Cisco Nonstop Forwarding

First Published: July 22, 2002
Last Updated: December 4, 2006

Cisco Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) feature in Cisco IOS software. 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.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Cisco Nonstop Forwarding" section on page 26.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Note Throughout this document, the term "Route Processor" 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 called the Performance Routing Engine (PRE), on the Cisco 12000 series Internet router the RP is called the Gigabit Route Processor (GRP), and on the Cisco 7500 series router the RP is called the Route Switch Processor (RSP).

Contents

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

Prerequisites for Cisco Nonstop Forwarding

- 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.

Restrictions for Cisco Nonstop Forwarding

General Restrictions

- The Hot Standby Routing Protocol (HSRP) is not supported with Cisco Nonstop Forwarding with Stateful Switchover. Do not use HSRP with Cisco Nonstop Forwarding with Stateful Switchover.

BGP NSF

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

EIGRP NSF

- All neighboring devices participating in EIGRP NSF operation must be NSF-capable or NSF-aware.
- An NSF-aware router cannot support two NSF-capable peers performing an NSF restart operation at the same time. However, both neighbors will reestablish peering sessions after the NSF restart operation is complete.

OSPF NSF

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

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(23)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.

Information About Cisco Nonstop Forwarding

Cisco NSF works with the Stateful Switchover (SSO) feature in Cisco IOS software. 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.

NSF Dependency on SSO

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 "How to Implement Cisco NSF" section.

Cisco NSF Routing and Forwarding Operation

Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. Of the routing protocols, BGP, EIGRP, 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	**12.0(23)S**	**12.0(24)S**	**12.2(18)S**	**12.2(28)SB**	**12.2(33)SRA**
BGP	Cisco 7200	Yes[1]	Yes[1]	Yes[1]	No[2]	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	Yes	No
	Cisco 12000	Yes	Yes	Yes	No	No	No
OSPF	Cisco 7200	Yes[1]	Yes[1]	Yes[1]	No[2]	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	No	No
	Cisco 12000	Yes	Yes	Yes	No	No	No
IS-IS	Cisco 7200	Yes[1]	Yes[1]	Yes[1]	No[2]	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	Yes	No
	Cisco 12000	Yes	Yes	Yes	No	No	No

Table 1 Routing Protocol and CEF Support in Cisco NSF

Protocol	Platform	NSF Support in Cisco IOS Software Release					
		12.0(22)S	12.0(23)S	12.0(24)S	12.2(18)S	12.2(28)SB	12.2(33)SRA
CEF	Cisco 7200[3]	—	—	—	—	—	—
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	Yes	Yes	Yes	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	Yes	Yes	Yes	No	No	No
	Cisco 12000	Yes	Yes	Yes	No	No	No
EIGRP	Cisco 7200	No	No	No	Yes[2]	No	No
	Cisco 7304	No	No	No	No	Yes	No
	Cisco 7500	No	No	No	Yes	No	No
	Cisco 7600	No	No	No	No	No	Yes
	Cisco 10000	No	No	No	No	No	No
	Cisco 12000	No	No	No	No	No	No

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, EIGRP, 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 NSF-aware in the Cisco IOS Release 12.2(18)S.
3. 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.

EIGRP Operation

EIGRP NSF capabilities are exchanged by EIGRP peers in hello packets. The NSF-capable router notifies its neighbors that an NSF restart operation has started by setting the restart (RS) bit in a hello packet. When an NSF-aware router receives notification from an NSF-capable neighbor that an NSF-restart operation is in progress, the NSF-capable and NSF-aware routers immediately exchange their topology tables. The NSF-aware router sends an end-of-table (EOT) update packet when the transmission of its topology table is complete. The NSF-aware router then performs the following actions to assist the NSF-capable router:

- The EIGRP hello hold timer is expired to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware router to reply to the NSF-capable router more quickly reducing the amount of time required for the NSF-capable router to rediscover neighbors and rebuild the topology table.
- The route-hold timer. is started. This timer is used to set the period of time that the NSF-aware router will hold known routes for the NSF-capable neighbor. This timer is configured with the **timers nsf route-hold** command. The default time period is 240 seconds.
- The NSF-aware router notes in the peer list that the NSF-capable neighbor is restarting, maintains adjacency, and holds known routes for the NSF-capable neighbor until the neighbor signals that it is ready for the NSF-aware router to send its topology table or the route-hold timer expires. If the route-hold timer expires on the NSF-aware router, the NSF-aware router will discard held routes and treat the NSF-capable router as a new router joining the network and reestablishing adjacency accordingly.
- The NSF-aware router will continue to send queries to the NSF-capable router which is still in the process of converging after switchover, effectively extending the time before a stuck-in-active (SIA) condition can occur.

When the switchover operation is complete, the NSF-capable router notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting routers. The NSF-capable then returns to normal operation. The NSF-aware router will look for alternate paths (go active) for any routes that are not refreshed by the NSF-capable (restarting router). The NSF-aware router will then return to normal operation. If all paths are refreshed by the NSF-capable router, the NSF-aware router will immediately return to normal operation.

Note NSF-aware routers are completely compatible with non-NSF aware or capable neighbors in an EIGRP network. A non-NSF aware neighbor will ignore NSF capabilities and reset adjacencies and otherwise maintain the peering sessions normally.

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.

The OSPF RFC 3623 graceful restart feature allows you to configure IETF NSF in multivendor networks. For more information, see *OSPF RFC 3623 Graceful Restart*, Cisco IOS Release 12.2(31)SB2.

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.

Cisco NSF Benefits

The Cisco NSF feature has several benefits, including the following:

- 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 link flapping—Because the interfaces remain up across a switchover, neighboring routers do not detect a link flap (that is, 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.

How to Implement Cisco NSF

- Configuring and Verifying CEF NSF, page 10
- Configuring and Verifying BGP NSF, page 10
- Configuring and Verifying EIGRP NSF, page 12

- Configuring and Verifying OSPF NSF, page 14
- Configuring and Verifying IS-IS NSF, page 15

Configuring and Verifying CEF NSF

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

The following task explains how to verify that CEF is NSF-capable.

SUMMARY STEPS

1. **enable**
2. **show cef state**

DETAILED STEPS

	Command	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`show cef state`** **Example:** `Router# configure terminal`	Displays the state of Cisco Express Forwarding on a networking device.

Configuring and Verifying BGP NSF

The following task explains how to configure BGP for NSF. Repeat this task on each of the BGP NSF peer devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*]

DETAILED STEPS

	Command	Purpose
Step 1	**`enable`** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**`configure terminal`** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**`router bgp`** *`autonomous-system-number`* **Example:** `Router(config)# router bgp 120`	Enables a BGP routing process, and enters router configuration mode.
Step 4	**`bgp graceful-restart`** [**`restart-time`** *`seconds`* | **`stalepath-time`** *`seconds`*] **Example:** `Router(config-router)#` **`bgp graceful-restart`**	Enables the BGP graceful restart capability, which starts NSF for BGP.

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. The following task explains how to perform this function.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy** [**detail**]]]

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the contents of the current running configuration file. Verify that the phrase "bgp graceful-restart" appears in the BGP configuration of the SSO-enabled router. Repeat this step on each of the BGP neighbors.
Step 3	**show ip bgp neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **received prefix-filter** | **received-routes** | **routes** | **policy** [**detail**]]] **Example:** `Router# show ip bgp neighbors`	display information about BGP and TCP connections to neighbors On the SSO device and the neighbor device, this command verifies that the graceful restart function is shown as both advertised and received, and confirms the address families that have the graceful restart capability. If no address families are listed, then BGP NSF also will not occur.

Configuring and Verifying EIGRP NSF

EIGRP NSF support is enabled by default. Distributed platforms that run a supporting version of Cisco IOS software can support full NSF capabilities. These routers can perform a restart operation and can support other NSF capable peers. Single processor platforms that run a supporting version of Cisco IOS software support only NSF awareness. These routers maintain adjacency and hold known routes for the NSF-capable neighbor until it signals that it is ready for the NSF-aware router to send its topology table or the route-hold timer expires.

Note An NSF-aware router must be completely converged with the network before it can assist an NSF-capable router in an NSF restart operation.

The following task explains how to configure EIGRP for NSF. Repeat this procedure on each of the EIGRP NSF peer devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*]
5. **timers nsf converge** *seconds*
6. **timers nsf route-hold** *seconds*
7. **timers nsf signal** *seconds*

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 109`	Enables an EIGRP routing process, and enters router configuration mode.
Step 4	**nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*] **Example:** `Router(config-router)# nsf`	Enables EIGRP NSF support on an NSF capable router. This command is entered on only NSF-capable routers. NSF awareness is enabled by default when a supporting version of Cisco IOS software is installed on a router that supports NSF capability or NSF awareness.
Step 5	**timers nsf converge** *seconds* **Example:** `Router(config-router)# timers nsf converge 60`	Adjusts the maximum time that restarting router will wait for the EOT notification from an NSF-capable or NSF-aware peer.
Step 6	**timers nsf route-hold** *seconds* **Example:** `Router(config-router)# timers nsf route-hold 120`	Sets the route-hold timer to determine how long an NSF-aware router that is running EIGRP will hold routes for an inactive peer.
Step 7	**timers nsf signal** *seconds* **Example:** Router(config-router)# **timers nsf signal** *seconds*	Adjusts the maximum time for the initial restart period.

To verify NSF for EIGRP, you must check that NSF awareness and/or capability is enabled on the SSO-enabled networking device and on the neighbor devices. The following task explains how to perform this function.

SUMMARY STEPS

1. **enable**
2. **show ip protocols**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip protocols** **Example:** `Router# show ip protocols`	Displays the parameters and current state of the active routing protocol process. Repeat this step on each of the EIGRP neighbors.

Configuring and Verifying 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.

The following task explains how to configure OSPF for NSF.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*]

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 12`	Enables an OSPF routing process, and places the router in router configuration mode.
Step 4	**nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*] **Example:** `Router(config-router)# nsf`	Enables EIGRP NSF support on an NSF capable router. This command is entered on only NSF-capable routers. NSF awareness is enabled by default when a supporting version of Cisco IOS software is installed on a router that supports NSF capability or NSF awareness.

The following task explains how to verify OSPF for NSF.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show ip ospf** [*process-id*]

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the contents of the current running configuration file.
Step 3	**show ip ospf** [*process-id*] **Example:** `Router# show ip ospf`	Displays general information about OSPF routing processes.

Configuring and Verifying IS-IS NSF

The following task describe how to configure NSF for IS-IS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router isis** *area-tag*
4. **nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*]
5. **nsf interval** *minutes*
6. **nsf t3** {**manual** *seconds* | **adjacency**}
7. **nsf interface wait** *seconds*

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis cisco1`	Enables the IS-IS routing protocol to specify an IS-IS process, and places the router in router configuration mode.
Step 4	**nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*] **Example:** `Router(config-router)# nsf 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 5	**nsf interval** *minutes* **Example:** `Router(config-router)# nsf interval 2`	Configures the minimum time between Cisco NSF restart attempts.
Step 6	**nsf t3** {**manual** *seconds* | **adjacency**} **Example:** `Router(config-router)# nsf t3 manual 40`	Specifies the methodology used to determine how long IETF Cisco 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.
Step 7	**nsf interface wait** *seconds* **Example:** `Router(config-router)# nsf interface wait 15`	Specifies how long a Cisco NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.

To verify NSF for IS-IS, you must check that the NSF function is configured on the SSO-enabled networking device. The following task describes how to verify NSF for IS-IS.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show isis nsf**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the contents of the current running configuration file.
Step 3	**show isis nsf** **Example:** `Router# show isis nsf`	Displays current state information regarding IS-IS NSF.

Troubleshooting Tips

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

Command	Purpose
Router# **debug eigrp nsf**	Displays notifications and information about NSF events for an EIGRP routing process.
Router# **debug ip eigrp notifications**	Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.
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.

Command	Purpose
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 ip protocols**	Displays the parameters and current state of the active routing protocol process. The status of EIGRP NSF configuration and support is displayed in the output.
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 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.

EIGRP adjacencies reset too often.

Neighbor adajacencies are maintained during NSF switchover operations. If adjacencies between NSF-capable and NSF-aware neighbors are being reset too often, the route-hold timers may need to be adjusted. The **show ip eigrp neighbor detail** command can be used to help determine if the route-hold timer value should be set to a longer time period. The output will display the time that adjacency is established with specific neighbors. This time will tell you if adjacencies are being maintained or reset and when the last time that specific neighbors have been restarted.

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 IS-IS, the standby RP must be stable for 5 minutes (which is the 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:

Verifying that CEF Is NSF Capable: Example

The following example is used to verify that CEF is NSF capable.

```
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
```

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
```

Verifying BGP NSF: Example

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
```

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
```

Configuring EIGRP NSF Converge Timer: Example

The **timers nsf converge** command is used to adjust the maximum time that restarting router will wait for the EOT notification from an NSF-capable or NSF-aware peer. The following example sets the converge timer to 1 minute.

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# timers nsf converge 60
```

Configuring EIGRP NSF Route-Hold Timer: Example

The **timers nsf route-hold** command is used to set the maximum period of time that an NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation. The following example sets the route-hold timer to 2 minutes.

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# timers nsf route-hold 120
```

Configuring EIGRP NSF Signal Timer: Example

The **timers nsf signal** command is used to adjust the maximum time for the initial restart period. The following example sets the signal timer to 10 seconds.

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# timers nsf signal 10
```

Verifying EIGRP NSF: Example

Verify that EIGRP NSF support is present in the installed Cisco IOS software image by entering the **show ip protocols** command. "EIGRP NSF-aware route hold timer is..." is displayed in the output when either NSF awareness or capability is supported by the router. This line displays the default or user-defined value for the route-hold timer. "EIGRP NSF..." is displayed in the output only when the NSF capability is supported by the router. This line will also print "disabled" or "enabled" depending on the status of the EIGRP NSF feature.

```
Router# show ip protocols

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

Disabling EIGRP NSF Support: Example

EIGRP NSF capability is enabled by default on distributed platforms that run a supporting version of Cisco IOS software. The **nsf** command used to enable or disable the EIGRP NSF capability. The following example disables NSF capability:

```
Router# configure terminal
Router(config)# router eigrp 101
Router(config-router)# no nsf
```

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
```

Verifying OSPF NSF: Example

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

Next, 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
```

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
```

Verifying IS-IS NSF: Example

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 example indicates that the device uses the Cisco implementation of IS-IS NSF:

```
Router# show running-config

router isis
nsf cisco
```

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 example shows output for the Cisco configuration on the active RP. In this example, note the presence of the phrase "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 example shows sample output for the Cisco configuration on the standby RP. In this example, note the presence of the phrase "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
```

The following example 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
```

Additional References

The following sections provide references related to the Cisco Nonstop Forwarding feature.

Related Documents

Related Topic	Document Title
High availability commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS High Availability Command Reference*
Stateful switchover	*Stateful Switchover*, Cisco IOS feature module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3623	*Graceful OSPF Restart*
RFC 3847	*Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
RFC 4781	*Graceful Restart Mechanism for BGP*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Feature Information for Cisco Nonstop Forwarding

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.0(22)S or a later release appear in the table.

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

Table 2 Cisco Nonstop Forwarding Feature History

Release	Modification
12.0(22)S	This feature was introduced.
12.0(23)S	Support was added for 1xGE and 3xGE line cards on the
12.0(24)S	Support was added for the following line cards on the Engine 1 • 2-port OC-12/STM-4c DPT Engine 2 • 1-port OC-48/STM-16c DPT • 8-port OC-3/STM-1c ATM IP Service Engine (ISE) • 4-port OC-3c/STM-1c POS/SDH ISE • 8-port OC-3c/STM-1c POS/SDH ISE • 16-port OC-3c/STM-1c POS/SDH ISE • 4-port OC-12c/STM-4c POS/SDH ISE • 1-port OC-48c/STM-16c POS/SDH ISE • 4-port channelized OC-12/STM-4 (DS3/E3, OC-3c/STM-1c) POS/SDH ISE • 1-port channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c) POS/SDH ISE

12.2(18)S	This feature was integrated into Cisco IOS Release 12.2(18)S. Support was added for EIGRP.
12.2(20)S	Support for the Cisco 7304 router was added.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The following features were added: • OSPF RFC 3623 Graceful Restart