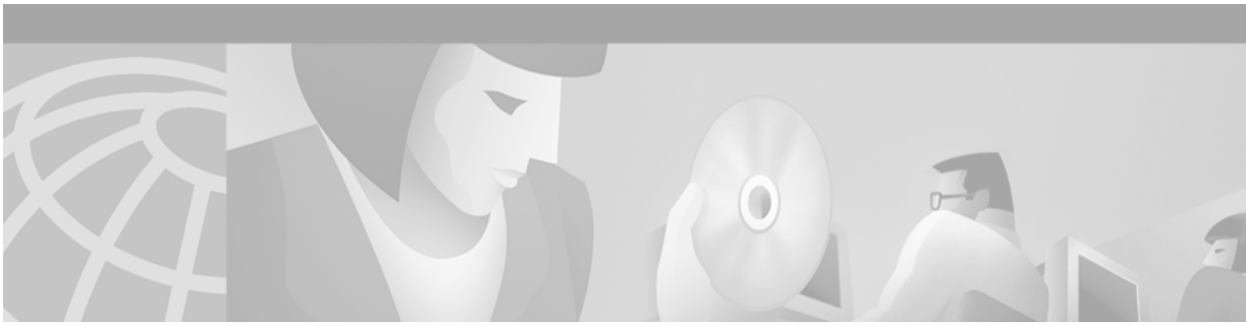

Cisco Nonstop Forwarding

Feature History

Release	Modification
12.0(22)S	This feature was introduced.

This document describes the Cisco Nonstop Forwarding (NSF) feature in Cisco IOS Release 12.0(22)S. It includes the following sections:

Note Throughout this document, the term "Route Processor" (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted. For example, on the Cisco 10000 series Internet router the RP is referred to as the Performance Routing Engine (PRE), on the Cisco 12000 series Internet router the RP is referred to as the Gigabit Route Processor (GRP), and on the Cisco 7500 series router the RP is referred to as the Route Switch Processor (RSP).

Feature Overview

Cisco NSF works with the Stateful Switchover (SSO) feature in Cisco IOS software. SSO is a prerequisite of Cisco NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco NSF is to continue forwarding IP packets following a route processor (RP) switchover.

Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. Cisco NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to Cisco NSF operation.

SSO Dependency

Cisco NSF always runs together with SSO. This section provides some background information on the SSO feature.

In specific Cisco networking devices that support dual RPs, SSO establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizes information between them. A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

In networking devices running SSO, both RPs must be running the same configuration so that the standby RP is always ready to assume control following a fault on the active RP. The configuration information is synchronized from the active RP to the standby RP at startup and whenever changes to the active RP configuration occur. Following an initial synchronization between the two processors, SSO maintains RP state information between them, including forwarding information.

During switchover, system control and routing protocol execution is transferred from the active processor to the standby processor. The time required by the device to switch over from the active to the standby processor ranges from just a few seconds to approximately 30 seconds, depending on the platform.

SSO supported protocols and applications must be high-availability (HA)-aware. A feature or protocol is HA aware if it maintains, either partially or completely, undisturbed operation through an RP switchover. For some HA aware protocols and applications, state information is synchronized from the active to the standby processor. For Cisco NSF, enhancements to the routing protocols (Cisco Express Forwarding, or CEF; Open Shortest Path First, or OSPF; Border Gateway Protocol, or BGP; and Intermediate System-to-Intermediate System, or IS-IS) have been made to support the HA features in SSO.

For more information on SSO, see the section “Related Documents.”

Cisco NSF Routing and Forwarding Operation

Cisco NSF is supported by the BGP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. Of the routing protocols, BGP, OSPF, and IS-IS have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices. The IS-IS protocol can be configured to use state information that has been synchronized between the active and the standby RP to recover route information following a switchover instead of information received from peer devices.

In this document, a networking device is said to be NSF-aware if it is running NSF-compatible software. A device is said to be NSF-capable if it has been configured to support NSF; therefore, it would rebuild routing information from NSF-aware or NSF-capable neighbors.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

Table 1 lists the routing protocol and CEF support in Cisco NSF.

Table 1 Routing Protocol and CEF Support in Cisco NSF

Protocol	Platform	NSF Support in Cisco IOS Software Release 12.0(22)S
BGP	Cisco 7200	Yes[1]
	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes
OSPF	Cisco 7200	Yes[1]
	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes
IS-IS	Cisco 7200	Yes[1]
	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes
CEF	Cisco 7200	N/A[2]
	Cisco 7500	Yes
	Cisco 10000	Yes
	Cisco 12000	Yes

1. The Cisco 7200 is a single-route processor system and cannot maintain its forwarding table in the event of a route processor failure. It cannot perform nonstop forwarding of packets. However, it supports the NSF protocol extensions for BGP, OSPF, and ISIS. Therefore, it can peer with NSF-capable routers and facilitate the resynchronization of routing information with such routers.
2. The Cisco 7200 is a single processor device and does not support SSO; therefore, CEF support for NSF does not apply.

Cisco Express Forwarding

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the

forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates to CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version ("epoch") number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

Routing Protocols

The routing protocols run only on the active RP, and they receive routing updates from their neighbor routers. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables. Alternately, the IS-IS protocol can be configured to synchronize state information from the active to the standby RP to help rebuild the routing table on the NSF-capable device in environments where neighbor devices are not NSF-aware.

Note For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information.

BGP Operation

When a NSF-capable router begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a declaration that the NSF-capable device has "graceful restart capability." Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the NSF-capable router and its BGP peer(s) need to exchange the Graceful Restart Capability in their OPEN messages, at the time of session establishment. If both the peers do not exchange the Graceful Restart Capability, the session will not be graceful restart capable.

If the BGP session is lost during the RP switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable router as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the NSF-capable router reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable router as having restarted.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding information. The NSF-aware device uses the network information to remove stale routes from its BGP table. Following that, the BGP protocol is fully converged.

If a BGP peer does not support the graceful restart capability, it will ignore the graceful-restart capability in an OPEN message but will establish a BGP session with the NSF-capable device. This function will allow interoperability with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware BGP peers will not be graceful restart capable.

Note BGP support in NSF requires that neighbor networking devices be NSF-aware; that is, the devices must have the Graceful Restart Capability and advertise that capability in their OPEN message during session establishment. If an NSF-capable router discovers that a particular BGP neighbor does not have Graceful Restart Capability, it will not establish an NSF-capable session with that neighbor. All other neighbors that have Graceful Restart Capability will continue to have NSF-capable sessions with this NSF-capable networking device.

OSPF Operation

When an OSPF NSF-capable router performs an RP switchover, it must perform two tasks in order to resynchronize its Link State Database with its OSPF neighbors. First, it must relearn the available OSPF neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the Link State Database for the network.

As quickly as possible after an RP switchover, the NSF-capable router sends an OSPF NSF signal to neighboring NSF-aware devices. Neighbor networking devices recognize this signal as a cue that the neighbor relationship with this router should not be reset. As the NSF-capable router receives signals from other routers on the network, it can begin to rebuild its neighbor list.

Once neighbor relationships are reestablished, the NSF-capable router begins to resynchronize its database with all of its NSF-aware neighbors. At this point, the routing information is exchanged between the OSPF neighbors. Once this exchange is complete, the NSF-capable device uses the routing information to remove stale routes, update the RIB, and update the FIB with the new forwarding information. The OSPF protocols are then fully converged.

Note OSPF NSF requires that all neighbor networking devices be NSF-aware. If an NSF-capable router discovers that it has non-NSF -aware neighbors on a particular network segment, it will disable NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware routers will continue to provide NSF capabilities.

IS-IS Operation

When an IS-IS NSF-capable router performs an RP switchover, it must perform two tasks in order to resynchronize its Link State Database with its IS-IS neighbors. First, it must relearn the available IS-IS neighbors on the network without causing a reset of the neighbor relationship. Second, it must reacquire the contents of the Link State Database for the network.

The IS-IS NSF feature offers two options when configuring NSF:

- Internet Engineering Task Force (IETF) IS-IS
- Cisco IS-IS

If neighbor routers on a network segment are NSF-aware, meaning that neighbor routers are running a software version that supports the IETF Internet draft for router restartability, they will assist an IETF NSF router which is restarting. With IETF, neighbor routers provide adjacency and link-state information to help rebuild the routing information following a switchover. A benefit of IETF IS-IS configuration is operation between peer devices based on a proposed standard.

Note If you configure IETF on the networking device, but neighbor routers are not IETF-compatible, NSF will abort following a switchover.

If the neighbor routers on a network segment are not NSF-aware, you must use the Cisco configuration option. The Cisco IS-IS configuration transfers both protocol adjacency and link-state information from the active to the standby RP. A benefit of Cisco configuration is that it does not rely on NSF-aware neighbors.

IETF IS-IS Configuration

Using the IETF IS-IS configuration, as quickly as possible after an RP switchover, the NSF-capable router sends IS-IS NSF restart requests to neighboring NSF-aware devices. Neighbor networking devices recognize this restart request as a cue that the neighbor relationship with this router should not be reset, but that they should initiate database resynchronization with the restarting router. As the restarting router receives restart request responses from routers on the network, it can begin to rebuild its neighbor list.

Once this exchange is complete, the NSF-capable device uses the link-state information to remove stale routes, update the RIB, and update the FIB with the new forwarding information. IS-IS is then fully converged.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. The IS-IS NSF operation waits for a specified interval to ensure that connections are stable before attempting another restart of IS-IS NSF. This functionality prevents IS-IS from attempting back-to-back NSF restarts with stale information.

Cisco IS-IS Configuration

Using the Cisco configuration option, full adjacency and LSP information is saved, or "checkpointed," to the standby RP. Following a switchover, the newly active RP maintains its adjacencies using the checkpointed data, and can quickly rebuild its routing tables.

Note Following a switchover, Cisco IS-IS NSF has complete neighbor adjacency and LSP information; however, it must wait for all interfaces that had adjacencies prior to the switchover to come up. If an interface does not come up within the allocated interface wait time, the routes learned from these neighbor devices are not considered in routing table recalculation. IS-IS NSF provides a command to extend the wait time for interfaces that, for whatever reason, do not come up in a timely fashion.

The switchover from one RP to the other happens within seconds. IS-IS reestablishes its routing table and resynchronizes with the network within a few additional seconds. At this point, IS-IS waits for a specified interval before it will attempt a second NSF restart. During this time, the new standby RP will boot up and synchronize its configuration with the active RP. Once this synchronization is completed, IS-IS adjacency and LSP data is checkpointed to the standby RP; however, a new NSF restart will not be attempted by IS-IS until the interval time expires. This functionality prevents IS-IS from attempting back-to-back NSF restarts.

Benefits

Improved Network Availability

NSF continues forwarding network traffic and application state information so that user session information is maintained after a switchover.

Overall Network Stability

Network stability may be improved with the reduction in the number of route flaps that had been created when routers in the network failed and lost their routing tables.

Neighboring Routers Do Not Detect a Link Flap

Because the interfaces remain up across a switchover, neighboring routers do not detect a link flap (the link does not go down and come back up).

Prevents Routing Flaps

Because SSO continues forwarding network traffic in the event of a switchover, routing flaps are avoided.

No Loss of User Sessions

User sessions established prior to the switchover are maintained.

Restrictions

General Restrictions

- For NSF operation, you must have SSO configured on the device.

BGP NSF

- All neighboring devices participating in BGP NSF must be NSF-capable, having been configured for BGP graceful restart as specified in the "Configuring BGP NSF" section.

OSPF NSF

- OSPF NSF for virtual links is not supported.
- All OSPF networking devices on the same network segment must be NSF-aware (running an NSF software image).

IS-IS NSF

- For IETF IS-IS, all neighboring devices must be running an NSF-aware software image.

Cisco 7200 Series Router

- The Cisco 7200 series router has a single CPU; therefore, it cannot support the stateful switchover in the event of a network processor engine (NPE) fault.

  The Cisco 7206 does support NSF and can operate in a peer role with a Cisco 7500, 10000, or 12000 series router running Cisco IOS Release 12.0(22)S. With NSF enabled, an RP switchover on the Cisco 7500, 10000, or 12000 series router peer should not cause a loss of PPP, ATM, high-level data link control (HDLC), or Frame Relay sessions, or a loss of any OSPF, BGP, or IS-IS adjacencies established between the Cisco 7200 and the peer.

Related Features and Technologies

- Stateful Switchover
- BGP
- OSPF

- IS-IS
- CEF

Related Documents

- *Stateful Switchover*, Cisco IOS Release 12.0(22)S feature module
- *Cisco IOS Network Protocols Configuration Guide, Part 1*, Release 12.0
- *Cisco IOS Switching Services Configuration Guide*, Release 12.0

Supported Platforms

The NSF feature is supported on the following platforms:

- Cisco 7500 series
- Cisco 10000 series
- Cisco 12000 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

Restart Signaling for ISIS, Internet Engineering Task Force (IETF) Network Working Group Internet Draft, September 2001

MIBs

- *Graceful Restart Mechanism for BGP* (draft-ietf-idr-restart-05.txt)

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- NSF must be configured on a networking device that has been configured for SSO.
- On platforms supporting the Route Switch Processor (RSP), and where the CEF switching mode is configurable, configure distributed CEF (dCEF) switching mode using the **ip cef distributed** command.

Configuration Tasks

See the following sections for configuration tasks for the SSO feature. Each task in the list is identified as either required or optional.

- Configuring CEF NSF (required)
- Configuring BGP NSF (required)
- Configuring OSPF NSF (required)
- Configuring IS-IS NSF (required)
- Verifying CEF NSF (optional)
- Verifying BGP NSF (optional)
- Verifying OSPF NSF (optional)
- Verifying IS-IS NSF (optional)

Configuring CEF NSF

The CEF NSF feature operates by default while the networking device is running in SSO mode. No configuration is necessary.

Configuring BGP NSF

Note You must configure BGP graceful restart on all peer devices participating in BGP NSF.

To configure BGP for NSF, use the following commands beginning in privileged EXEC mode, and repeat this procedure on each of the BGP NSF peer devices:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# router bgp` *as-number*	Enables a BGP routing process, which places the router in router configuration mode.
Step 3	`Router(config-router)# bgp graceful-restart`	Enables the BGP graceful restart capability, starting NSF for BGP. If you enter this command after the BGP session has been established, you must restart the session for the capability to be exchanged with the BGP neighbor. Use this command on the restarting router and all of its peers.

Configuring OSPF NSF

Note All peer devices participating in OSPF NSF must be made OSPF NSF-aware, which happens automatically once you install an NSF software image on the device.

To configure NSF for OSPF, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# router ospf` *processID*	Enables an OSPF routing process, which places the router in router configuration mode.
Step 3	`Router(config-router)# nsf`	Enables NSF operations for OSPF.

Configuring IS-IS NSF

To configure NSF for IS-IS, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# router isis [tag]`	Enables an IS-IS routing process, which places the router in router configuration mode.
Step 3	`Router(config-router)# nsf [cisco | ietf]`	Enables NSF operation for IS-IS. Enter the **ietf** keyword to enable IS-IS in homogeneous network where adjacencies with networking devices supporting IETF draft-based restartability is guaranteed. Enter the **cisco** keyword to run IS-IS in heterogeneous networks that might not have adjacencies with NSF-aware networking devices.
Step 4	`Router(config-router)# nsf interval [minutes]`	(Optional) Specifies the minimum time between NSF restart attempts. The default time between *consecutive* NSF restart attempts is 5 minutes.
Step 5	`Router(config-router)# nsf t3 {manual [seconds] | adjacency}`	(Optional) Specifies the time IS-IS will wait for the IS-IS database to synchronize before generating overloaded link-state information for itself and flooding that information out to its neighbors. The **t3** keyword applies only if you selected **IETF** operation. Specifying **adjacency** means that the restarting router obtains its wait time from neighboring devices.
Step 6	`Router(config-router)# nsf interface wait seconds`	(Optional) Specifies how long an IS-IS NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart. The default is 10 seconds.

Verifying CEF NSF

To verify that CEF is NSF-capable, use the **show cef state** command:

```
router# show cef state

CEF Status [RP]
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
CEF default capabilities:
Always FIB switching:      yes
Default CEF switching:     yes
Default dCEF switching:    yes
Update HWIDB counters:     no
```

```
Drop multicast packets:    no
.
.
.
CEF NSF capable:           yes
IPC delayed func on SSO:   no
RRP state:
I am standby RRP:          no
My logical slot:           0
RF PeerComm:               no
```

Verifying BGP NSF

To verify NSF for BGP, you must check that the graceful restart function is configured on the SSO-enabled networking device and on the neighbor devices. Perform the following steps:

Step 1 Verify that "bgp graceful-restart" appears in the BGP configuration of the SSO-enabled router by entering the **show running-config** command:

```
Router# show running-config

.
.
.
router bgp 120
.
.
.
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
.
.
.
```

Step 2 Repeat step 1 on each of the BGP neighbors.

Step 3 On the SSO device and the neighbor device, verify that the graceful restart function is shown as both advertised and received, and confirm the address families that have the graceful restart capability. If no address families are listed, then BGP NSF also will not occur:

```
router#show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
    Address family IPv4 Unicast:advertised and received
    Address famiiy IPv4 Multicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

Verifying OSPF NSF

To verify NSF for OSPF, you must check that the NSF function is configured on the SSO-enabled networking device. Perform the following steps:

Step 1 Verify that 'nsf' appears in the OSPF configuration of the SSO-enabled device by entering the **show running-config** command:

```
Router# show running-config

router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
.
.
.
```

Step 2 Use the **show ip ospf** command to verify that NSF is enabled on the device:

```
router> show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
 Area has no authentication
 SPF algorithm executed 3 times
```

Verifying IS-IS NSF

To verify NSF for IS-IS, you must check that the NSF function is configured on the SSO-enabled networking device. Perform the following steps:

Step 1 Verify that 'nsf' appears in the IS-IS configuration of the SSO-enabled device by entering the **show running-config** command. The display will show either Cisco IS-IS or IETF IS-IS configuration. The following display indicates that the device uses the Cisco implementation of IS-IS NSF:

```
Router# show running-config
.
.
.
router isis
nsf cisco
.
.
.
```

Step 2 If the NSF configuration is set to **cisco**, use the **show isis nsf** command to verify that NSF is enabled on the device. Using the Cisco configuration, the display output will be different on the active and standby RPs. The following display shows sample output for the Cisco configuration on the active RP. In this example, note the presence of "NSF restart enabled":

```
router# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

The following display shows sample output for the Cisco configuration on the standby RP. In this example, note the presence of "NSF restart enabled":

```
router# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

Step 3 If the NSF configuration is set to **ietf**, enter the **show isis nsf** command to verify that NSF is enabled on the device. The following display shows sample output for the IETF IS-IS configuration on the networking device:

```
router# show isis nsf

NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

```
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

Troubleshooting Tips

To troubleshoot the NSF feature, use the following commands in privileged EXEC mode, as needed:

Command	Purpose
Router# **clear cef epoch**	Begins a new epoch and increments the epoch number for a CEF table.
Router# **debug isis nsf** [**detail**]	Displays information about the IS-IS state during a Cisco NSF restart.
Router# **debug ospf nsf** [**detail**]	Displays debugging messages related to OSPF Cisco NSF commands.
Router# **show cef nsf**	Displays the current NSF state of CEF on both the active and standby RPs.
Router# **show cef state**	Displays the state of CEF on a networking device.
Router# **show clns neighbors**	Display both end-system (ES) and intermediate system (IS) neighbors.
Router> **show ip bgp**	Displays entries in the BGP routing table.
Router# **show ip bgp neighbor**	Displays information about the TCP and BGP connections to neighbor devices.
Router# **show ip cef**	Displays entries in the FIB that are unresolved, or displays a FIB summary.
Router> **show ip ospf**	Displays general information about OSPF routing processes.
Router> **show ip ospf neighbor** [**detail**]	Displays OSPF-neighbor information on a per-interface basis.
Router# **show isis database** [**detail**]	Displays the IS-IS link-state database.
Router# **show isis nsf**	Displays the current state information regarding IS-IS Cisco NSF.

The following tips may help you to troubleshoot the device.

The system displays FIB errors.

Use the **show cef state** command to verify that distributed CEF switching is enabled on your platform. To enable distributed CEF, enter the **ip cef distributed** command in global configuration mode on the active RP.

Note For Cisco 10000 series Internet routers and Cisco 12000 series Internet routers, distributed CEF is always enabled and is not configurable.

Cannot determine if an OSPF neighbor is NSF-aware.

To verify whether an OSPF neighbor device is NSF-aware and if NSF is operating between them, use the **show ip ospf neighbor detail** command.

The system loses, or appears to lose, adjacencies with network peers following a stateful switchover.

Use the **show clns neighbors detail** command **to** find any neighbors that do not have "NSF capable" and make sure that they are running NSF-aware images.

Additionally, for ISIS, the standby RP must be stable for 5 minutes (default) before another restart can be initiated. Use the **nsf interval** command to reset the restart period.

Configuration Examples

This section provides the following configuration examples:

- Configuring BGP NSF Example
- Configuring BGP NSF Neighbor Device Example
- Configuring OSPF NSF Example
- Configuring IS-IS NSF Example

Configuring BGP NSF Example

The following example configures BGP NSF on a networking device:

```
router# configure terminal
router(config)# router bgp 590
router(config-router)# bgp graceful-restart
```

Configuring BGP NSF Neighbor Device Example

The following example configures BGP NSF on a neighbor router. All devices supporting BGP NSF must be NSF-aware, meaning that these devices recognize and advertise graceful restart capability.

```
router# configure terminal
router(config)# router bgp 770
router(config-router)# bgp graceful-restart
```

Configuring OSPF NSF Example

The following example configures OSPF NSF on a networking device:

```
router# configure terminal
router(config)# router ospf 400
router(config-router)# nsf
```

Configuring IS-IS NSF Example

The following example configures Cisco proprietary IS-IS NSF operation on a networking device:

```
router# configure terminal
router(config)# router isis
router(config-router)# nsf cisco
```

The following example configures IS-IS NSF for IETF operation on a networking device:

```
router# configure terminal
router(config)# router isis
router(config-router)# nsf ietf
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS high-availability command reference publications for various releases.

New Commands

- **bgp graceful-restart**
- **debug ip ospf nsf**
- **debug isis nsf**
- **nsf (IS-IS)**
- **nsf (OSPF)**
- **nsf interface wait**
- **nsf interval**
- **nsf t3**
- **show cef nsf**
- **show cef state**
- **show isis nsf**

Modified Commands

- **clear ip cef epoch**
- **show clns neighbors**
- **show ip bgp**
- **show ip bgp neighbors**
- **show ip cef**
- **show ip ospf**
- **show ip ospf neighbor**

bgp graceful-restart

To enable the Border Gateway Protocol (BGP) graceful restart capability, use the **bgp graceful-restart** command in router configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]

no bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]

Syntax Description

restart-time	(Optional) Used to set the maximum time to wait for a graceful-restart-capable neighbor to come back up after a restart. The default is 120 seconds.
stalepath-time	(Optional) Used to set the maximum time to hold on to the stale paths of a gracefully restarted peer. All stale paths are deleted after the expiration of this timer. The default is 360 seconds.
seconds	(Optional) The **restart-time** or **stalepath-time** value in number of seconds. The valid range is from 1 to 3600 seconds.

Defaults

BGP Cisco Nonstop Forwarding (NSF) is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The BGP graceful restart capability is negotiated in the OPEN message. If the user enters the **bgp graceful-restart** command after the BGP session is established, the session will need to be restarted.

When you enter the **bgp graceful-restart** command, the **bgp graceful-restart restart-time** and **bgp graceful-restart stalepath-time** commands are enabled by default. After the **bgp graceful-restart** command is used to configure the graceful restart capability, you may tune the configuration using the **restart-time** and **stalepath-time** keywords. If you do not first configure the graceful restart capability using the **bgp graceful-restart** command, the tuning values will not appear in the configuration file.

We recommend that the **bgp graceful-restart restart-time** and **bgp graceful-restart stalepath-time** commands remain set to their default values.

Examples

The following example shows how to configure the BGP graceful restart capability. Enter one command per line:

```
Router# configure terminal
Router(config)# router bgp 65001
Router(config-router)# bgp graceful-restart
Router(config-router)# end
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

clear ip cef epoch

To begin a new epoch and increment the epoch number for a Cisco Express Forwarding (CEF) table, use the **clear ip cef epoch** command in privileged EXEC mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

clear ip cef epoch [**all-vrfs | full | vrf** [*name*]]

no clear ip cef epoch [**all-vrfs | full | vrf** [*name*]]

Syntax Description

all-vrfs	(Optional) Begin a new epoch for all CEF tables.
full	(Optional) Begin a new epoch for all tables, including adjacency tables.
vrf	(Optional) Begin a new virtual private network (VPN) routing and forwarding instance CEF table.
name	(Optional) VPN VRF instance name.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)EX	This command was introduced.
12.0(22)S	This command was introduced on Cisco 7500, 10000, 12000 series Internet routers.

Usage Guidelines

Use the **clear ip cef epoch** command when you want to rebuild a table. This command allows old and new table entries to be distinguished within the same data structure and allows you to retain the old CEF database table while constructing the new table.

Examples

The following example shows the output before and after you clear the epoch table and increment the epoch number:

```
router# show ip cef epoch

CEF epoch information:

Table: Default-table
 Table epoch: 2 (43 entries at this epoch)

Adjacency table
 Table epoch: 2 (5 entries at this epoch)

router# clear ip cef epoch full
```

```
router# show ip cef epoch

CEF epoch information:
Table: Default-table
 Table epoch: 3 (43 entries at this epoch)

Adjacency table
 Table epoch: 3 (5 entries at this epoch)
```

Related Commands

Command	Description
show cef state	Displays the state of CEF.

debug ip ospf nsf

To display debugging messages about Open Shortest Path First (OSPF) during a Cisco Nonstop Forwarding (NSF) restart, use the **debug ip ospf nsf** command in privileged EXEC mode. To disable the display of debugging output, use the **no** form of this command.

debug ip ospf nsf [**detail**]

no debug ip ospf nsf [**detail**]

Syntax Description

detail	(Optional) Displays detailed debug messages.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

Use the **debug ip ospf nsf** command to diagnose problems with OSPF link-state database (LSDB) resynchronization and NSF operations.

Examples

The following example shows that OSPF NSF events debugging is enabled:

```
router# debug ip ospf nsf
```

Related Commands

Command	Description
nsf (OSPF)	Configures NSF operations for OSPF.
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf neighbor	Displays OSPF-neighbor information on a per-interface basis.

debug isis nsf

To display information about the Intermediate System-to-Intermediate System (IS-IS) state during a Cisco Nonstop Forwarding (NSF) restart, use the **debug isis nsf** command in EXEC mode. To disable debugging output, use the **no** form of this command.

debug isis nsf [**detail**]

no debug isis nsf [**detail**]

Syntax Description

detail	(Optional) Provides detailed debugging information.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

Use the **debug isis nsf** command to display basic information about the IS-IS state during an NSF restart. Use the **debug isis nsf detail** command to display additional IS-IS state detail during an NSF restart.

Examples

The following example displays IS-IS state information during an NSF restart:

```
router# debug isis nsf

IS-IS NSF events debugging is on
```

The following example displays detailed IS-IS state information during an NSF restart:

```
router# debug isis nsf detail

IS-IS NSF events (detailed) debugging is on
router#
Jan 24 20:04:54.090:%CLNS-5-ADJCHANGE:ISIS:Adjacency to gsr1 (GigabitEthernet2/0/0) Up,
Standby adjacency
Jan 24 20:04:54.090:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/1, cnt 0/1, ht 10 (NEW)
Jan 24 20:04:54.142:ISIS-NSF:Rcv LSP - L2 000B.0000.0000.00-00, seq 251, csum B0DC, ht
120, len 123 (local)
Jan 24 20:04:55.510:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.00-00, seq 23E, csum D20D, ht
120, len 100 (local)
Jan 24 20:04:56.494:ISIS-NSF:ADJ:000C.0000.0000 (Gi2/0/0), type 8/0, cnt 0/1, ht 30
Jan 24 20:04:56.502:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.01-00, seq 21C, csum 413, ht 120,
len 58 (local)
Jan 24 20:04:58.230:ISIS-NSF:Rcv LSP - L2 000C.0000.0000.00-00, seq 11A, csum E197, ht
1194, len 88 (Gi2/0/0)
Jan 24 20:05:00.554:ISIS-NSF:Rcv LSP - L1 000B.0000.0000.00-00, seq 23F, csum 1527, ht
120, len 111 (local)
```

Related Commands

Command	Description
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interface wait	Specifies how long an NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf interval	Specifies the minimum time between NSF restart attempts.
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
show clns neighbors	Displays both ES and IS neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf (IS-IS)

To configure Cisco Nonstop Forwarding (NSF) operations for Intermediate System-to-Intermediate System (IS-IS), use the **nsf** command in router configuration IS-IS mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

nsf [**cisco** | **ietf**]

no nsf [**cisco** | **ietf**]

Syntax Description

cisco	(Optional) Enables Cisco proprietary IS-IS NSF.
ietf	(Optional) Enables IETF IS-IS NSF.

Defaults

NSF is disabled by default.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The user must configure NSF operation only if a router is expected to perform NSF during restart. The optional **cisco** keyword enables the use of checkpointing to allow the standby route processor (RP) to restore protocol state when an NSF restart occurs.

Examples

The following example enables Cisco proprietary IS-IS NSF operation:

```
nsf cisco
```

The following example enables IETF IS-IS NSF operation:

```
nsf ietf
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf interval	Specifies the minimum time between NSF restart attempts.
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.

Command	Description
show clns neighbors	Displays both ES and IS neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf (OSPF)

To configure Cisco Nonstop Forwarding (NSF) operations for Open Shortest Path First (OSPF), use the **nsf** command in router configuration OSPF mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

nsf [**enforce global**]

no nsf [**enforce global**]

Syntax Description

enforce global	(Optional) Cancels NSF restart when non-NSF-aware neighboring networking devices are detected.

Defaults

NSF is disabled by default.

Command Modes

Router configuration OSPF

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

In router configuration mode, enter OSPF mode to enter and use this command. The user must configure NSF operation only if a router is expected to perform NSF during restart. For users to have full NSF benefits, all neighbors of the specified router must be NSF-aware.

If non-NSF-aware neighbors are detected on a network interface, NSF restart is aborted on that interface; however, NSF restart will continue on other interfaces. This functionality applies to the default NSF mode of operation when NSF is configured.

If the user configures the optional **enforce global** keywords, NSF restart will be canceled for the entire process when non-NSF-aware neighbors are detected on any network interface during restart. To revert to the default NSF mode, configure the **nsf** command without any keywords.

Examples

The following example enters router configuration OSPF mode and cancels the NSF restart for the entire OSPF process if non-NSF-aware neighbors are detected on any network interface during restart:

```
router(config)# router ospf 1
router(config-router)# nsf enforce global
```

Related Commands

Command	Description
debug ip ospf nsf	Displays debugging messages related to OSPF NSF commands.
router ospf	Enables OSPF routing, which places the router in router configuration mode.

nsf interface wait

To specify how long a Cisco Nonstop Forwarding (NSF) restart will wait for all interfaces with Intermediate System-to-Intermediate System (IS-IS) adjacencies to come up before completing the restart, use the **nsf interface wait** command in router configuration IS-IS mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

nsf interface wait *seconds*

no nsf interface wait *seconds*

Syntax Description

seconds	The valid range is from 1 to 60 seconds.

Defaults

The default value is 10 seconds.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The **nsf interface wait** command can be used if Cisco proprietary IS-IS NSF is configured or if Internet Engineering Task Force (IETF) IS-IS NSF is enabled using the **nsf t3 manual** command. You can use this command if an interface is slow to come up.

Examples

The following example specifies that NSF restart will wait 15 seconds for all interfaces with IS-IS adjacencies to come up before completing the restart:

```
router(config)# router isis
router(config-router)# nsf cisco
router(config-router)# nsf interface wait 15
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interval	Specifies the minimum time between NSF restart attempts.
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
show clns neighbors	Displays both ES and IS neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf interval

To configure the minimum time between Cisco Nonstop Forwarding (NSF) restart attempts, use the **nsf interval** command in router configuration Intermediate System-to-Intermediate System (IS-IS) mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

nsf interval *minutes*

no nsf interval *minutes*

Syntax Description

minutes	The length of time in minutes between restart attempts. The valid range is from 0 to 1440 minutes.

Defaults

The default value is 5 minutes.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The **nsf interval** command can be used with both Cisco proprietary IS-IS NSF and Internet Engineering Task Force (IETF) IS-IS NSF. When you use Cisco proprietary IS-IS NSF, the active route processor (RP) must be up for at least 5 minutes before IS-IS will attempt to perform an NSF restart as part of a stateful switchover.

When you use the **nsf** command with the **ietf** keyword, the standby RP must be up for at least 5 minutes before IS-IS will attempt to perform an NSF restart as part of a stateful switchover.

Examples

The following example configures the minimum time between NSF restart attempts to be 2 minutes:

```
router(config-router)# router isis
router(config-router)# nsf cisco
router(config-router)# nsf interval 2
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.

Command	Description
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
show clns neighbors	Displays both IS and ES neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

nsf t3

To specify the methodology used to determine how long Internet Engineering Task Force (IETF) Cisco Nonstop Forwarding (NSF) will wait for the link-state packet (LSP) database to synchronize before generating overloaded link-state information for itself and flooding that information out to its neighbors, use the **nsf t3** command in router configuration IS-IS mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

nsf t3 {**manual** *seconds* | **adjacency**}

no nsf t3 {**manual** *seconds* | **adjacency**}

Syntax Description

manual	The amount of time that IETF NSF waits for the LSP database to synchronize is set manually by the user.
seconds	The range is from 5 to 3600 seconds.
adjacency	The time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover.

Defaults

The default value is 30 seconds.

Command Modes

Router configuration IS-IS

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

When the **nsf t3 adjacency** command is enabled, the time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover. When the **nsf t3 manual** command is enabled, the specified time in seconds is used.

The **nsf t3 manual** command can be used only if IETF IS-IS NSF is configured.

Examples

In the following example, the amount of time that IETF NSF waits for the LSP database to synchronize is set to 40 seconds:

```
nsf t3 manual 40
```

In the following example, the amount of time that IETF NSF waits for the LSP database to synchronize is determined by the adjacency holdtime advertised to the neighbors of the specified RP before switchover:

```
nsf t3 adjacency
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf interval	Specifies the minimum time between NSF restart attempts.
show clns neighbors	Displays both IS and ES neighbors.
show isis nsf	Displays current state information regarding IS-IS NSF.

show cef nsf

To show the current Cisco Nonstop Forwarding (NSF) state of Cisco Express Forwarding (CEF) on both the active and standby route processors (RPs), use the **show cef nsf** command in privileged EXEC mode.

show cef nsf

Syntax Description

The command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

If you enter the **show cef nsf** command before a switchover occurs, no switchover activity is reported. After a switchover occurs, you can enter the **show cef nsf** command to display details about the switchover as reported by the newly active RP. On the Cisco 12000 and 7500 series Internet routers, details about line card switchover are also provided.

Examples

The following example shows the current NSF state:

```
router# show cef nsf

Last switchover occurred:        00:01:30.088 ago
 Routing convergence duration:   00:00:34.728
 FIB stale entry purge durations:00:00:01.728 - Default
                                  00:00:00.088 - Red

          Switchover
 Slot    Count   Type   Quiesce Period
 1           2    sso   00:00:00.108
 2           1   rpr+   00:00:00.948
 3           2    sso   00:00:00.152
 5           2    sso   00:00:00.092
 6           1   rpr+   00:00:00.632

 No NSF stats available for the following linecards:4 7
```

Table 2 describes the significant fields in the display.

Table 2 show cef nsf Field Descriptions

Field	Description
Last switchover occurred	Time since the last system switchover.
Routing convergence duration	Time taken after the switchover before the routing protocol signalled CEF that they had converged.

Table 2 show cef nsf Field Descriptions (continued)

Field	Description
Stale entry purge	Time taken by CEF to purge any stale entries in each FIB table. In the example, these are the FIB tables names “Default” and “Red.”
Switchover	Per-linecard NSF statistics.
Slot	Line card slot number.
Count	Number of times line card has switched over. This will always be 1, unless the type is SSO.
Type	Type of switchover the linecard performed last. This can be SSO, RPR+ or RPR.
Quiesce Period	Period of time when the line card was disconnected from the switching fabric. During this time, no packet forwarding can take place. Other system restart requirements may add additional delay until the linecard can start forwarding packets.

Related Commands

Command	Description
clear ip cef epoch	Begins a new epoch and increments the epoch number for a CEF table.
show cef state	Displays the state of CEF on a networking device.

show cef state

To display the state of Cisco Express Forwarding (CEF) on a networking device, use the **show cef state** command in privileged EXEC mode.

show cef state

Syntax Description

The command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500, 10000, and 12000 series Internet routers.

Examples

The following example shows the state of CEF on the active route processor (RP):

```
router# show cef state

RRP state:
     I am standby RRP:          no
     RF Peer Presence:          yes
     RF PeerComm reached:       yes
     Redundancy mode:           SSO(7)
     CEF NSF:                   enabled/running
```

The following example shows the state of CEF on the standby RP:

```
router# show cef state

RRP state:
     I am standby RRP:          yes
     My logical slot:           0
     RF Peer Presence:          yes
     RF PeerComm reached:       yes
     CEF NSF:                   running
```

Related Commands

Command	Description
clear ip cef epoch	Begins a new epoch and increments the epoch number for a CEF table.
show cef nsf	Displays the current NSF state of CEF on both the active and standby RPs.

show clns neighbors

To display both end systems (ES) and intermediate systems (IS) neighbors, use the **show clns neighbors** command in EXEC mode.

show clns *area-tag* **neighbors** [*interface-type interface-number*] [**detail**]

Syntax Description

area-tag	Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area. Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
detail	(Optional) When specified, the area addresses advertised by the neighbor in the hello messages is displayed. Otherwise, a summary display is provided.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **area** and **detail** keywords were added.
12.0(22)S	The “NSF capable” line was added to the output.

Examples

The following is sample output from the **show clns neighbors** command. This display is a composite of the **show clns es-neighbor** and **show clns is-neighbor** commands.

```
Router# show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
000A.0000.0000 Se3/0/2     *HDLC*          Stby   30        L1L2 IS-IS
000C.0000.0000 Gi2/0/0     000c.0000.0000  Stby   30        L1L2 IS-IS
```

Table 3 describes the significant fields shown in the display.

Table 3 show clns neighbors Field Descriptions

Field	Description
System ID	Six-byte value that identifies a system in an area.
Interface	Interface from which the system was learned.
SNPA	Subnetwork Point of Attachment. This is the data-link address.
State	State of the ES or IS.

Table 3 show clns neighbors Field Descriptions (continued)

Field	Description
Init	System is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent.
Up	Believes the ES or IS is reachable.
Holdtime	Number of seconds before this adjacency entry times out.
Type	The adjacency type. Possible values are as follows:
ES	End-system adjacency either discovered via the ES-IS protocol or statically configured.
IS	Router adjacency either discovered via the ES-IS protocol or statically configured.
L1	Router adjacency for Level 1 routing only.
L1L2	Router adjacency for Level 1 and Level 2 routing.
L2	Router adjacency for Level 2 only.
Protocol	Protocol through which the adjacency was learned. Valid protocol sources are ES-IS, IS-IS, ISO IGRP, Static, and DECnet.

The following is sample output from the **show clns neighbors detail** command:

```
Router# show clns neighbors detail

System Id       SNPA        Interface    State  Holdtime  Type Protocol
Router2          Se0          *HDLC*       Up      25    L1L2    IS-IS
Area Address(es):49
IP Address(es): 10.16.255.255*
Uptime:6d23h
NSF capable
```

Notice that the information displayed in the **show clns neighbors detail** output includes everything shown in the **show clns neighbors** output in addition to the area address associated with the IS neighbor and its uptime. When IP routing is enabled, Integrated-ISIS adds information to the output of the **show clns** commands. The **show clns neighbors detail** command output shows the IP addresses that are defined for the directly connected interface and an asterisk (*) to indicate which IP address is the next hop.

Related Commands

Command	Description
clear clns neighbors	Removes CLNS neighbor information from the adjacency database.

show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC mode.

show ip bgp [*network*] [*network-mask*] [**longer-prefixes**]

Syntax Description

network	(Optional) Network number, entered to display a particular network in the BGP outing table.
network-mask	(Optional) Displays all BGP routes matching the address and mask pair.
longer-prefixes	(Optional) Displays the route and more specific routes.

Command Modes

User EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The display of prefix advertisement statistics was added.
12.0(6)T	The display of a message indicating support for route refresh capability was added.
12.0(22)S	A new status code indicating stale routes was added.

Examples

The following example is from the **show ip bgp** command:

```
router# show ip bgp

BGP table version is 9, local router ID is a.a.a.a
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal,
             S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
S> 10.100.100.0/24 192.168.2.2             0             0 65002 i
S> 10.10.0.0        192.168.2.2                          0 65002 65003 i
S> 10.20.0.0        192.168.2.2                          0 65002 65003 i
S> 10.30.0.0/8      192.168.2.2                          0 65002 65003 i
S> 10.40.33.0/24   192.168.2.2                           0 65002 65003 i
*>                  0.0.0.0                 0          32768 i
S> 10.50.0.0/8      192.168.2.2                          0 65002 65003 i
S> 10.60.100.0    192.168.2.2               0             0 65002 i
S> 10.70.200.0    192.168.2.2               0             0 65002 i
```

Table 4 describes the significant fields shown in the displays.

Table 4 show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number increments when the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is damped. h—History of the table entry. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session. S—The table entry is stale.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The value of the inter-autonomous system metric.
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is damped. h—History of the table entry. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session. S—The table entry is stale.

The following example of the **show ip bgp** command specifies a network:

```
router# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 7
Paths:(1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65002 65003, (stale)
```

```
    192.168.2.2 from 192.168.2.2 (0.0.0.0)
      Origin IGP, localpref 100, valid, external, best
router#
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

show ip bgp neighbors

To display information about TCP/IP and Border Gateway Protocol (BGP) connections to neighbors, use the **show ip bgp neighbors** command in EXEC mode.

show ip bgp neighbors [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | {**paths** *regexp*} | **dampened-routes**] [**received prefix-filter**]

Syntax Description

neighbor-address	(Optional) Address of the neighbor whose routes you have learned from. If you omit this argument, all neighbors are displayed.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. This is a subset of the output from the **received-routes** keyword.
advertised-routes	(Optional) Displays all the routes the router has advertised to the neighbor.
paths *regexp*	(Optional) Regular expression that is used to match the paths received.
dampened-routes	(Optional) Displays the dampened routes to the neighbor at the IP address specified.
received prefix-filter	(Optional) Displays the configured prefix list for the specified IP address.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **received-routes** keyword was added.
12.0(21)ST	This command was updated to display MPLS label information.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was added. The **received prefix-filter** keyword was added.

Examples

The following is sample output from the **show ip bgp neighbors** command in privileged EXEC mode.

```
Router# show ip bgp neighbors 172.16.254.3

BGP neighbor is 172.16.254.3,  remote AS 150, internal link
  BGP version 4, remote router ID 172.16.254.3
  BGP state = Established, up for 19:24:07
  Last read 00:00:06, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
    Address family IPv4 Unicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast
  Received 4231 messages, 0 notifications, 0 in queue
```

```
  Sent 4167 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 5 seconds

 For address family:IPv4 Unicast
  BGP table version 159559, neighbor version 159559
  Index 90, Offset 11, Mask 0x4
  Route refresh request:received 0, sent 0
  10031 accepted prefixes consume 441364 bytes
  Prefix advertised 29403, suppressed 0, withdrawn 9801
  Number of NLRIs in the update sent:max 242, min 0

  Connections established 2; dropped 1
  Last reset 19:26:54, due to NSF peer closed the session
Connection state is ESTAB, I/O status:1, unread input bytes:0
Local host:150.254.254.2, Local port:11005
Foreign host:172.16.254.3, Foreign port:179

Enqueued packets for retransmit:0, input:0  mis-ordered:0 (0 bytes)

Event Timers (current time is 0x4371A84):
Timer          Starts    Wakeups            Next
Retrans          1380         22             0x0
TimeWait            0          0             0x0
AckHold          1377        870             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:1875330775  snduna:1875639119  sndnxt:1875639119     sndwnd: 16308
irs:3577079138  rcvnxt:3577393901  rcvwnd:     16137  delrcvwnd:   247

SRTT:300 ms, RTTO:607 ms, RTV:3 ms, KRTT:0 ms
minRTT:0 ms, maxRTT:408 ms, ACK hold:200 ms
Flags:higher precedence, nagle

Datagrams (max data segment is 536 bytes):
Rcvd:2984 (out of order:1), with data:1800, total data bytes:314762
Sent:3190 (retransmit:22, fastretransmit:0), with data:1751, total data bytes:308343
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
remote AS	Autonomous system of the neighbor.
external link	Indicates that this peer is an EBGP peer.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	IP address of the neighbor.
BGP state	Internal state of this BGP connection.
up for	Amount of time, in seconds, that the underlying TCP connection has been in existence.

Table 5 show ip bgp neighbors Field Descriptions (continued)

Field	Description
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period, in seconds, between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
MPLS Label capability	Indicates that MPLS labels are both sent and received by the EBGP peer.
Address family IPv4 Unicast:	IP Version 4 unicast-specific properties of this neighbor.
Address family IPv4 Multicast:	IP Version 4 multicast-specific properties of this neighbor.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer.
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.
Route refresh request:	Number of route refresh requests sent and received from this neighbor.
advertisement runs	Value of minimum advertisement interval.
For address family:	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Community attribute	Appears if the **neighbor send-community** command is configured for this neighbor.
Inbound path policy	Indicates if an inbound policy is configured.
Outbound path policy	Indicates if an outbound policy is configured.
uni-in	Name of inbound route map for the unicast address family.
uni-out	Name of outbound route map for the unicast address family.
mul-in	Name of inbound route map for the multicast address family.
mul-out	Name of outbound route map for the multicast address family.
Sending Prefix & Label	Indicates that the EBGP peer sends MPLS labels with its routes.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.

Table 5 show ip bgp neighbors Field Descriptions (continued)

Field	Description
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time since this peering session was last reset.
Connection state	State of BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of local router, plus port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table displays the number of starts and wakeups for each timer.
iss	Initial send sequence number.
snduna	Last send sequence number the local host sent but has not received an acknowledgment for.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrcvwnd	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout.
RTTO	Round-trip timeout.
RTV	Variance of the round-trip time.
KRTT	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (hard wire value used for calculation).
maxRTT	Largest recorded round-trip timeout.
ACK hold	Time the local host will delay an acknowledgment in order to piggyback data on it.
Flags	IP precedence of the BGP packets.
Datagrams: Rcvd	Number of update packets received from a neighbor.
with data	Number of update packets received with data.
total data bytes	Total bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show ip bgp neighbors** command with the **advertised-routes** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*>i110.0.0.0        172.16.232.179         0    100      0 ?
*> 200.2.2.0        0.0.0.0                0         32768 i
```

The following is sample output from the **show ip bgp neighbors** command with the **routes** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbors 172.16.232.178 routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.0.0         172.16.232.178        40             0 10 ?
*> gg.0.0.0         172.16.232.178        40             0 10 ?
```

Table 6 describes the significant fields shown in the displays.

Table 6 show ip bgp neighbors advertised-routes and routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number increments when the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened and will not be advertised to BGP neighbors. h—The table entry does not contain the best path based on historical information. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.

Table 6 show ip bgp neighbors advertised-routes and routes Field Descriptions (continued)

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp neighbors** command with the **paths** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbors 171.69.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

The following is sample output from the **show ip bgp neighbors** command with the **received prefix-filter** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbor 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family:	Configured address family mode.
ip prefix-list	Configured prefix list for the specified neighbor.

show ip cef

To display entries in the Forwarding Information Base (FIB) or to display a summary for the FIB, use the **show ip cef** command in privileged EXEC mode.

show ip cef [**vrf** *vrf-name*] [**unresolved** | [**detail** | **summary**]

Specific FIB Entries Based on Stateful Switchover

show ip cef [**epoch**]

Specific FIB Entries Based on IP Address Information

show ip cef [**vrf** *vrf-name*] [**network** [**mask**]] [**longer-prefixes**] [**detail**]

Specific FIB Entries Based on Nonrecursive Routes

show ip cef [**vrf** *vrf-name*] **nonrecursive** [**detail**]

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
unresolved	(Optional) Displays unresolved FIB entries.
detail	(Optional) Displays detailed FIB entry information.
summary	(Optional) Displays a summary of the FIB.
epoch	TBD
nsf	TBD
network	(Optional) Displays the FIB entry for the specified destination network.
mask	(Optional) Displays the FIB entry for the specified destination network and mask.
longer-prefixes	(Optional) Displays FIB entries for more specific destinations.
nonrecursive	(Optional) Displays only nonrecursive routes.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12012 Internet router.
11.1 CC	Multiple platform support was added.
12.0(5)T	The **vrf** keyword was added.
12.0(22)S	The **epoch** and **nsf** keywords were added.

Usage Guidelines

The **show ip cef** command without any keywords or arguments shows a brief display of all FIB entries.

The **show ip cef detail** command shows detailed FIB entry information for all FIB entries.

The **show ip cef summary** command shows a summary of FIB entry information for all FIB entries.

Examples

The following is sample output from the **show ip cef unresolved** command:

```
Router# show ip cef unresolved

IP Distributed CEF with switching (Table Version 136632)
45776 routes, 13 unresolved routes (0 old, 13 new)
45776 leaves, 2868 nodes, 8441480 bytes, 136632 inserts, 90856 invalidations
1 load sharing elements, 208 bytes, 1 references
1 CEF resets, 1 revisions of existing leaves
refcounts: 527292 leaf, 465617 node

10.214.0.0/16, version 136622
0 packets, 0 bytes
  via 171.69.233.56, 0 dependencies, recursive
  unresolved
10.215.0.0/16, version 136623
0 packets, 0 bytes
  via 171.69.233.56, 0 dependencies, recursive
  unresolved
10.218.0.0/16, version 136624
0 packets, 0 bytes
```

The following is sample output from the **show ip cef summary** command on the active route processor (RP), after a switchover has occurred:

```
Router# show ip cef summary

Non-stop forwarding:
      13 routes at switchover
      11 routes available after convergence (2 purged)
```

The following is sample output from a system that is not running Cisco Express Forwarding (CEF) Nonstop Forwarding (NSF), after a switchover has occurred:

```
router# show ip cef summary

Non-stop forwarding:
      CEF NSF was not running at switchover
      5 routes available after convergence (0 purged)
```

The following is sample output from the **show ip cef detail** command for Ethernet interface 0. It shows all the prefixes resolving through adjacency pointing to next hop Ethernet interface 0/0 and next hop interface IP address 172.19.233.33.

```
Router# show ip cef detail

IP Distributed CEF with switching (Table Version 136808)
45800 routes, 8 unresolved routes (0 old, 8 new) 45800 leaves, 2868 nodes, 8444360 bytes,
136808 inserts, 91008 invalidations 1 load sharing elements, 208 bytes, 1 references 1
CEF resets, 1 revisions of existing leaves refcounts: 527343 leaf, 465638 node

172.19.233.33/32, version 7417, cached adjacency 172.19.233.33 0 packets, 0 bytes,
Adjacency-prefix
via 172.19.233.33, Ethernet0/0, 0 dependencies
next hop 172.19.233.33, Ethernet0/0
valid cached adjacency
```

The following example shows output from the **show ip cef epoch** command:

```
Router#show ip cef epoch

CEF epoch information:

Table: Default
  Table epoch: 0 (35 entries at this epoch)

Adjacency table
  Table epoch: 0 (7 entries at this epoch)
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip cef epoch Field Descriptions

Field	Description
Table: Default	Specifies the active epoch numbers for the forwarding information base (FIB) table called Default.
Table epoch	Specifies the active epoch numbers and the number of entries with each epoch number.
Adjacency table	Specifies the active epoch number in the adjacency table.

The following example shows the forwarding table associated with the VRF named vrf1:

```
Router# show ip cef vrf vrf1

Prefix              Next Hop            Interface
10.0.0.0/32          receive
10.10.0.0/8          10.60.0.1           Ethernet1/3
10.20.0.0/8          10.62.0.2           POS6/0
10.50.0.0/8          attached            Ethernet1/3
10.50.0.0/32         receive
10.60.0.1/32         10.62.0.1           Ethernet1/3
10.60.0.2/32         receive
10.255.255.255/32    receive
10.62.0.0/8          52.0.0.2            POS6/0
192.168.0.0/24       receive
192.168.255.255/32   receive
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip cef vrf Field Descriptions

Field	Description
Prefix	Specifies the network prefix.
Next Hop	Specifies the Border Gateway Protocol (BGP) next hop address.
Interface	Specifies the VRF interface.

Related Commands

Command	Description
clear ip cef epoch	Begins a new epoch and increments the epoch number for a CEF table.
show cef state	Displays the state of CEF on a networking device.

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in user EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.

Command Modes

User EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	Fields of information were added to the command output.

Examples

The following example output is from the **show ip ospf** command when entered without a specific OSPF process ID:

```
router> show ip ospf

Routing Process "ospf 1" with ID 10.2.2.2 and Domain ID 10.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
cisco Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
 Area has no authentication
 SPF algorithm executed 3 times
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip ospf Field Descriptions

Field	Description
Routing Process “ospf 1" with ID 10.2.2.2	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).

Table 11 show ip ospf Field Descriptions (continued)

Field	Description
Redistributing External Routes from	Lists of redistributed routes, by protocol (displayed if the networking device is an autonomous system boundary router).
Number of areas	Number of areas in router, area addresses, and so on.
Cisco Non-Stop Forwarding enabled	The OSPF process is configured to perform Cisco Nonstop Forwarding (NSF) on a switchover.
last NSF restart	Indicates how long ago (in hours:minutes:seconds) a successful NSF restart took place and how long (in seconds) it took to perform the procedure.

Related Commands

Command	Description
debug ip ospf nsf	Displays debugging messages related to OSPF NSF commands.
show ip ospf neighbor	Displays OSPF-neighbor information on a per-interface basis.

show ip ospf neighbor

To display Open Shortest Path First (OSPF)-neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in user EXEC mode.

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).

Command Modes

User EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	Fields of information were added to the command output.

Examples

The following is sample output from the **show ip ospf neighbor detail** command:

```
router> show ip ospf neighbor detail

Neighbor 10.3.3.3, interface address 172.16.10.3
In the area 0 via interface POS3/0
Neighbor priority is 0, State is FULL, 6 state changes
DR is 10.0.0.0 BDR is 10.0.0.0
Options is 0x52
LLS Options is 0x1 (LR), last OOB-Resync 00:02:22 ago
Dead timer due in 00:00:37
Neighbor is up for 00:03:07
Index 1/1, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 1, maximum is 1
Last retransmission scan time is 0 msec, maximum is 0 msec
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip ospf neighbor Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor and neighbor state.
State	OSPF state.

Table 12 show ip ospf neighbor Field Descriptions (continued)

Field	Description
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2: 2 indicates area is not a stub; 0 indicates area is a stub.)
LLS Options is 0x1 (LR)	Indicates whether the neighbor is NSF-aware.
last OOB-resync...ago	Indicates how long ago (in hours:minutes:seconds) the last successful link-state database (LSDB) resynchronization was performed with this neighbor.
Dead timer	Expected time (in hours:minutes:seconds) before Cisco IOS software will declare the neighbor dead.

Related Commands

Command	Description
debug ip ospf nsf	Displays debugging messages related to OSPF NSF commands.
show ip ospf	Displays general information about OSPF routing processes.

show isis nsf

To display current state information regarding Intermediate System-to-Intermediate System (IS-IS) Cisco Nonstop Forwarding (NSF), use the **show isis nsf** command in EXEC mode.

show isis nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.

Usage Guidelines

The **show isis nsf** command can be used with both Cisco proprietary IS-IS NSF and Internet Engineering Task Force (IETF) IS-IS NSF. The information displayed when this command is entered depends on which protocol has been configured. To configure nsf for a specific routing protocol, use the **router bgp**, **router ospf**, or **router isis** commands in global configuration mode.

Examples

The following example shows state information for an active RP that is configured to use Cisco proprietary IS-IS NSF:

```
router# show isis nsf

NSF enabled, mode 'cisco'
RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

The following example shows state information for a standby RP that is configured to use Cisco proprietary IS-IS NSF:

```
router# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 314
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

The following example shows state information when the networking device is configured to use IETF IS-IS NSF:

```
router# show isis nsf

NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
```

```
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
```

Related Commands

Command	Description
debug isis nsf	Displays information about the IS-IS state during an NSF restart.
nsf (IS-IS)	Configures NSF operations for IS-IS.
nsf t3	Specifies the methodology used to determine how long IETF NSF will wait for the LSP database to synchronize before generating overloaded link state information for itself and flooding that information out to its neighbors.
nsf interface wait	Specifies how long a NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.
nsf interval	Specifies the minimum time between NSF restart attempts.
show clns neighbors	Displays both ES and IS neighbors.