8

Nonstop Forwarding (NSF)

Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.4SY supports only Ethernet interfaces. Cisco IOS Release 15.4SY does not support any WAN features or commands.
- Stateful switchover (SSO) and nonstop forwarding (NSF) do not support IPv6 multicast traffic.

Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

Prerequisites for NSF

None.

Restrictions for NSF

General Restrictions

- NSF requires SSO (see Chapter 7, “Stateful Switchover (SSO)”).
- 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.

Restrictions for 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 for NSF” section on page 8-8.

Restrictions for 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.

Restrictions for 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.

Restrictions for IS-IS NSF

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

Restrictions for IPv6 NSF

- IPv6 must be enabled on your router for IPv6 NSF to be supported.

Information About NSF

NSF Overview

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 while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards 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.

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.

A networking device is NSF-aware if it is running NSF-compatible software. A device is NSF-capable if it has been configured to support NSF and would rebuild routing information from NSF-aware or NSF-capable neighbors.

CEF is always enabled on the switch and cannot be disabled. The routing protocols depend 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 and CEF updates the line cards with the new FIB information.

Feature Interaction with NSF

- Cisco Express Forwarding, page 8-4
- Routing Protocol Operation, page 8-4
- BGP Operation, page 8-4
- EIGRP Operation, page 8-5
- IS-IS Operation, page 8-6
- OSPF Operation, page 8-7
- IPv6 Routing Protocol Operation, page 8-7

Cisco Express Forwarding

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF is always enabled on the switch and cannot be disabled. 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 Protocol Operation

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.

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.

IS-IS Operation

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.

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.

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 re-acquire 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 the *OSPF RFC 3623 Graceful Restart* document.

IPv6 Routing Protocol Operation

IPv6 support for NSF includes the following features:

- Nonstop Forwarding and Graceful Restart for MP-BGP IPv6 Address Family, page 8-8
- Nonstop Forwarding for IPv6 RIP, page 8-8

- Nonstop Forwarding for IPv6 Static Routes, page 8-8

Nonstop Forwarding and Graceful Restart for MP-BGP IPv6 Address Family

The switch supports the graceful restart capability for IPv6 BGP unicast and VPNv6 address families, enabling Cisco NSF functionality for BGP IPv6. The BGP graceful restart capability allows the BGP routing table to be recovered from peers without keeping the TCP state.

NSF continues forwarding packets while routing protocols converge, therefore avoiding a route flap on switchover. Forwarding is maintained by synchronizing the FIB between the active and standby RP. On switchover, forwarding is maintained using the FIB. The RIB is not kept synchronized; therefore, the RIB is empty on switchover. The RIB is repopulated by the routing protocols and subsequently informs FIB about RIB convergence by using the NSF_RIB_CONVERGED registry call. The FIB tables are updated from the RIB, removing any stale entries. The RIB starts a failsafe timer during RP switchover, in case the routing protocols fail to notify the RIB of convergence.

The Cisco BGP address family identifier (AFI) model is modular and scalable, and supports multiple AFIs and subsequent address family identifier (SAFI) configurations.

For information about how to configure the IPv6 BGP graceful restart capability, see the "*Implementing Multiprotocol BGP for IPv6*" document.

Nonstop Forwarding for IPv6 RIP

RIP registers as an IPv6 NSF client. Doing so has the benefit of using RIP routes installed in the Cisco Express Forwarding table until RIP has converged on the standby.

Nonstop Forwarding for IPv6 Static Routes

Cisco NSF supports IPv6 static routes.

Default Settings for NSF

None.

How to Configure NSF

- Configuring and Verifying BGP for NSF, page 8-8 (optional)
- Configuring and Verifying EIGRP NSF, page 8-10 (optional)
- Configuring and Verifying OSPF NSF, page 8-11 (optional)
- Configuring and Verifying IS-IS NSF, page 8-12 (optional)
- Troubleshooting Cisco Nonstop Forwarding, page 8-14 (optional)

Configuring and Verifying BGP for NSF

- Configuring BGP for NSF, page 8-9
- Verifying NSF for BGP, page 8-9

Configuring BGP for NSF

Perform this task to configure BGP for NSF. Repeat this task on each BGP NSF peer device:

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

This example shows how to configure BGP for NSF:

```
Router> enable
Router# configure terminal
Router(config)# router bgp 120
Router(config-router)# bgp graceful-restart
```

Verifying NSF for BGP

Perform this task to verify that the graceful restart function is configured on the SSO-enabled networking device and on the neighbor devices:

	Command	Purpose
Step 1	`Router>` **`enable`**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`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	`Router#` **`show ip bgp neighbors`** `[`*`ip-address`* `[`**`advertised-routes`** `|` **`dampened-routes`** `|` **`flap-statistics`** `|` **`paths`** `[`*`reg-exp`*`]` `|` **`received prefix-filter`** `|` **`received-routes`** `|` **`routes`** `|` **`policy`** `[`**`detail`**`]]]`	Displays 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.

This example shows how to NSF for BGP:

```
Router> enable
Router# configure terminal
Router# show running-config
Router# show ip bgp neighbors
```

Configuring and Verifying EIGRP NSF

- Configuring EIGRP for NSF, page 8-10
- Verifying EIGRP for NSF, page 8-11

Configuring EIGRP for NSF

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.
- 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.

Perform this task to configure EIGRP for NSF. Repeat this procedure on each EIGRP NSF peer device:

	Command	Purpose
Step 1	Router> **enable**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **router eigrp** *as-number*	Enables an EIGRP routing process, and enters router configuration mode.
Step 4	Router(config-router)# **nsf** [{**cisco** | **ietf**} | **interface wait** *seconds* | **interval** *minutes* | **t3** [**adjacency** | **manual** *seconds*]	(Optional) Enables EIGRP NSF support on an NSF capable router. Enter this command 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	Router(config-router)# **timers nsf converge** *seconds*	Adjusts the maximum time that restarting router will wait for the EOT notification from an NSF-capable or NSF-aware peer.
Step 6	Router(config-router)# **timers nsf route-hold** *seconds*	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	Router(config-router)# **timers nsf signal** *seconds*	Adjusts the maximum time for the initial restart period.

This example shows how to configure EIGRP for NSF:

```
Router> enable
Router# configure terminal
Router(config)# router eigrp 109
Router(config-router)# nsf
Router(config-router)# timers nsf converge 60
Router(config-router)# timers nsf route-hold 120
Router(config-router)# timers nsf signal seconds
```

Verifying EIGRP for NSF

Perform this task to verify that NSF awareness or capability or both are enabled on the SSO-enabled networking device and on the neighbor devices.

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`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.

This example shows how to verify EIGRP for NSF:

```
Router> enable
Router# show ip protocols
```

Configuring and Verifying OSPF NSF

- Configuring OSPF for NSF, page 8-11
- Verifying OSPF for NSF, page 8-12

Configuring OSPF for NSF

Note All peer devices participating in OSPF NSF must be made OSPF NSF aware; 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.

Perform this task to configure OSPF for NSF:

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# router ospf process-id [vrf vpn-name]`	Enables an OSPF routing process, and places the router in router configuration mode.
Step 4	`Router(config-router)# nsf [{cisco | ietf} | interface wait seconds | interval minutes | t3 [adjacency | manual seconds]`	Enables EIGRP NSF support on an NSF capable router. • Enter this command on NSF-capable routers only.

This example shows how to configure OSPF for NSF:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12
Router(config-router)# nsf
```

Verifying OSPF for NSF

Perform this task to verify OSPF for NSF:

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# show ip ospf [process-id]`	Displays general information about OSPF routing processes.

This example shows how to verify OSPF for NSF:

```
Router> enable
Router# show ip ospf
```

Configuring and Verifying IS-IS NSF

- Configuring NSF for IS-IS, page 8-12
- Verifying NSF for IS-IS, page 8-13

Configuring NSF for IS-IS

Perform this task to configure NSF for IS-IS:

	Command	Purpose
Step 1	`Router> enable`	Enables privileged EXEC mode (enter your password if prompted).
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# router isis area-tag`	Enables the IS-IS routing protocol to specify an IS-IS process, and places the router in router configuration mode.
Step 4	`Router(config-router)# nsf [{cisco | ietf} | interface wait seconds | interval minutes | t3 [adjacency | manual seconds]`	Enables NSF operation for IS-IS. • **ietf**—Enables IS-IS in homogeneous network where adjacencies with networking devices supporting IETF draft-based restartability is guaranteed. • **cisco**—Runs IS-IS in heterogeneous networks that might not have adjacencies with NSF-aware networking devices.

	Command	Purpose
Step 5	`Router(config-router)# nsf interval minutes`	Configures the minimum time between Cisco NSF restart attempts.
Step 6	`Router(config-router)# nsf t3 {manual seconds | adjacency}`	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	`Router(config-router)# nsf interface wait seconds`	Specifies how long a Cisco NSF restart will wait for all interfaces with IS-IS adjacencies to come up before completing the restart.

This example shows how to configure NSF for IS-IS:

```
Router> enable
Router# configure terminal
Router(config)# router isis cisco1
Router(config-router)# nsf ietf
Router(config-router)# nsf interval 2
Router(config-router)# nsf t3 manual 40
Router(config-router)# nsf interface wait 15
```

Verifying NSF for IS-IS

Perform this task to verify NSF for IS-IS:

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

This example shows how to verify NSF for IS-IS:

```
Router> enable
Router# show running-config
Router# show isis nsf
```

Troubleshooting Cisco Nonstop Forwarding

To troubleshoot Cisco Nonstop Forwarding, use the following commands 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 CEF state on a networking device.
`Router# show clns neighbors`	Display both end-system and intermediate system 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 eigrp neighbors [interface-type | as-number | static | detail]`	To display detailed information about neighbors discovered by EIGRP.
`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.

Configuration Examples for NSF

- Example: Configuring BGP NSF, page 8-15
- Example: Configuring BGP NSF Neighbor Device, page 8-15
- Example: Verifying BGP NSF, page 8-15
- Example: Configuring EIGRP NSF Converge Timer, page 8-16
- Example: EIGRP Graceful-Restart Purge-Time Timer Configuration, page 8-16
- Example: Configuring EIGRP NSF Route-Hold Timer, page 8-16
- Example: Configuring EIGRP NSF Signal Timer, page 8-16

- Example: Disabling EIGRP NSF Support, page 8-17
- Example: Verifying EIGRP NSF, page 8-16
- Example: Configuring OSPF NSF, page 8-17
- Example: Verifying OSPF NSF, page 8-17
- Example: Configuring IS-IS NSF, page 8-18
- Example: Verifying IS-IS NSF, page 8-18

Example: Configuring BGP NSF

The following example shows how to configure BGP NSF on a networking device.

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

Example: Configuring BGP NSF Neighbor Device

The following example shows how to configure 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
```

Example: Verifying BGP NSF

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 family 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
```

Example: Configuring EIGRP NSF Converge Timer

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

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

Example: EIGRP Graceful-Restart Purge-Time Timer Configuration

The **timers graceful-restart purge-time** command is used to set the route-hold timer that determines how long an NSF-aware router that is running EIGRP will hold routes for an inactive peer. The following example shows how to set the route-hold timer to two minutes:

```
Router(config-router)# timers graceful-restart purge-time 120
```

Example: Configuring EIGRP NSF Route-Hold Timer

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 shows how to set the route-hold timer to two minutes.

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

Example: Configuring EIGRP NSF Signal Timer

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

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

Example: Verifying EIGRP NSF

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. 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. 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
```

Example: Disabling EIGRP NSF Support

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 shows how to disable NSF capability:

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

Example: Configuring OSPF NSF

The following example shows how to configure OSPF NSF on a networking device:

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

Example: Verifying OSPF NSF

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
```

Example: Configuring IS-IS NSF

The following example shows how to configure 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 shows how to configure IS-IS NSF for IETF operation on a networking device:

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

Example: Verifying IS-IS NSF

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
```

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum