EIGRP Nonstop Forwarding

EIGRP nonstop forwarding (NSF) capabilities are exchanged by EIGRP peers in hello packets. NSF works with the SSO feature in Cisco software to minimize the amount of time that a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover.

Note Throughout this document, the term Route Processor (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for EIGRP Nonstop Forwarding

- The networking device that is to be configured for NSF must first be configured for SSO. For more information, see the “Configuring Stateful Switchover” chapter in the *High Availability Configuration Guide*.
- All neighboring devices must be NSF-capable or NSF-aware.

- An NSF-aware device must be completely converged with the network before it can assist an NSF-capable device in an NSF restart operation.
- On platforms that support the Route Switch Processor (RSP), and where the Cisco Express Forwarding (CEF) switching mode is configurable, configure distributed CEF (dCEF) switching mode using the **ip cef distributed** command.

Note Distributed platforms that run a supporting version of Cisco software can support full NSF capabilities. These devices can perform a restart operation and can support other NSF capable peers.

Restrictions for EIGRP Nonstop Forwarding

- An NSF-aware device cannot support two NSF-capable peers that are performing an NSF restart operation at the same time. However, both neighbors will reestablish peering sessions after the NSF restart operation is complete.
- Single processor platforms that run a supporting version of Cisco software support only NSF awareness. These devices maintain adjacency and hold known routes for the NSF-capable neighbor until it signals that it is ready for the NSF-aware device to send its topology table or until the route-hold timer expires.

Information About EIGRP Nonstop Forwarding

Nonstop Forwarding

Note In the following content, the term Route Processor (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted.

NSF works with the SSO feature in Cisco software to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following an 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. NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

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 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 NSF operation.

The NSF feature provides the following benefits:

- Improved network availability—NSF continues forwarding network traffic and application state information so that user session information is maintained after a switchover.
- Overall network stability—Network stability may be improved with the reduction in the number of route flaps that had been created when devices in the network failed and lost their routing tables.
- Neighboring devices do not detect link flapping—Because the interfaces remain up across a switchover, neighboring devices do not detect a link flap (that is, the link does not go down and come back up).
- Prevention of 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.

NSF always runs together with SSO. 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 during an RP switchover. For some HA-aware protocols and applications, state information is synchronized from the active to the standby processor.

EIGRP NSF Operations

Cisco NSF is supported by the EIGRP protocol for routing and by CEF for forwarding. EIGRP 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.

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

- The EIGRP hello hold timer is expired to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware device to reply to the NSF-capable device more quickly reducing the amount of time required for the NSF-capable device 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 device will hold known routes for the NSF-capable neighbor.
- The NSF-aware device 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 device to send its topology table or the route-hold timer expires. If the route-hold timer expires on the NSF-aware device, the NSF-aware device will discard held routes and treat the NSF-capable device as a new device joining the network and reestablishing adjacency accordingly.
- The NSF-aware device will continue to send queries to the NSF-capable device that is still 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 device notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting devices. The NSF-capable device then returns to normal operation. The NSF-aware device will look for alternate paths (go

active) for any routes that are not refreshed by the NSF-capable (restarting device). The NSF-aware device will then return to normal operation. If all paths are refreshed by the NSF-capable device, the NSF-aware device will immediately return to normal operation.

NSF-aware devices are completely compatible with non-NSF-aware or non-NSF-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.

How to Configure EIGRP Nonstop Forwarding

Configuring and Verifying EIGRP NSF

Repeat this task on each peer device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **nsf**
5. **timers nsf converge** *seconds*
6. **timers nsf signal** *seconds*
7. **timers graceful-restart purge-time** *seconds*
8. **end**
9. **show ip protocols**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Device(config)# router eigrp 109`	Enables an EIGRP routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	**nsf** **Example:** `Device(config-router)# nsf`	Enables NSF capabilities. • This command is enabled by default. To disable nonstop forwarding capability, use the **no** form of this command.
Step 5	**timers nsf converge** *seconds* **Example:** `Device(config-router)# timers nsf converge 120`	Use this optional command to adjust the maximum time that the restarting device will wait for the EOT notification from an NSF-capable or NSF-aware peer. • Enter this command on NSF-capable devices only.
Step 6	**timers nsf signal** *seconds* **Example:** `Device(config-router)# timers nsf signal 20`	Use this optional command to adjust the maximum time for the initial restart period. • Enter this command on NSF-capable devices only.
Step 7	**timers graceful-restart purge-time** *seconds* **Example:** `Device(config-router)# timers graceful-restart purge-time 240`	Use this optional command to set the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer.
Step 8	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 9	**show ip protocols** **Example:** `Device# show ip protocols`	Displays the parameters and current state of the active routing protocol process.

Troubleshooting EIGRP Nonstop Forwarding

Use the following commands in any order to troubleshoot issues with nonstop forwarding using the EIGRP protocol.

SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug ip eigrp notifications**
4. **show cef nsf**
5. **show cef state**
6. **show ip cef**
7. **show ip eigrp neighbors detail**

DETAILED STEPS

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **debug eigrp nsf**

Example:

```
Device# debug eigrp nsf
```

Displays notifications and information about NSF events for an EIGRP routing process.

Step 3 **debug ip eigrp notifications**

Example:

```
Device# debug ip eigrp notifications
```

Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.

Step 4 **show cef nsf**

Example:

```
Device# show cef nsf
```

Displays the current NSF state of CEF on both the active and standby RPs.

Step 5 **show cef state**

Example:

```
Device# show cef state
```

Displays the CEF state on a networking device.

Step 6 **show ip cef**

Example:

```
Device# show ip cef
```

Displays entries in the FIB that are unresolved or displays a FIB summary.

Step 7 **show ip eigrp neighbors detail**

Example:

```
Device# show ip eigrp neighbors detail
```

Displays detailed information about neighbors discovered by EIGRP.

Configuration Examples for EIGRP Nonstop Forwarding

Example: EIGRP NSF

The following sample output shows that EIGRP NSF support is present in the installed software image.

- "EIGRP NSF-aware route hold timer is . . ." is displayed in the output for either NSF-aware or NSF-capable devices, and the default or user-defined value for the route-hold timer is displayed.
- "EIGRP NSF enabled" or "EIGRP NSF disabled" appears in the output only when the NSF capability is supported by the device.

```
Device# 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
```

Feature Information for Overview of Cisco TrustSec

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.