPv6 GRE tunneling is not supported on Cisco Catalyst 3850 Series Switches.**

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 endpoint service-policy output

To configure a Quality of Service (QoS) policy for a tunnel in an output direction, use the **tunnel endpoint service-policy output** command in configuration interface mode. To remove the QoS policy for a tunnel, use the **no** form of the command.

tunnel endpoint service-policy output *policy-name*

Syntax Description

policy-name	Name of the policy map to associate with a tunnel.

Command Default

By default no policy is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 13.3S	This command was introduced.

Usage Guidelines

Use the **tunnel endpoint service policy output** command to associate a service policy with Ethernet over GRE (EoGRE) tunnels. Use the **policy-map** command in global configuration mode, to create a policy map.

The following example shows how to configure a Quality of Service (QoS) policy for outward traffic on a tunnel:

```
Device(config)# interface tunnel 1
Device(config-if)# tunnel source Loopback 0
Device(config-if)# tunnel vlan 10, 20
Device(config-if)# ip address unnumbered Loopback 0
Device(config-if)# tunnel mode ethernet gre ipv4
Device(config-if)# tunnel endpoint service-policy output tunnel-qos-policy
Device(config-if)# ip subscriber l2-connected
Device(config-subscriber)# initiator unclassified mac-address
Device(config-subscriber)# initiator dhcp
Device(config-subscriber)# exit
```

Related Commands

Command	Description
policy-map	Creates a policy map that can be attached to one or more interfaces.
show policy-map multipoint tunnel	Displays information about a specific QoS policy for a multipoint tunnel interface.

tunnel entropy

To achieve load balancing of tunnel packets in a network, use the **tunnel entropy** command in interface configuration mode. To stop load balancing, use the **no** form of the command.

tunnel entropy

no tunnel entropy

Command Default

Calculation of tunnel entropy is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

You can enable tunnel entropy calculation only in Generic Routing Encapsulation (GRE) mode. If you configure a 32-bit tunnel key, you must remove the existing key first.

To disable tunnel entropy calculation, you must remove the configured tunnel key before using the **no tunnel entropy** command to disable entropy calculation.

Use the **show interfaces tunnel** command to verify whether tunnel entropy calculation is enabled or not. If it is enabled, the key size is also displayed.

Example

The following example shows how to configure tunnel entropy calculation for GRE mode of the tunnel interface:

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 21
Device(config-if)# tunnel source 10.1.1.1
Device(config-if)# tunnel destination 172.168.2.1
Device(config-if)# tunnel mode gre ip
Device(config-if)# tunnel key 4683
Device(config-if)# tunnel entropy
Device(config-if)# end
```

The following is sample output from the **show interfaces tunnel** command, which displays that tunnel entropy calculation is enabled with a 24-bit key:

```
Device# show interfaces tunnel 21

Tunnel21 is up, line protocol is up
Hardware is Tunnel
MTU 17864 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.1.1.1, destination 172.168.2.1
```

```
Tunnel protocol/transport GRE/IP
Key 0x124B, sequencing disabled
Checksumming of packets disabled
Tunnel Entropy Calculation Enabled (24-bit Key)
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1472 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:03:07
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on a device or access server.
show ip route	Displays the current state of the routing table.

tunnel key

To enable an ID key for a tunnel interface, use the**tunnelkey** 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

key-number	Number from 0 to 4294967295 that identifies the tunnel key.

Command Default

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.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

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 **noipmroute-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:

```
Device(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 return to the default mode, use the **no** form of this command.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **ethernet gre** {**ipv4** | **ipv6**} | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp** }
no tunnel mode

Command Syntax for Cisco Catalyst 3850 Series Switches

tunnel mode gre ip
no tunnel mode

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol (DMVRP).
ethernet gre ipv4	Ethernet over Generic Routing Encapsulation (GRE) IPv4.
ethernet gre ipv6	Ethernet over GRE IPv6.
eon	EON–compatible Connectionless Network Service (CLNS) tunnel.
gre	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

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	This command was modified. The **aurp**, **dvmrp**, and **ipip** keywords were added.
11.2	This command was modified. The optional **decapsulate-any** keyword was added.
12.2(13)T	This command was modified. The **gre multipoint** keyword was added.
12.3(7)T	This command was modified. The following keywords were added: • **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	This command was modified. The **ipsec ipv4** keyword was added.
12.2(18)SXE	This command was modified. The **gre multipoint** keyword was 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	This command was modified. The **ipsec ipv6** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
15.1SY	This command was integrated into Cisco IOS Release 15.1SY.
Cisco IOS XE Release 3.9S	This command was modified. The **ethernet gre** keyword was added.

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 enables 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 mrouted (multicast) router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

Ethernet over GRE

Use Ethernet over GRE to send ethernet traffic from low-end resident gateways (RGs) or Customer Premises Equipment (CPE) to aggregation routers where Mobile Access Gateway (MAG) is enabled over GRE tunnels. The RGs and CPE can then provide mobility services to mobile nodes (MNs).

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 to another security gateway router, and provides crypto IPsec protection for traffic from an internal network when it is transmitted across the public IPv6 Internet. IPv6 IPsec is very similar to the security gateway model using IPv4 IPsec protection.

Note **Only GRE tunneling is supported on Cisco Catalyst 3850 Series Switches.**

Cayman Tunneling

The following example shows how to enable Cayman tunneling:

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

Ethernet over GRE Tunneling

The following example shows how to enable Ethernet over GRE tunneling for IPv6:

```
Device(config)# interface tunnel 0
Device(config)# mac-address 0000.0000.00001
Device(config-if)# ip address 10.1.1.2 255.255.255.0
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel mode gre ipv6
Device(config-if)# tunnel vlan 1023
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

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

GRE Tunneling Examples for Cisco Catalyst 3850 Series Switches

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in Global or non- VRF environment on Cisco Catalyst 3850 Series Switches:

```
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment on Cisco Catalyst 3850 Series Switches. Use the **vrf definition** *vrf-name* and the**vrf forwarding** *vrf-name* commands to configure and apply VRF.

```
Device(config)# vrf definition RED
Device(config-vrf)#  address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)#  exit
Device(config)# interface tunnel 2
Device(config)# vrf forwarding RED
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

Note **IPv6 GRE tunneling is not supported on Cisco Catalyst 3850 Series Switches.**

IPsec in IPv4 Transport

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

```
Device (config)# crypto ipsec profile PROF
Device (config)# set transform tset
Device (config)# interface tunnel 0
Device (config-if)# ip address 10.1.1.1 255.255.255.0
Device (config-if)# tunnel mode ipsec ipv4
Device (config-if)# tunnel source loopback 0
Device (config-if)# tunnel destination 172.16.1.1
```

IPsec in IPv6 Transport

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

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

```
Device(config)# interface tunnel 0
```

```
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(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.
mac-address	Specifies a MAC address to use as the common router MAC address for interfaces on the active and standby chassis.
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 vlan	Associates a VLAN ID for the Ethernet over GRE 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 **tunnelpath-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. • *aging-mins* --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. • *mtu-bytes*-- Number of bytes. Range is from 92 to 65535. Default is 92.

Command Default

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 *mtu-bytes* 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 **showinterfacestunnel** 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 **tunnelrbscpack_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

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

Command Default

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 **tunnelrbscpack_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 **tunnelrbscpdelay** 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.

Command Default

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 **tunnelrbscpdelay** 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 **tunnelrbscpinput_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

bw-delay-products	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.

Command Default

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

Use the **tunnelrbscpinput_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.

Use this command in conjunction with the **tunnelrbscplong_drop** command which allows packets that are waiting in an RBSCP tunnel encapsulation queue to be dropped after a period of time.

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 **tunnelrbscplong_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.

Command Default

No queued packets are dropped.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **tunnelrbscplong_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 **tunnelrbscpinput_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 **tunnelrbscpreport** 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.

Command Default

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 **tunnelrbscpreport** 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 **tunnelrbscpwindow_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

step-size	Increment step size for the TCP window scale. Range is from 1 to 20. Default is 1.

Command Default

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 **tunnelrbscpwindow_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 **tunnelroute-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

interface-type	Indicates the type of interface.
interface-number	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 **tunnelroute-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 **tunnelsequence-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.

Command Default

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-addressipv6-address* | *interface-type interface-number* | **dynamic**}
no tunnel source

Command Syntax for Cisco Catalyst 3850 Series Switches

tunnel source *ip-address*
no tunnel source

Syntax Description

dynamic	Applies the tunnel source address dynamically to the tunnel interface.
ip-address	Source IP address of packets in the tunnel. • In case of traffic engineering (TE) tunnels, the control packets are affected.
ipv6-address	Source IPv6 address of packets in the tunnel.
interface-type	Interface type.
interface-number	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 an IPv6 address as the source address allowing 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.

Release	Modification
15.1SY	This command was integrated into Cisco IOS Release 15.1SY.
Cisco IOS XE Release 3.7S	This command was modified. The **dynamic** keyword was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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 addresses. The workaround is to create a loopback interface and source packets from 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 addresses.



Note **Only GRE tunneling is supported on Cisco Catalyst 3850 Series Switches.**

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, and not the tunnel itself.

GRE tunnel encapsulation and deencapsulation for multicast packets are handled by the hardware. 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 that the hardware-assisted tunnels do not share a source.

Cayman Tunnel Example

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

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

Dynamic Tunnel Example

The following example shows how to set the tunnel source dynamically:

```
Device(config)# interface tunnel0
Device(config-if)# tunnel source dynamic
Device(config-if)# *Nov 22 19:38:28.271: Tunnel notified source change: dynamic is set
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
 no ip address
```

```
 tunnel source dynamic
end
```

If the tunnel source is configured to be set dynamically, you cannot configure the tunnel source address without removing the dynamic configuration.

```
Device(config)# interface tunnel0
Device(config-if)# tunnel source ethernet 0/0
Device(config-if)# *Nov 22 21:39:52.423: Tunnel notified source change: dynamic is set
*Nov 22 21:39:52.423: Tunnel notified source change, src ip 1.1.1.1
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
 no ip address
 tunnel source dynamic
end
Device# configure terminal
Device(config)# interface tunnel0
Device(config-if)# no tunnel source
Device(config-if)# *Nov 22 21:41:10.287: Tunnel notified source change: dynamic is not set
```

GRE Tunneling Example

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

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

GRE Tunneling Examples for Cisco Catalyst 3850 Series Switches

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in Global or non- VRF environment on Cisco Catalyst 3850 Series Switches:

```
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment on Cisco Catalyst 3850 Series Switches. Use the **vrf definition** *vrf-name* and the**vrf forwarding** *vrf-name* commands to configure and apply VRF.

```
Device(config)# vrf definition RED
Device(config-vrf)#  address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)#  exit
Device(config)# interface tunnel 2
Device(config)# vrf forwarding RED
```

```
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

Note **IPv6 GRE tunneling is not supported on Cisco Catalyst 3850 Series Switches.**

MPLS TE Tunnel Example

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

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

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

Command Default

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 **tunneltos** 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 **tunneltos**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 **tunnelttl** 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 destination commandtunnel ttl *hop-count*
no tunnel ttl

Syntax Description

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

Command Default

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 or interface configuration mode. To disassociate a VRF from the tunnel destination, interface, or subinterface, use the **no** form of this command.

tunnel vrf *vrf-name*
no tunnel vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

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	This command was integrated into Cisco IOS Release 12.2(33)SRA. Support was added for the Cisco 10000 Series Routers.
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.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

To associate a VRF instance with a specific tunnel destination, ensure that the tunnel source and destination are in the same VRF.

Use the **ip vrf forwarding** command to associate a VRF instance with an interface or a subinterface other than a tunnel interface.

Use the **no ip vrf forwarding** *vrf-name* command or the **no tunnel vrf** *vrf-name* command to set either the IP VRF or the tunnel VRF to the global routing table.

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

Cisco 10000 Series Routers and Cisco ASR 1000 Series Aggregation Services Routers

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 is looked up in the VRF named vrf2.

```
Device(config)# interface tunnel0
Device(config-if)# ip vrf forwarding vrf1
Device(config-if)# ip address 10.3.3.3 255.255.255.0
Device(config-if)# tunnel source loop 0
Device(config-if)# tunnel destination 10.5.5.5
Device(config-if)# tunnel vrf vrf2
```

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 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.

type STS48c

Use this command to configure protection group type.

type STS48c

There are no keywords for this command.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Examples

The following example shows how to configure protection group:

```
enable
configure terminal
protection-group 401 type STS48c
controller protection group 401
type STS48c
cem-group 19001 cep
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

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

number	Maximum number of transmit buffers that the specified interface can subscribe.

Command Default

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 **showcontrollersmci** 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.

ucse subslot imc password-reset

To reset the Cisco Integrated Management Controller (CIMC) password, use the **ucse subslot imc password-reset** command in privileged EXEC mode.

ucse subslot *slot/subslot* **imc password-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

After you enter this command, at the next login, the system requests that you set a new password to access CIMC.

Examples

The following example shows how to reset the CIMC password in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 imc password-reset
Router#
 IMC ACK: UCSE password reset successful for IMC
```

ucse subslot server

To reload, reset, start, or stop the hardware on the server module, use the **ucse subslot server** command in privileged EXEC mode.

ucse subslot *slot/subslot* **server** {**reload** | **reset** | **start** | **stop**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
reload	Powers down the server module and then powers it on. **Note** The **reload** keyword is not supported on the NIM E-Series-NCE. Instead, we recommend that you use the following commands from the router: **1.** Router # **ucse subslot** *slot/subslot* **shutdown** **2.** Router # **ucse subslot** *slot/subslot* **start** If a reload is necessary, use the following command: Router # **hw-module subslot 0/***NIM-slot-number* **reload** **Note** This command power-cycles the module. The CIMC and server reboot.
reset	Resets the hardware on the server module.
start	Powers on the server module.
stop	Immediately powers down the server module. **Note** The **stop** keyword is not supported on the NIM E-Series-NCE. Instead, we recommend that you use the following command from the router: Router # **ucse subslot** *slot/subslot* **shutdown** If it is necessary to do an immediate power down of the server, use the following command: Router # **hw-module subslot 0/***NIM-slot-number* **stop** **Note** This command powers down the module. The CIMC and server power off.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

Use the **reset** keyword only to recover from a shutdown or failed state.



Caution Using the **reset** keyword does *not* provide an orderly software shutdown and may impact file operations that are in progress.

Examples

The following example shows how to reload the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server reload
Router#
 IMC ACK: UCSE Server reload successful.
```

The following example shows how to reset the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server reset
Router#
 IMC ACK: UCSE Server reset successful.
```

The following example shows how to start the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server start
Router#
 IMC ACK: UCSE Server start successful.
```

The following example shows how to stop the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server stop
Router#
 IMC ACK: UCSE Server stop successful.
```

ucse subslot server password-reset

To reset the BIOS or RAID password, use the **ucse subslot server password-reset** command in privileged EXEC mode.

ucse subslot *slot/subslot* **server password-reset** {**BIOS** | **RAID**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
BIOS	Resets the BIOS password.
RAID	Resets the RAID password. **Note** RAID is not supported on the NIM E-Series NCE.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

After you enter this command, at the next login, the system requests that you set a new password to access BIOS or configure RAID.

Examples

The following example shows how to reset the BIOS password in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server password-reset BIOS
Router#
 IMC ACK: UCSE password reset successful for BIOS
```

The following example shows how to reset the RAID password in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server password-reset RAID
Router#
 IMC ACK: UCSE password reset successful for RAID
```

ucse subslot shutdown

To gracefully shut down the server module, use the **ucse subslot shutdown** command in privileged EXEC mode.

ucse subslot *slot/subslot* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

The NIM E-Series NCE might take up to 60 seconds to shut down. After two or three shut down attempts, if the NIM E-Series NCE does not shut down, enter the following commands from the router:

1. Router # **hw-module subslot 0/***NIM-slot-number* **stop**
2. Router # **hw-module subslot 0/***NIM-slot-number* **start**

Examples

The following example shows how to shut down an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 shutdown
Router#
 IMC ACK: UCSE Server shutdown successful.
```

ucse subslot statistics

To display or clear server module statistics, use the **ucse subslot statistics** command in privileged EXEC mode.

ucse subslot *slot/subslot* **statistics** [**clear**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
clear	(Optional) Clears the server module statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example shows how to display the statistics of an E-Series Server:

```
Router# ucse subslot 1/0 statistics
 Count of number of shutdowns command : 1
 Count of number of status commands : 0
 Count of number of server raid password  : 1
 Count of number of imc password-reset : 2
 Count of number of server bios password reset : 1
 Count of number of server reload : 1
 Count of number of server reset : 1
 Count of number of server start : 1
 Count of number of server stop : 1
 Count of number of vlan commands : 0
 Count of number of access-port commands : 1
 Count of number of IMC configured IP or DHCP commands: 1
```

ucse subslot status

To display configuration information related to the hardware and software on the server module, use the **ucse subslot status** command in privileged EXEC mode.

ucse subslot *slot/subslot* **status** [**detailed**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
detailed	(Optional) Displays detailed information about the server module, such as its status and settings of the reset and heartbeat-reset flags.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example shows how to display the status of an E-Series Server:

```
Router#  ucse subslot 1/0 status
CPU info
        Name         Cores    Version
        ------------ -------- --------------------------------------------------
        CPU1         4        Intel(R) Xeon(R) CPU E5-2418L 0 @ 2.00GHz

Memory info
        Name                 Capacity        Channel Speed (MHz) Channel Type
        -------------------- --------------- ------------------- ---------------
        Node0_Dimm0          Not Installed   Unknown             Unknown
        Node0_Dimm1          16384 MB        1333                DDR3
        Node0_Dimm2          8192 MB         1333                DDR3

Hard drive info
        Slot Number Controller Status                Manufacturer   Model          Drive
Firmware Coerced Size   Type  SED
        ----------- ---------- ---------------------- -------------- --------------
-------------- -------------- ----- -----
```

```
        1           SLOT-5     online                  ATA             ST91000640NS   CC02
         952720 MB      HDD   false
        2           SLOT-5     online                  ATA             ST91000640NS   CC02
         952720 MB      HDD   false
        3           SLOT-5     online                  ATA             ST91000640NS   CC02
         952720 MB      HDD   false

Virtual drive info
        Virtual Drive  Status               Name                      Size       RAID Level

        -------------- -------------------- ------------------------- ---------- ----------

        0              Optimal                                        1905440 MB RAID 5


PCI card info
        Name                 Slot       Vendor ID            Device ID            Product
Name
        -------------------- ---------- -------------------- --------------------
-------------------------
        PCIe Adapter1        0          0xe414               0x5716               Broadcom
 5719 1 Gbps 4...
       PCIe Adapter2        2          0x0010              0x7300              LSI 9240-8i
 MegaRAID S...

Network Setting
            IPv4 Address: 10.1.1.2
            IPv4 Netmask: 255.255.255.0
            IPv4 Gateway: 10.1.1.1

            NIC Mode: shared_lom
            NIC Redundancy: none
            NIC Interface: ge1
```

ucse cmos-reset

To reset the BIOS CMOS, use the **ucse cmos-reset** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **cmos-reset**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **cmos-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

This command sets the BIOS CMOS back to the factory defaults. User changes made in the BIOS will be lost.

Examples

The following example shows how to reset the BIOS CMOS in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 cmos-reset
```

Examples

The following example shows how to reset the BIOS CMOS in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 cmos-reset
```

ucse heartbeat-reset

To enable or disable Cisco IOS software from rebooting the Cisco E-Series Server when the heartbeat is lost, use the **ucse heartbeat-reset** command in EXEC mode.

ucse *slot* **heartbeat-reset** [**disable** | **enable**]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
enable	Does not allow the Cisco IOS software to reboot the Cisco E-Series Server when the heartbeat is lost.
disable	Allows the Cisco IOS software to reboot the Cisco E-Series Server when the heartbeat is lost.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to reset the slot server heartbeat:

```
Router# ucse 2 heartbeat-reset enable
```

ucse imc config

To save the CIMC configuration to a file on the router's flash drive or to restore the CIMC configuration from a file on the router's flash drive, use the **ucse imc config** command in EXEC mode.

ucse *slot* **imc config** {**restore** | **save**} **url**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
restore	Restores the CIMC configuration from a file.
save	Saves the CIMC configuration to a file.
url	The url where the configuration file is located.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Itis important to store the CIMC configuration to a file in case you need to move the HDDs from one module to another.

Examples

The following example shows how to save the CIMC configuration to a file:

```
Router# ucse 2 imc config save flash0:my-imc-config
```

ucse imc file delete

To delete the CIMC image file, use the **ucse imc file delete** command in EXEC mode. The file can be either a .iso or .img file.

ucse *slot* **imc file delete** *file_name*

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
file_name	Name of the CIMC image file to delete. **Note** The name of the file must match exactly the name of the file as displayed by the output of the **show ucse** *slot* **imc files**command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You can only delete one file at a time.

Examples

The following example shows how to delete the CIMC image file:

```
Router# ucse 2 imc file delete xxxxx.iso

Delete the IMC file xxxxx.iso [confirm]
Deleted
```

ucse imc file download

To download the CIMC image file in the background to an internal storage device, use the **ucse imc file download** command in EXEC mode. The file must have a .iso file extension.

ucse *slot* **imc file download** {**URL** *url* | **abort**}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url	Downloads the CIMC image file from the specified HTTP, HTTPS, SFTP, or FTPS server.
abort	Aborts the downloading of the file.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You can only download one file at a time.

To check the download progress after initiating a download, issue the **show ucse** *slot* **imc download progress** command.

Examples

The following example shows how to download the CIMC image file:

```
Router# ucse 2 imc file download URL http://xxxxx.iso
Started downloading file from http://xxxxx.iso

Router# show ucse 2 imc file download progress
Downloaded 23%
```

The following example shows how to abort a download of the CIMC image file:

```
Router# ucse 2 imc file download abort

Abort the IMC file download? [confirm] y
Download aborted.
```

ucse password-reset

To reset the BIOS, CIMC, or RAID password, use the **ucse password-reset** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **password-reset** {**BIOS** | **BMC** | **RAID**}

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **password-reset** {**BIOS** | **BMC** | **RAID**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
BIOS	Resets the BIOS password.
BMC	Resets the CIMC password.
RAID	Resets the RAID password. **Note** RAID is not applicable for the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series NCE installed in an ISR G2.

Usage Guidelines

After this command has been entered, the system requests that a new password be set when accessing the BIOS or BMC.

RAID is not applicable for the EHWIC E-Series NCE.

Examples

The following example shows how to reset the BIOS password in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 password-reset BIOS

Reset command sent
```

Examples

The following example shows how to reset the BIOS password in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 password-reset BIOS

Reset command sent
```

ucse server boot

To reload, reset, or boot the Cisco E-Series Server from a particular URL, use the **ucse server boot** command in EXEC mode.

ucse *slot* **server** {**reload** | **reset** | **start**} **boot** {**url** *url* | **device** *device_type*} [**argument** *text*]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from an externally stored file, which can be either a .iso or .img file. The URL can be one of the following types: • HTTP • FTP • SFTP • FTPS://XXXXX.iso Restrictions: • This argument accepts IPv6 and IPv4 addresses, as well as literal names. • The name of the file must match exactly the name of the file as displayed by the output of the **show ucse** *slot* **imc file**command.
device *device_type*	The device type from which the E-Series Server boots. It can be one of the following: • HDD:*device_name* —Hard disk drive • FDD—Floppy disk drive • CDROM:*device_name* —Bootable CD-ROM • PXE—PXE boot • EFI—Extensible Firmware Interface **Note** The name of the devices must match exactly the names as displayed by the output of the **show ucse** *slot* **server boot devices**command.
argument *text*	An arbitrary text string.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command works by first downloading the specified file to local storage, reloading the server from that file, and then booting the installed system.

After issuing this command, the system modifies the boot order so that the downloaded image is first.

After you have issued this command with the **url** argument and keyword, use the **show** *ucse* **slot server boot progress**command to see the results.

After you have issued this command with the **device** argument and keyword, use the **show** *ucse* **slot server boot order**command to see the results.

Examples

The following example shows how to boot the server from a URL:

```
Router# ucse 2 server reload boot url http://path/to/iso
Router# show ucse 2 server boot progress

Downloading http://path/to/iso 44%
```

The following example shows how to boot the server from an HDD:

```
Router# ucse 2 server reset boot device HDD
Router# show ucse 2 server boot progress

System started
```

The following example shows how to start the server from an HDD:

```
Router# ucse 2 server start boot device HDD
Router# show ucse 2 server boot progress
```

ucse server boot order

To configure the boot order for the Cisco E-Series Server, use the **ucse server boot order** command in EXEC mode.

ucse *slot* **server boot order device_1** [**device_2**] [**device_3**] [**device_4**]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
device_1 device_2 device_3 device_4	Specifies the devices to boot. **Note** The name of the devices must match exactly the names as displayed by the output of the **show ucse** *slot* **server boot devices**command. The device can be any of the following, but you can only use each device name once when issuing this command: • PXE—PXE boot • FDD—Floppy disk drive • HDD:*device_name* —Hard disk drive • CDROM:*device_name* —Bootable CD-ROM

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Due to BIOS limitations, you can only specify each device type (PXE, FDD, HDD, and CDROM) once per group. Therefore, it is impossible to set up a boot order with two HDDs or two CDROMs.

To determine the devices available from which you can boot the server, issue the **show ucse** *slot* **server boot devices** command.

To check the boot order configuration after issuing this command, issue the **show ucse** *slot* **server boot order** command.

Examples

The following example shows how to configure the boot order:

```
Router# show ucse 2 server boot devices

PXE
FDD
HDD:HDD3
HDD:RAID-MD0
HDD:USB-FF5D6CC3DAA67F12-1
CDROM:USB-CD
```

```
Router# ucse 2 boot order PXE CDROM:USB-CD FDD HDD:RAID-MD0
Router# show ucse 2 server boot order
Currently booted from CDROM:USB-CD
Boot order:
1) PXE
2) CDROM:USB-CD
3) FDD
4) HDD:RAID-MD0
```

ucse server erase device hdd

To erase all existing data from the Cisco E-Series Server hard drive devices (HDDs), use the **ucse server erase device hdd** command in EXEC mode.

ucse *slot* **server erase device hdd** {**ALL** | **use** *device_list*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
device_list	Erases the data from only the specified HDDs. **Note** The name of the devices must exactly match the names as displayed by the output of the **show ucse** *slot* **server boot devices**command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command if you need to remove sensitive data from a hard drive before shipping the server. The system prompts you to confirm that you really want to erase the data from the hard drive device.



Caution Use this command with caution, as it erases the contents of the HDDs.

To check the status of the hard drive after you have issued this command, use the **show ucse** *slot* **server erase device status** command.

Examples

The following example shows how to erase the data from the device called HDD2, and then display the status:

```
Router# ucse 2 server erase device hdd use hdd2

You are about to erase all data on the selected hard drives.
Proceed with drive erasure? y

Erasing HDD2 started

Router# show ucse 2 server erase device status

HDD2 erased 0 %
```

ucse server raid level

To configure the RAID array on the Cisco E-Series Server, use the **ucse server raid level** command in EXEC mode.

ucse *slot* **server raid level** {**0** | **1** | **5** | **NONE** | **use** *device_list*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
0	Data is stored evenly in stripe blocks across two or more disks without redundancy (mirroring).
1	Data is stored in mirrored set of disk drives with an optional hot spare disk drive.
5	Data is stored in stripe blocks with parity data staggered across all disk drives.
NONE	Disk drives of a computer are not configured as RAID and are put in a JBOD configuration.
use *device_list*	Allows you to configure more than one device at a time. If you do not use the **use** keyword, then the system configures all hard drives into a RAID in the order in which they are detected by the module. Enter the list of HDDs using a comma-separated list, such as HDD1, HDD2, HDD3. This command only applies to the internal HDDs, which are named according to their physical location. **Note** The name of the devices must match exactly the names as displayed by the output of the **show ucse** *slot* **server boot devices**command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command only applies to HDDs.

Caution Use this command with caution, as it destroys the contents of the HDDs. Do not use this command to migrate the RAID configuration.

After you have issued this command, use the **show** *ucse* **slot server raid level**command to see the results.

Examples

The following example shows how to configure RAID level 1:

```
Router# ucse 2 server raid level 1

You are about to change RAID configuration.
```

```
This will destroy all data on the hard drives.
Proceed with setting new RAID level? [confirm] y
RAID reconfigured

Router# show ucse 2 server raid level

RAID 0 (Ctrl:SLOT-5 ID:0 Size:1905440 MB State:Optimal)
        HDD1 :              953869 MB online (0 errors)
        HDD255 :              953869 MB online (0 errors)

        HDDs not in the RAID:
        HDD2 :              286102 MB system (0 errors)
```

ucse server reload boot

To boot the Cisco E-Series Server from a particular url or device type, use the **ucse server reload boot** command in EXEC mode.

ucse *slot* **server reload boot** {**url** *url* | **device** *device_type*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from the specified url.
device *device_type*	The device type from which the Cisco E-Series Server boots. It can be one of the following: • CDROM: Virtual-CD • EFI • FDD: Virtual-Floppy • HDD: RAID • HDD: SD2 • HDD: Virtual-HiFD • PXE: GIGETH0 • PXE: GIGETH1 • PXE: GIGETH3

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command to safely reload the server.

Examples

The following example shows how to reload the server:

```
Router# ucse 2 server reload boot url http://220.0.0.100/OS/image.iso
```

ucse server reset boot

To reset the hardware on the Cisco E-Series Server, use the **ucse server reset boot** command in EXEC mode.

ucse *slot* **server reset boot** {**url** *url* | **device** *device_type*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from the specified url.
device *device_type*	The device type from which the Cisco E-Series Server boots. It can be one of the following: • CDROM: Virtual-CD • EFI • FDD: Virtual-Floppy • HDD: RAID • HDD: SD2 • HDD: Virtual-HiFD • PXE: GIGETH0 • PXE: GIGETH1 • PXE: GIGETH3

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command only to recover from a shutdown or failed state.

Caution Using this command does *not* provide an orderly software shutdown and may impact file operations that are in progress.

Examples

The following example shows how to reset the server:

```
Router# ucse 2 server reset boot url http://220.0.0.100/OS/image.iso
```

ucse session

To start or close a host or CIMC session, use the **ucse session** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **session** {**imc** [**clear**] | **host** [**clear**]}

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **session** {**imc** [**clear**] | **host** [**clear**]}

Note The **ucse** *slot* **session imc** command will work only if you have configured a router-side IP address (for instance, ip unnumbered GigabitEthernet0/0) on the interface.

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
imc	Starts a session with CIMC.
imc clear	Closes the existing CIMC session.
host	Starts a session with the host Cisco E-Series Server.
host clear	Closes the host Cisco E-Series Server session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

The **imc clear** and **host clear** commands close the active session of the CIMC or the host. As a result, the system closes the sessions of any other users currently logged in.

Only one active session is allowed in the CIMC or host at any time. If you receive a “connection refused” message when sessioning in, close the current active session by entering the **imc clear** or **host clear** commands.

Examples

The following example shows how to clear the CIMC session in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 session imc clear
```

Examples

The following example shows how to clear the CIMC session in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 session imc clear
```

ucse shutdown

To shut down the system gracefully, use the **ucse shutdown** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **shutdown**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

Use this command when removing or replacing a hot-swappable module during online insertion and removal (OIR).

Examples

The following example shows how to gracefully shut down an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 shutdown
```

Examples

The following example shows how to gracefully shut down an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 shutdown
```

ucse server start boot

To power on the Cisco E-Series Server using the boot option, use the **ucse server start boot** command in EXEC mode .

ucse *slot* **server start boot** {**url** *url* | **device** *device_type*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from the specified url.
device *device_type*	The device type from which the Cisco E-Series Server boots. It can be one of the following: • CDROM: Virtual-CD • EFI • FDD: Virtual-Floppy • HDD: RAID • HDD: SD2 • HDD: Virtual-HiFD • PXE: GIGETH0 • PXE: GIGETH1 • PXE: GIGETH3

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command to power on the server that was previously turned off.

Examples

The following example shows how to start the Cisco E-Series Server using the boot option:

```
Router# ucse 2 server start boot url http://220.0.0.100/OS/image.iso
```

ucse statistics

To display or clear the reset and reload server information, use the **ucse statistics** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **statistics [clear]**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **statistics [clear]**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
clear	(Optional) Clears the E-Series Server's reset and reload information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to display the server statistics in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 statistics

Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
  Registration request timeout reset count = 0
```

```
  Error recovery timeout reset count = 0
  Module registration count = 1
```

Examples

The following example shows how to display the server statistics in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 statistics

Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 1
```

ucse status

To display configuration information related to the hardware and software of a server, use the **ucse status** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **status** [**detailed**]

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **status** [**detailed**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
detailed	(Optional) Displays detail information about the Cisco E-Series Server such as the status of the service module and settings of the reset and heartbeat-reset flags.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to display server status in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 status

Service Module is Cisco ucse 2/0
Service Module supports session via TTY line 131
Service Module is in Steady state
```

```
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
```

Examples

The following example shows how to display server status in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 status

Service Module is Cisco ucse 0/3
Service Module supports session via TTY line 131
Service Module is in Steady state
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
```

ucse stop

To immediately power down the server, use the **ucse stop** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **stop**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **stop**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to power down an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 stop
Send server stop command
```

Examples

The following example shows how to power down an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 stop

Send server stop command
```

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.

Command Default

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 **showudld** 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 l3 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 udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.
```

```
Enable l3 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 udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.
Enable l3 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 **upgradefpdauto** 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.

Command Default

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 **noupgradefpdauto** command. The **upgradefpdpath** 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.

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

The **routersearchesthe**primary Flash file system (disk0:) for the FPD image package file when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

The router searches all of its Flash file systems for the FPD image package when an FPD incompatibility is detected and **upgradefpdauto** 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**upgradehw-modulesubslot** 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 **showupgradefpdprogress** 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 **upgradefpdauto** 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 ...
*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 **upgradefpdpath** 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 "/".

Command Default

The **upgradefpdpath** 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:

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

The **routersearchesthe**primary Flash file system (disk0:) for the FPD image package file when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

The router searches all of its Flash file systems for the FPD image package when an FPD incompatibility is detected and **upgradefpdauto** 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

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 **upgradefpdpath** 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 XXXXXXX is the FTP password:

```
upgrade fpd path ftp://john:XXXXXXX@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.
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 **upgradefpga** 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.

Command Default

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 **noupgradefpga**. 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 **upgradefpgaall** 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 **upgradefpgaprompt**command was introduced
12.2(20)S6	The **noupgradefpga** command was introduced and became the default setting. The **force** option was introduced. The **noupgradefpgaprompt** command behavior was changed. The **noupgradefpgaprompt** configuration no longer automatically begins an FPGA upgrade when an FPGA mismatch is detected.

Usage Guidelines

Note that **noupgradefpga** 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 **noupgradefpga** is maintained, FPGA is not upgraded when an FPGA mismatch is detected and the user is not prompted regarding an FPGA upgrade. If the **upgradefpgaprompt** command is entered, a prompt asking users whether they would like to perform an FPGA upgrade appears on the console when FPGA

mismatches are detected. If the **upgradefpgaforce** command is entered, an FPGA upgrade occurs automatically when an FPGA mismatch is detected.

In Cisco IOS Releases 12.2(20)S4 and 12.2(20)S5, the **noupgradefpgaprompt** configuration automatically started an FPGA upgrade when an FPGA mismatch was detected. Starting in Cisco IOS Release 12.2(20)S6, the **noupgradefpgaprompt** configuration is the same configuration as **noupgradefpga**. When this setting of **noupgradefpga** is maintained, the FPGA is not upgraded when an FPGA mismatch is detected and the user is not prompted regarding an FPGA upgrade.

While the **noupgradefpga** command can be entered as a configuration command, the **upgradefpga** command cannot be entered unless the **force** or **prompt** options are also entered.

The **force** or **prompt** options are not necessary when entering the no upgrade fpga command. The options can be entered, but the system configuration will revert to the **noupgradefpga** configuration regardless of whether a keyword is entered.

Note that when the FPGA prompt is configured, the prompt appears on the console screen only. If you are connecting to a router using a telnet connection through a line card, SPA, or port adapter, you will not see this prompt. If you are connecting to the router through one of these methods, we recommend not configuring **upgradefpgaprompt** because you will not be able to see the prompt and the prompt will time out.

Examples

In the following example, the system configuration has been changed so that users will be prompted regarding an FPGA upgrade if an FPGA mismatch is detected during bootup or after an OIR hardware insertion.

```
Router# upgrade fpga prompt
```

The following example is the output of a router that has detected an FPGA mismatch when the **upgradefpgaprompt**command is configured. Note the “Upgrade slot 5 LC FPGA? [y/n]” prompt. In this example, the prompt is answered and the FPGA upgrade is performed.

```
The following board(s) have an FPGA image that is different
from the IOS bundled FPGA image
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
                          HARDWARE        FPGA VERSION ESTIMATED TIME
SLOT  FPGA                VERSION    CURRENT    IOS BUNDLED    TO UPDATE
----  ----                --------   -------    ----------- --------------
 5    6T3                  03.03      00.20        00.21       up to 12 minutes
Upgrade slot 5 LC FPGA? [y/n]y
Slot 5 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...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA
flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone

  Comparing with the source file...Passed
Slot 5 LC FPGA successfully updated from version 00.20 to version 00.21
Slot 5 linecard reset after FPGA update...
Slot 5 linecard successfully reset
```

In the following example, the system configuration has been changed so that an FPGA upgrade will occur automatically if an FPGA mismatch is detected during bootup or after an OIR hardware insertion:

```
Router# upgrade fpga force
```

The following example is from a router that has detected an FPGA mismatch when **upgradefpgaforce** is configured. Note that the upgrade occurs automatically without the user being prompted for any information.

```
The following board(s) have an FPGA image that is different
from the IOS bundled FPGA image
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
                          HARDWARE        FPGA VERSION ESTIMATED TIME
SLOT  FPGA                VERSION    CURRENT    IOS BUNDLED    TO UPDATE
----  ----                --------   -------    ----------- --------------
 5    6T3                  03.03      00.20        00.21       up to 12 minutes
Slot 5 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...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA
flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone

  Comparing with the source file...Passed
Slot 5 LC FPGA successfully updated from version 00.20 to version 00.21
Slot 5 linecard reset after FPGA update...
Slot 5 linecard successfully reset
```

In the following example, the default configuration where no prompt and no forced upgrade occurs when an FPGA mismatch occurs is restored.

```
Router# no upgrade fpga
```

The following example is from a router that has detected an FPGA mismatch when **noupgradefpga** is configured. Note that the FPGA upgrade was not performed. If you receive these messages and want to upgrade FPGA, enter the **upgradefpgaall** command to manually perform an FPGA upgrade.

```
00:00:05:%PLATFORM-4-FPGA_MISMATCH:FPGA image in slot 0 (name = NPEG100, hardware version
= 01.00, current fpga version = 02.04) does not match the FPGA image in Cisco IOS software
 (version 02.05). Approximate time to update the FPGA image is 12 minutes.
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.

Command	Description
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 **upgradefpgaall**command in privileged EXEC mode.

upgrade fpga all

Syntax Description

This command has no arguments or keywords.

Command Default

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 **showc7300** command is entered to see FPGA versions after an FPGA upgrade has been performed but not completed by reloading the hardware, the bundled FPGA version should match the Flash memory version. After the hardware is reloaded, the bundled, the Flash, and the system FPGA should all match and the upgrade should be complete.

Examples

The following example shows a manual FPGA upgrade for a router using Cisco IOS Release 12.2(20)S6 or later. Note that the user elects to reject the NPE-G100 upgrade. More importantly, note the user is prompted about reloading the 6T3 line card to complete the FPGA upgrade after electing to perform that FPGA upgrade. In this example, the user decides to reject the card reload for the 6T3 line card in slot 5 and the FPGA upgrade for that card is not finalized.

```
Router# upgrade fpga all
The following board(s) have an FPGA image that is different
from the IOS bundled FPGA image
                          HARDWARE        FPGA VERSION ESTIMATED TIME
SLOT  FPGA                VERSION    CURRENT    IOS BUNDLED    TO UPDATE
----  ----                --------   -------    ----------- --------------
 0    NPEG100              01.00      02.04        02.05       up to 12 minutes
 5    6T3                  03.03      00.20        00.21       up to 12 minutes
Upgrade slot 0 NPEG100 FPGA? [y/n]n
%Warning:FPGA update skipped
Slot 0 NPEG100 FPGA may contain incompatible FPGA version.
This may cause system to be unstable.
00:07:54:%PLATFORM-6-FPGAUPDSKIP:Slot 0 NPEG100 FPGA update skipped.
Upgrade slot 5 LC FPGA? [y/n]y
The card in slot 5 should be reloaded for the new FPGA image to take effect.
Do you want to reload the card? [Y/N]n
Slot 5 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...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA
flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone

  Comparing with the source file...Passed
Slot 5 LC FPGA successfully updated from version 00.20 to version 00.21
00:20:27:%PLATFORM-6-FPGAUPDSUCCESS:Slot 5 LC FPGA successfully updated from version 00.20
 to 00.21.
00:20:27:%PLATFORM-4-FPGAUPD_RELOAD_SKIP:After the FPGA update, the card in slot 5 was not
 reloaded. The card should be reloaded for the new FPGA image to take effect.
```

The following example shows how to manually start the FPGA image update process for an NSE for a router running a pre-Cisco IOS Release 12.2(20)S6 software image:

```
Router# upgrade fpga all
The following board(s) may have incompatible FPGA(s) and may
need an upgrade or downgrade.
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
SLOT  FPGA                CURRENT VERSION  BUNDLED VERSION  ESTIMATED TIME TO
                           ON THE BOARD         IN IOS            UPDATE
----  ----                ---------------  ---------------  -----------------
 0    NSE100 (MB)              00.03            00.12       up to 15 minutes
 0    NSE100 (DB)              00.03            00.10       up to 6 minutes
Upgrade slot 0 NSE MB FPGA? [y/n]y
Upgrade slot 0 NSE DB FPGA? [y/n]y
Slot 0 NSE MB 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...
```

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
 vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
 vvvvvvvvvvvvvDone
Comparing with the source file...Passed
Slot 0 NSE MB FPGA successfully updated from version 0.3 to version 0.12
Slot 0 NSE DB 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...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvvDone
  Comparing with the source file...Passed
Slot 0 NSE DB FPGA successfully updated from version 0.3 to version 0.10
System will be reloaded now for the new FPGA to take effect...
```

The following example shows how to manually update the FPGA image of a line card on a router running pre-Cisco IOS Release 12.2(20)S6 software:

```
Router# upgrade fpga all
The following board(s) may have incompatible FPGA(s) and may
need an upgrade or downgrade.
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
SLOT  FPGA                CURRENT VERSION  BUNDLED VERSION  ESTIMATED TIME TO
                           ON THE BOARD         IN IOS             UPDATE
----  ----                ---------------  ---------------  -----------------
 4    OC48 POS                 00.13            00.12       up to 5 minutes
Downgrade slot 4 LC FPGA? [y/n]y
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...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone
  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.

Command	Description
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 **upgradehw-moduleslot** 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

slot	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 Cisco 7200 VXR Installation and Configuration Guide.
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.
file	Specifies that a file will be downloaded.
file-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.
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.

Command Default

No default behavior or values.

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 **upgradehw-moduleslot** command is used to manually upgrade the FPD images; therefore, the **upgradehw-moduleslot**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 **noupgradefpdauto** 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 **showupgradefpdprogress** 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 **upgradehw-moduleslotfpdfile**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

slot	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 Cisco 7200 VXR Installation and Configuration Guide .
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.
file-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.
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.

Command Default

No default behavior or values.

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 **noupgradefpdauto** 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 **showupgradefpdprogress** 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/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
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.
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.

Note The upgrade hw-module subslot command is not available in Cisco IOS Release 12.0(33)S2 and later Cisco IOS 12.0S 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 **upgradehw-modulesubslot** 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

slot	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.
subslot	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.
file-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.
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.

Command Default

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 **upgradehw-modulesubslot** command is used to manually upgrade the FPD images; therefore, the **upgradehw-modulesubslot**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 **noupgradefpdauto** command can be entered to disable automatic FPD upgrades.

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.

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 **showupgradeprogress** 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.

Command	Description
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatability 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	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 **upgradehw-modulesubslotfpdfile**command in privileged EXEC mode.

Cisco 7304 and Cisco uBR10012 Universal Broadband Router
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

slot	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.
subslot	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-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.
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.

Command Default

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 **noupgradefpdauto** command can be entered to disable automatic FPD upgrades.

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.

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.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

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 **showupgradeprogress** 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 **upgradehw-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.
filename	Specifies the hw-programmable upgrade package file and its file system location. For filename, specify one of the following system locations and a package file name: • 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 upgade on a Cisco ASR 1000 Series Router. The package file name is typically named asr1000-hw-programmables.<release_name>.pkg.
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 **upgraderom-monitordefault** 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.

Command Default

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 **upgradesatellitesatellite** command in privileged EXEC mode.

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

Syntax Description

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

utc offset leap-second offset

To configure the current UTC offset, leap second event date and Offset value (+1 or -1), use the **utc offset leap-second offset** command in PTP clock configuration mode.

utc offset *value* **leap-second** *"date time"* **offset** {**-1** | **1**}

Syntax Description

value	Current UTC offset value. Valid values are from 0-255. The default value is 36.
"date time"	Leap second effective date in dd-mm-yyyy hh:mm:ss format.

Command Default

By default no UTC offset or leap second is configured.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
Cisco IOS XE 3.18SP	This command was introduced.
Cisco IOS XE 3.18.1SP	This command was modified. The **leap-second** and **offset** keywords were added.

Usage Guidelines

Use the **utc offset leap-second offset** command to configure the current UTC offset, leap second event date and Offset value (+1 or -1).

The following example shows how to configure the current UTC offset, leap second event date and offset value:

```
Device(config)# ptp clock boundary domain 0 hybrid
Router(config-ptp-clk)# time-properties persist 600
Router(config-ptp-clk)#utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
```

Related Commands

Command	Description
time-properties persist	Configures time properties holdover time.

vectoring

To enable the vectoring mode in C86xVAE platforms, use the **vectoring** command in controller configuration mode. To restore the default value, use the **no** form of this command.

vectoring {friendly | none}

no vectoring

Syntax Description

friendly	Enables friendly vectoring mode in both Annex A and Annex B.
none	Disables vectoring mode completely.

Command Default

Default mode is Vectoring friendly in Annex A and Annex B from Release 15.6(3)M.

Command Modes

Controller Configuration (config-controller)

Command History

Release	Modification
15.6(3)M	This command was introduced on the Cisco C86xVAE series routers.

Usage Guidelines

This command is used to enable or disable vectoring on C867VAE-K9 and C866VAE-K9 platforms. By default, the vectoring is friendly on both annex A and Annex B. This command is introduced under "controller vdsl 0" mode.

Examples

The following example shows how to enable vectoring :

```
Router(config-controller)#vectoring friendly
```

The following example shows how to disable vectoring :

```
Router(config-controller)#vectoring none
```

Related Commands

Command	Description
controller vdsl	Configures the controller status.

vtg

To configure the Circuit Emulation Services over Packet Switched Network (CESoPSN) CEM group, use the **vtg** command in controller configuration STS mode.

vtg *vtg_number* **t1** *t1_line_number* **cem-group** *channel-number* **timeslots** *list-of-timesolts*

Syntax Description

For NCS 4200 Series Routers:

vtg *vtg-number* **vt** *vt-line-number* **cem-group** *cem-group-number* **cep**

vtg_number	Specifies the VTG number. The range is 1 to 7.
t1	Specifies the T1 line configuration.
t1_line_number	Specifies the T1 line number. The range is 1 to 4.
cem-group	Specifies the timeslots to CEM group mapping.
channel-number	Specifies the channel number. The range is 0 to 2015.
timeslots	Specifies the timeslots in the CEM group.
list-of-timesolts	Specifies the list of timeslots. The range is 1 to 24
vt	Specifies the Virtual Tributary (VT) under vtg of STS.
vt-line-number	Specifies the VT line number.
cem-group	Specifies the CEM group for T1 line.
cem-group-number	The *cem-group-number* keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.
cep	Configures Circuit Emulation Service over Packet (CEP) mode.

Command Default

None

Command Modes

Controller configuration STS

Command History

Release	Modification
15.1(01)S	This command was introduced on the Cisco 7600 routers.
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Examples

This example shows how to configure the (CESoPSN) CEM group:

```
Router(config)# controller sonet-acr 1
```

```
Router(config-controller)#
sts-1 2
Router (config-ctrlr-sts1)#vtg 2 T1 2 cem-group 2 timeslots 2
```

Examples

For NCS 4200 Series, this command is used to configure the VT-15 CEP mode:

```
enable
configure terminal
controller Mediatype 0/5/0
controller sonet 0/5/0
sts-1 1
vtg 1 vt 1 cem-group 100 cep
end
```

Related Commands

Command	Description
sts-1	Configures the Synchronous Transport Signal (STS) (level)-1 in the SONET hierarchy.
mode vt-15	Configures the path operation mode.
controller sonet-acr	Configures the SONET Access Circuit Redundancy (ACR) virtual controller.
show controller sonet	Displays SONET controller configuration.

wanphy flag j1 transmit

T o 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 **wanphyflagj1transmit***byte-value*commandin 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 **wanphyflagj1transmit**command has been 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

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

wanphy report-alarm {*defaultlinepathsectionwis*}
no wanphy threshold

Syntax Description

default	Alarm reporting of line, section, and path to their default configured values.
line	The line-level alarm reporting status.
path	The path-level alarm reporting status.
section	The section-level alarm reporting status.
wis	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 **wanphyreport-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 **nowanphyreport-alarm** command.

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

T o 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 **wanphythreshold**commandin the Controller configuration mode. To reset the threshold alarm values to its default values, use the **no** form of the command.

wanphy threshold {*b1-tcab2-tcasd-bersf-ber*}
no wanphy threshold

Syntax Description

b1-tca	The B1 BER threshold-crossing alarm value. The default b1-tca value is 10e-6. The valid range is 4 to 9.
b2-tca	The B2 BER threshold-crossing alarm values. The default b2-tca value is 10e-6. The valid range is 3 to 9.
sd-ber	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.
sf-ber	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 **wanphythreshold**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

remote-ip-address	IP address of an interface--physical or loopback--on the destination router.
virtual-connect-ID	Virtual connect ID (VCID). For CEM over IP (CEoIP), you must enter a value of 0.
encapsulation	Sets the encapsulation type.
encapsulation-type	Encapsulation type. You must set the encapsulation type to UDP. For Cisco NCS 4200 Series, you must set the encapsulation type to mpls.

Command Default

No CEM connections are built.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
XE 3.18SP	This command was implemented on the Cisco NCS 4200 Series.
XE 3.18.1SP	This command was implemented on the Cisco ASR 900 Series Routers.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 920 Routers.

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)#
```

Examples

The following example shows how to enter CEM xconnect configuration mode.

```
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-xconnect)#
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.

Command	Description
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.

Command Default

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
```