EIGRP Nonstop Forwarding (NSF) Awareness

Nonstop Forwarding (NSF) awareness allows an NSF-aware router to assist NSF-capable and NSF-aware neighbors to continue forwarding packets during a switchover operation or during a well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running Enhanced Interior Gateway Routing Protocol (EIGRP) to forward packets along routes that are already known for a router that is performing a switchover operation or is in a well-known failure mode. This capability allows the EIGRP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

Feature Specifications for the EIGRP Nonstop Forwarding (NSF) Awareness feature

Feature History	
Release	**Modification**
12.2(15)T	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.2(15)T, use Cisco Feature Navigator as described below.	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites for EIGRP Nonstop Forwarding Awareness

This document assumes that your network is configured to run EIGRP. The following tasks must also be completed before you can configure this feature:

- An NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in an NSF restart operation.
- A version of Cisco IOS that support NSF awareness or NSF capabilities must be installed.

Restrictions for EIGRP Nonstop Forwarding Awareness

The following restrictions apply to the EIGRP Nonstop Forwarding Awareness feature:

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

Information About EIGRP Nonstop Forwarding Awareness

To configure this feature, you must understand the following concepts:

- Cisco NSF Routing and Forwarding Operation, page 2
- Cisco Express Forwarding, page 3
- EIGRP Nonstop Forwarding Awareness, page 3
- EIGRP NSF Capable and NSF Aware Interoperation, page 4
- Non-NSF Aware EIGRP Neighbors, page 4
- EIGRP NSF Route-Hold Timers

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, 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.

Note Currently, EIGRP supports only NSF awareness. Full support for NSF and SSO for EIGRP will be integrated into a future release.

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.

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 for 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

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.

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

EIGRP Nonstop Forwarding Awareness

NSF awareness allows a router that is running EIGRP to assist NSF-capable neighbors to continue forwarding packets during a switchover operation or well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature provides EIGRP with the capability to detect a neighbor that is undergoing an NSF restart event (route processor [RP] switchover operation) or well-known failure condition, maintain the peering session with this neighbor, retain known routes, and continue to forward packets for these routes. The deployment of EIGRP NSF awareness can minimize the affects of the following:

- Well-known failure conditions (for example, a stuck-in-active event).
- Unexpected events (for example, an RP switchover operation).
- Scheduled events (for example, a hitless software upgrade).

EIGRP NSF awareness is enabled by default, and its operation is transparent to the network operator and EIGRP peers that do not support NSF capabilities.

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

EIGRP NSF Capable and NSF Aware Interoperation

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 router expires the EIGRP hello hold timer 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 and reduces the amount of time required for the NSF-capable router to rediscover neighbors and rebuild the topology table.
- The router starts the route-hold timer. 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 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.

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.

Non-NSF Aware EIGRP Neighbors

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 the adjacency when they are received.

The NSF-capable router will drop any queries that are received while converging to minimize the number of transient routes that are sent to neighbors. But the NSF-capable router will still acknowledge these queries to prevent these neighbors from resetting adjacency.

Note 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.

EIGRP NSF Route-Hold Timers

The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

The route-hold timer is configured with the **timers nsf route-hold** router configuration command. The default time period for the route-hold timer is 240 seconds. The configurable range is from 10 to 300 seconds.

How to Modify and Maintain EIGRP Nonstop Forwarding Awareness

This section contains the following procedures for configuring the EIGRP Nonstop Forwarding Awareness feature:

Adjusting NSF Route-Hold Timers

Use the following steps to configure NSF route-hold timers on an NSF-aware router:

Route-Hold Timers

The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router eigrp** *as-number*
4. **timers nsf route-hold** *seconds*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 101`	Enters router configuration mode and creates an EIGRP routing process.
Step 4	**timers nsf route-hold** seconds **Example:** `Router(config-router)# timers nsf route-hold 120`	Sets the maximum period of time that an NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation. The configurable range of time for the *seconds* argument is from 20 to 300 seconds. The default value is 240 seconds. The example sets the route-hold timer to 2 minutes.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and enters global configuration mode.

Troubleshooting Tips

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.

Monitoring EIGRP NSF Debug Events and Notifications

Use the following steps to monitor EIGRP NSF debug events and notifications on an NSF-aware router:

Debug Commands

The **debug eigrp nsf** and **debug ip eigrp notifications** commands do not need to be issued together or even in the same session as there are differences in the information that is provided. These commands are provided together for example purposes.

The output of debug commands can be very verbose. These commands should not be deployed in a production network unless you are troubleshooting a problem.

SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug eigrp ip notifications**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eigrp nsf** **Example:** `Router# debug eigrp nsf`	Displays NSF notifications and information about NSF events in an EIGRP network on the console of the router.
Step 3	**debug ip eigrp notifications** **Example:** `Router# debug ip eigrp notifications`	Displays EIGRP events and notifications in the console of the router. The output from this command also includes NSF notifications and information about NSF events.

Verifying the Local Configuration of EIGRP NSF Awareness

Use the following steps to verify the local configuration of NSF-awareness on a router that is running EIGRP:

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as 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. The output of this command can be used to verify EIGRP NSF-awareness.

Configuration Examples for EIGRP Nonstop Forwarding Awareness

EIGRP Route-Hold Timer Configuration 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(config-router)# timers nsf route-hold 120
```

Monitoring EIGRP NSF Debug Events and Notifications Configuration Example

The following example output shows that the NSF-aware router has received the restart notification. The NSF-aware router will now wait for EOT to be sent from the restarting neighbor (NSF-capable).

```
Router# debug ip eigrp notifications

*Oct  4 11:39:18.092:EIGRP:NSF:AS2. Rec RS update from 135.100.10.1,
00:00:00. Wait for EOT.
*Oct  4 11:39:18.092:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 2:Neighbor
135.100.10.1 (POS3/0) is up:peer NSF restarted
```

Verifying Local Configuration of EIGRP NSF Awareness

The following is example output from the **show ip protocols** command. The output from this command can be used to verify the local configuration of the EIGRP NSF awareness. The output below shows that the router is NSF-aware and that the route-hold timer is set to 240 seconds, which is the default value for the route-hold timer.

```
Router# show ip protocols

Routing Protocol is "eigrp 101"
  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 101
  EIGRP NSF-aware route hold timer is 240s
  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
```

Additional References

For additional information related to EIGRP Nonstop Forwarding Awareness feature, refer to the following references:

Related Documents

Related Topic	Document Title
CEF commands	*Cisco IOS Switching Services Configuration Guide*, Release 12.2
CEF configuration tasks	*Cisco IOS Switching Services Command Reference*, Release 12.2
EIGRP commands	*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*, Release 12.2
EIGRP configuration tasks	*Cisco IOS IP Configuration Guide*, Release 12.2

Standards

Standards[1]	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

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

http://www.cisco.com/register

RFCs

RFCs[1]	Title
draft-ietf-idr-restart-06.txt	*Graceful Restart Mechanism for BGP*

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new, debug, and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

New Commands

- **timers nsf route-hold**

Debug Commands

- **debug eigrp nsf**
- **debug ip eigrp notifications**

Modified Commands

- **show ip eigrp neighbors**
- **show ip protocols**

timers nsf route-hold

To set the route-hold timer to determine how long an NSF-aware router that is running EIGRP will hold routes for an inactive peer, use the **timers nsf route-hold** command in router configuration mode. To return the route-hold timer to the default value, use the **no** form of this command.

timers nsf route-hold *seconds*

no timers nsf route-hold

Syntax Description

seconds	The time, in seconds, that EIGRP will hold routes for an inactive peer. The configurable time range is from 20 to 300 seconds.

Defaults

EIGRP NSF awareness is enabled by default. The default value for the route-hold timer is 240 seconds.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The route-hold timer sets the maximum period of time that the NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

Examples

The following configuration example sets the route-hold timer value for an NSF-aware router. In the example, the route-hold timer is set to 2 minutes:

```
Router(config-router)# timers nsf route-hold 120
```

Related Commands

Command	Description
debug eigrp nsf	Displays EIGRP NSF-specific events in the console of a router.
debug ip eigrp notifications	Displays EIGRP events and notifications in the console of the router.
show ip eigrp neighbors	Displays the neighbors discovered by IP EIGRP.
show ip protocols	Displays the parameters and current state of the active routing protocol process.

debug eigrp nsf

To display NSF-specific events in the console of the router, use the **debug eigrp nsf** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug eigrp nsf

no debug eigrp nsf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The output from the **debug eigrp nsf** command displays NSF-specific events. This command can be issued on an NSF-capable or NSF-aware router.

Examples

The following example enables EIGRP NSF debugging:

```
Router# debug eigrp nsf
```

Related Commands

Command	Description
timers nsf route-hold	Sets the route-hold timer for NSF-aware routers that run EIGRP.

debug ip eigrp notifications

To display EIGRP events and notifications in the console of the router, use the **debug ip eigrp notifications** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ip eigrp notifications

no debug ip eigrp notifications

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The output from the **debug ip eigrp notifications** command displays EIGRP events and notifications.

Examples

The foll owing example output shows that the NSF-aware router has received the restart notification. The NSF-aware router will now wait for EOT to be sent from the restarting neighbor (NSF-capable).

```
Router# debug ip eigrp notifications

*Oct  4 11:39:18.092:EIGRP:NSF:AS2. Rec RS update from 135.100.10.1,
00:00:00. Wait for EOT.
*Oct  4 11:39:18.092:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 2:Neighbor
135.100.10.1 (POS3/0) is up:peer NSF restarted
```

Related Commands

Command	Description
timers nsf route-hold	Sets the route-hold timer for NSF-aware routers that run EIGRP.

show ip eigrp neighbors

To display the neighbors discovered by Enhanced IGRP (EIGRP), use the **show ip eigrp neighbors** command in EXEC mode.

show ip eigrp neighbors [*interface-type* | *as-number* | **static** | **detail**]

Syntax Description

interface-type	(Optional) Filters that output by interface.
as-number	(Optional) Filters that output by autonomous system number.
static	(Optional) Displays static routes.
detail	(Optional) Displays detailed neighbor information.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	The **static** keyword was added.
12.2(15)T	Support for NSF restart operations was integrated into the output.

Usage Guidelines

Use the **show ip eigrp neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

Examples

show ip eigrp neighbors Example

The following is sample output from the **show ip eigrp neighbors** command:

```
Router# show ip eigrp neighbors

IP-EIGRP Neighbors for process 77
Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14       0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12       0:02:02  0      4    5     20
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip eigrp neighbors Field Descriptions

Field	Description
process 77	Autonomous system number specified in the **router** configuration command.
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.

Table 1 show ip eigrp neighbors Field Descriptions (continued)

Field	Description
Holdtime	Length of time (in seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, the nondefault hold time will be displayed.
Uptime	Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.

show ip eigrp neighbors detail Example

The following is sample output from the **show ip eigrp neighbors** command when issued with the **detail** keyword:

```
Router# show ip eigrp neighbors detail

IP-EIGRP neighbors for process 101
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3 1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans:0, Retries:0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0               11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0               13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0               12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

Table 1 describes the significant fields shown in the display.

Table 2 show ip eigrp neighbors Field Descriptions

Field	Description
process 77	Autonomous system number specified in the **router** configuration command.
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.

Table 2 show ip eigrp neighbors Field Descriptions (continued)

Field	Description
Holdtime	Length of time (in seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, the nondefault hold time will be displayed.
Uptime	Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.
Retries	The number of times an attempt was made to retransmit a packet.
Restart time	Elapsed time (in hours:minutes: seconds) since the specified neighbor has restarted.

show ip protocols

To display the parameters and current state of the active routing protocol process, use the **show ip protocols** command in EXEC mode.

show ip protocols

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	Support for the route-hold timer was integrated into the output.

Usage Guidelines

The information displayed by the **show ip protocols** command is useful in debugging routing operations. Information in the Routing Information Sources field of the **show ip protocols** output can help you identify a router suspected of delivering bad routing information.

Examples

EIGRP Example

The following is sample output from the **show ip protocols** command that shows Enhanced IGRP processes:

```
Router# show ip protocols

Routing Protocol is "eigrp 77"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: eigrp 77
  Automatic network summarization is in effect
  Routing for Networks:
    172.180.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.180.81.28          90      0:02:36
    172.180.80.28          90      0:03:04
    172.180.80.31          90      0:03:04
  Distance: internal 90 external 170
```

Table 3 describes the significant fields shown in the display.

Table 3 show ip protocols Field Descriptions for Enhanced IGRP Processes

Field	Description
Routing Protocol is “eigrp 77”	Name and autonomous system number of the currently running routing protocol.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the **distribute-list out** command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the **distribute-list in** command.
Redistributing: eigrp 77	Indicates whether route redistribution has been enabled with the **redistribute** command.
Automatic network summarization...	Indicates whether route summarization has been enabled with the **auto-summary** command.
Routing for Networks:	Networks for which the routing process is currently injecting routes.
Routing Information Sources:	Lists all the routing sources that the Cisco IOS software is using to build its routing table. The following is displayed for each source: • IP address • Administrative distance • Time the last update was received from this source
Distance: internal 90 external 170	Internal and external distances of the router. Internal distance is the degree of preference given to Enhanced IGRP internal routes. External distance is the degree of preference given to Enhanced IGRP external routes.

IS-IS Example

The following is sample output from the **show ip protocols** command that shows Intermediate System-to-Intermediate System (IS-IS) processes:

```
Router# show ip protocols

Routing Protocol is "isis"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Routing for Networks:
    Serial0
  Routing Information Sources:
  Distance: (default is 115)
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip protocols Field Descriptions for IGRP Processes

Field	Description
Routing Protocol is “isis”	Specifies the routing protocol used.
Sending updates every 0 seconds	Specifies the time between sending updates.

Table 4 show ip protocols Field Descriptions for IGRP Processes (continued)

Field	Description
Invalid after 0 seconds	Specifies the value of the invalid parameter.
hold down 0	Specifies the current value of the hold-down parameter.
flushed after 0	Specifies the time (in seconds) after which the individual routing information will be thrown out (flushed).
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default networks	Specifies how these networks will be handled in both incoming and outgoing updates.
IGRP metric	Specifies the value of the K0-K5 metrics, and the maximum hop count.
Redistributing	Lists the protocol that is being redistributed.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

RIP Example

The following is sample output from the **show ip protocols** command that shows Routing Information Protocol (RIP) processes:

```
Router# show ip protocols

Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 2 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface         Send  Recv   Key-chain
    Ethernet0         2     2      trees
    Fddi0             2     2
  Routing for Networks:
    172.19.0.0
    10.2.0.0
    10.3.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip protocols Field Descriptions for IGRP Processes

Field	Description
Routing Protocol is “rip”	Specifies the routing protocol used.
Sending updates every 30 seconds	Specifies the time between sending updates.
next due in 2 seconds	Precisely when the next update is due to be sent.
Invalid after 180 seconds	Specifies the value of the invalid parameter.
hold down for 180	Specifies the current value of the hold-down parameter.
flushed after 240	Specifies the time (in seconds) after which the individual routing information will be thrown (flushed) out.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default version control:	Specifies the version of RIP packets that are sent and received.
Redistributing	Lists the protocol that is being redistributed.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

EIGRP NSF Awareness Verification Example

The following is sample output from the **show ip protocols** command. The output shows that the router is running EIGRP, is NSF-aware, and that the route-hold timer is set 240 seconds, which is the default value for the route-hold timer.

```
Router# show ip protocols

Routing Protocol is "eigrp 101"
  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 101
  EIGRP NSF-aware route hold timer is 240s
  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
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip protocols Field Descriptions for IGRP Processes

Field	Description
Routing Protocol is “eigrp 101”	Specifies the routing protocol used.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default networks...	Specifies how these networks will be handled in both incoming and outgoing updates.
EIGRP...	Specifies the value of the K0-K5 metrics, and the maximum hop count.
Redistributing	Lists the protocol that is being redistributed.
EIGRP NSF-Aware...	Displays the route-hold timer value.
Automatic network summarization...	Specifies that automatic summarization is enabled.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source