



Reducing Failure Detection Times in IS-IS Networks

First Published: November 30, 2007
Last Updated: March 26, 2009

This module describes how to customize IS-IS configuration to help you achieve fast convergence in your network. This module describes how to configure Bidirectional Failure Detection (BFD) as well as other tasks to optimize how a router that runs IS-IS detects link failures and topology changes, sends important topology change updates to its neighbors, and reacts to the topology change updates that it receives from its neighbors, in order to increase network performance.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Reducing Failure Detection Times in IS-IS Networks”](#) section on page 18.

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

Contents

- [Prerequisites for Reducing Failure Detection Times in IS-IS Networks, page 2](#)
- [Information About Reducing Failure Detection Times in IS-IS Networks, page 2](#)
- [How to Reduce Failure Detection Times in IS-IS Networks, page 2](#)
- [Configuration Examples for Reducing Failure Detection Times in IS-IS Networks, page 14](#)
- [Where to Go Next, page 16](#)



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

- [Additional References, page 16](#)
- [Feature Information for Reducing Failure Detection Times in IS-IS Networks, page 18](#)

Prerequisites for Reducing Failure Detection Times in IS-IS Networks

Before performing the tasks in this module, you should be familiar with the concepts described in the “[Overview of IS-IS Fast Convergence](#)” module.

Information About Reducing Failure Detection Times in IS-IS Networks

You should understand the following concept before you configure any features in this module:

[Importance of Fast Network Failure Detection, page 2](#)

Importance of Fast Network Failure Detection

You can customize your IS-IS network to reduce the amount of time it takes for network failures to be discovered. When failures are detected more quickly, networks can react to them sooner and alternate paths can be selected more quickly, speeding up network convergence.

How to Reduce Failure Detection Times in IS-IS Networks

The tasks in this section explain how to customize IS-IS to decrease failure detection times. The first task is required, but the other tasks are optional.

- [Using Bidirectional Forwarding Failure Detection to Decrease Failure Detection Times, page 2](#)
- [Using IP Event Dampening to Decrease Failure Detection Times, page 7](#)
- [Tuning IS-IS Hello Parameters to Decrease Link Failure Detection Times, page 8](#)
- [Configuring an IS-IS Point-to-Point Adjacency over Broadcast Media to Reduce Link Failure Detection Times, page 10](#)
- [Monitoring IS-IS Network Convergence Time, page 12](#)

Using Bidirectional Forwarding Failure Detection to Decrease Failure Detection Times

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the

network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.

For complete information about the BFD feature, see the following documentation:

[Bidirectional Forwarding Detection](#)

You must perform the following two tasks to configure BFD session parameters on the interface and configure BFD support for IS-IS:

- [Configuring BFD Session Parameters on the Interface, page 3](#)
- [Configuring BFD Support for IS-IS, page 4](#)

Configuring BFD Session Parameters on the Interface

The steps in this procedure show how to configure BFD on the interface by setting the baseline BFD session parameters on an interface. Repeat the steps in this procedure for each interface over which you want to run BFD sessions to BFD neighbors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface FastEthernet 6/0	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	<pre>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</pre> <p>Example: Router(config-if)# bfd interval 50 min_rx 50 multiplier 5</p>	Enables BFD on the interface.
Step 5	<pre>end</pre> <p>Example: Router(config-if)# end</p>	Exits interface configuration mode.

Configuring BFD Support for IS-IS

You can enable BFD support for routing protocols at the router level to enable BFD support globally for all interfaces or you can configure BFD on a per-interface basis at the interface level.

For Cisco IOS Release 12.4(4)T, and later releases, you must configure BFD support for one or more of the following routing protocols: BGP, IS-IS, and OSPF.

This section describes the procedures for configuring BFD support for IS-IS, so that IS-IS is a registered protocol with BFD and will receive forwarding path detection failure messages from BFD. There are two methods for enabling BFD support for IS-IS:

- You can enable BFD for all of the interfaces for which IS-IS is routing by using the **bfd all-interfaces** command in router configuration mode. You can then disable BFD for one or more of those interfaces using the **isis bfd disable** command in interface configuration mode.
- You can enable BFD for a subset of the interfaces for which IS-IS is routing by using the **isis bfd** command in interface configuration mode.

To configure BFD support for IS-IS, perform the steps in one of the following sections:

- [Configuring BFD Support for IS-IS for All Interfaces, page 4](#)
- [Configuring BFD Support for IS-IS for One or More Interfaces, page 6](#)

Prerequisites

IS-IS must be running on all participating routers.

The baseline parameters for BFD sessions on the interfaces that you want to run BFD sessions to BFD neighbors over must be configured. See the [“Configuring BFD Session Parameters on the Interface” section on page 3](#) for more information.

Configuring BFD Support for IS-IS for All Interfaces

To configure BFD on all IS-IS interfaces, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis area-tag**
4. **bfd all-interfaces**

5. **exit**
6. **interface** *type number*
7. **isis bfd** [**disable**]
8. **end**
9. **show bfd neighbors** [**details**]
10. **show clns interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router isis <i>area-tag</i> Example: Router(config)# router isis tag1	Specifies an IS-IS process and enters router configuration mode.
Step 4	bfd all-interfaces Example: Router(config-router)# bfd all-interfaces	Enables BFD globally on all interfaces associated with the IS-IS routing process.
Step 5	exit Example: Router(config-router)# exit	(Optional) Returns the router to global configuration mode. Enter this command only if you want to follow Step 6 and Step 7 to disable BFD for one or more interfaces.
Step 6	interface <i>type number</i> Example: Router(config)# interface fastethernet 6/0	(Optional) Enters interface configuration mode.
Step 7	isis bfd [disable] Example: Router(config-if)# isis bfd	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. Note You should use the disable keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the bfd all-interfaces command in router configuration mode.
Step 8	end Example: Router(config-if)# end	Returns the router to privileged EXEC mode.

	Command or Action	Purpose
Step 9	show bfd neighbors [details] Example: Router# show bfd neighbors details	Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. Note In order to display the full output of the show bfd neighbors details command on a Cisco 12000 series router, you must enter the command on the line card. Enter the attach slot-number command to establish a CLI session with a line card. The registered protocols are not shown in the output of the show bfd neighbors details command when it is entered on a line card.
Step 10	show clns interface Example: Router# show clns interface	Displays information that can be used to verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

Configuring BFD Support for IS-IS for One or More Interfaces

To configure BFD for only one or more IS-IS interfaces, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **isis bfd [disable]**
5. **end**
6. **show bfd neighbors [details]**
7. **show clns interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Router(config)# interface fastethernet 6/0	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	isis bfd [disable] Example: Router(config-if)# isis bfd	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. Note You should use the disable keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the bfd all-interfaces command in router configuration mode.
Step 5	end Example: Router(config-if)# end	Returns the router to privileged EXEC mode.
Step 6	show bfd neighbors [details] Example: Router# show bfd neighbors details	Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. Note In order to display the full output of the show bfd neighbors details command on a Cisco 12000 series router, you must enter the command on the line card. Enter the attach slot-number command to establish a CLI session with a line card. The registered protocols are not shown in the output of the show bfd neighbors details command when it is entered on a line card.
Step 7	show clns interface Example: Router# show clns interface	Displays information that can help verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

Using IP Event Dampening to Decrease Failure Detection Times

The task described in this section is recommended to make link failure detection faster and more reliable for IS-IS networks. IP event dampening introduces a configurable exponential delay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping, removing it from the network until it becomes stable again. Thus, the network becomes more stable, with a faster convergence time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **dampening** [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress-time restart-penalty*]
5. **exit**
6. **show dampening interface**
7. **show interface dampening**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type number</code> Example: Router(config)# interface FastEthernet 0/1	Enters interface configuration mode.
Step 4	<code>dampening [half-life-period reuse-threshold]</code> <code>[suppress-threshold max-suppress-time</code> <code>[restart-penalty]]</code> Example: Router(config-if)# dampening	Enables interface dampening. <ul style="list-style-type: none"> Entering the dampening command without any keywords or arguments enables interface dampening with the default configuration parameters. <p>Note The default values for the <i>half-life-period</i>, <i>reuse-threshold</i>, <i>suppress-threshold</i>, <i>max-suppress-time</i>, and <i>restart-penalty</i> arguments are 5, 1000, 2000, 20, and 2000, respectively.</p> <ul style="list-style-type: none"> When the timer for the <i>restart-penalty</i> argument is manually configured, the values must be manually entered for all arguments.
Step 5	<code>end</code> Example: Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	<code>show dampening interface</code> Example: Router# show dampening interface	Displays a summary of dampened interfaces.
Step 7	<code>show interface dampening</code> Example: Router# show interface dampening	Displays dampened interfaces on the local router.

Tuning IS-IS Hello Parameters to Decrease Link Failure Detection Times

Tuning hello parameters should be considered only when the link type does not offer fast enough link failure detection. The standard default values for the hello interval and hello multiplier are 10 seconds and 3 seconds. Therefore, the multiplier times the interval will give a default hold-time of 30 seconds.

Although a slower hello interval saves bandwidth and CPU usage, there are some situations when a faster hello interval is preferred. In the case of a large configuration that uses Traffic Engineering (TE) tunnels, if the TE tunnel uses ISIS as the Interior Gateway Protocol (IGP), and the IP routing process is restarted at the router at the ingress point of the network (headend), then all the TE tunnels get resignaled with the default hello interval. A faster hello interval prevents this resignaling. To configure a faster hello interval, you need to increase the ISIS hello interval manually using the **isis hello-interval** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**]
5. **isis hello-multiplier** *multiplier* [**level-1** | **level-2**]
6. **end**

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 Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-type interface-number</i> Example: Router(config)# interface Ethernet 0/1	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<pre>isis hello-interval {seconds minimal} [level-1 level-2]</pre> <p>Example: Router(config-if)# isis hello-interval 5 level-1</p>	<p>Specifies the length of time between the sending of IS-IS hello PDUs.</p> <ul style="list-style-type: none"> The default value is 10. The hello interval multiplied by the hello multiplier equals the hold time. If the minimal keyword is specified, the hold time is 1 second and the system computes the hello interval based on the hello multiplier. The hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because only a single type of hello PDU is sent on serial links, it is independent of Level 1 or Level 2.) The level-1 and level-2 keywords are used on X.25, SMDS, and Frame Relay multiaccess networks or LAN interfaces. <p>Note A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network, due to false failure detection events. A slower hello interval saves bandwidth and CPU. Especially when used in combination with a higher hello multiplier, this configuration may increase overall network stability, but has typical slower network convergence as a consequence.</p>
Step 5	<pre>isis hello-multiplier multiplier [level-1 level-2]</pre> <p>Example: Router(config-if)# isis hello-multiplier 6 level-1</p>	<p>Specifies the number of IS-IS hello PDUs a neighbor must miss before the router should declare the adjacency as down.</p> <ul style="list-style-type: none"> The default value is 3. A multiplier value of 1 is very aggressive—we recommend a value of at least 2.
Step 6	<pre>end</pre> <p>Example: Router(config-if)# end</p>	<p>Returns to privileged EXEC mode.</p>

Configuring an IS-IS Point-to-Point Adjacency over Broadcast Media to Reduce Link Failure Detection Times

Benefits of Configuring a Point-to-Point Adjacency

Configuring a point-to-point adjacency over a broadcast media can improve convergence times of a customer's network because it prevents the system from electing a designated router (DR), prevents flooding from using CSNPs for database synchronization, and simplifies shortest path first (SPF) computations.

Restrictions

We recommend that you perform this task only for IS-IS networks that consist of only two networking devices connected to broadcast media. Such networks are usually configured as a point-to-point link rather than a broadcast link. In this case, it is recommended to follow this task to decrease the link failure detection time.

Having a multipoint interface instead of the point-to-point interfaces will cause the creation of a pseudonode on the network. The addition of the pseudonode means that the router must retain information about it. To decrease the size of the topology database of the router, thereby reducing the memory requirement of the router and increasing the efficiency of the SPF calculation since there is one less node involved, configure point-to-point interfaces when possible.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isis network point-to-point**
5. **end**

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 Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-type interface-number</i> Example: Router(config)# interface Fastethernet 4/0	Configures an interface type and enters interface configuration mode.
Step 4	isis network point-to-point Example: Router(config-if)# isis network point-to-point	Configures a network of only two networking devices that use broadcast media and the integrated IS-IS routing protocol to function as a point-to-point link instead of a broadcast link.
Step 5	end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Monitoring IS-IS Network Convergence Time

You can use one or more of the following commands to monitor convergence times for your IS-IS network. You do not need to enter the **show** commands in any specific order.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isis display delimiter** [*return count* | *character count*]
4. **exit**
5. **show isis database** [*level-1*] [*level-2*] [*l1*] [*l2*] [*detail*] [*lspid*]
6. **show isis** [*area-tag*] **routes**
7. **show isis spf-log**
8. **show isis** [*process-tag*] **topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	isis display delimiter [return count character count] Example: Router(config)# isis display delimiter return 2	Makes output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information.
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.
Step 5	show isis database [level-1] [level-2] [11] [12] [detail] [lspid] Example: Router# show isis database detail	Displays the IS-IS link-state database.
Step 6	show isis [process-tag] routes Example: Router# show isis financetag routes	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	show isis spf-log Example: Router# show isis spf-log	Displays how often and why the router has run a full SPF calculation.
Step 8	show isis [process-tag] topology Example: Router# show isis financetag topology	Displays a list of all connected routers in all areas. <ul style="list-style-type: none">• If a process tag is specified, output is limited to the specified routing process. When “null” is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.

Configuration Examples for Reducing Failure Detection Times in IS-IS Networks

This section provides the following configuration examples:

- [Configuring BFD in an IS-IS Network: Example, page 14](#)
- [Configuring IS-IS to Achieve Fast Convergence by Reducing Failure Detection Times: Example, page 16](#)

Configuring BFD in an IS-IS Network: Example

In the following example, the simple IS-IS network consists of Router A and Router B. Fast Ethernet interface 0/1 on Router A is connected to the same network as Fast Ethernet interface 6/0 for Router B. The example, starting in global configuration mode, shows the configuration of BFD.

Configuration for Router A

```
!
interface FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 ip router isis
  bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 3/0.1
 ip address 172.17.0.1 255.255.255.0
 ip router isis
!
router isis
 net 49.0001.1720.1600.1001.00
  bfd all-interfaces
!
```

Configuration for Router B

```
!
interface FastEthernet 6/0
 ip address 172.16.10.2 255.255.255.0
 ip router isis
  bfd interval 50 min_rx 50 multiplier 3
!
interface FastEthernet 6/1
 ip address 172.18.0.1 255.255.255.0
 ip router isis
!
router isis
 net 49.0000.0000.0002.00
  bfd all-interfaces
!
```

The output from the **show bfd neighbors details** command from Router A verifies that a BFD session has been created and that IS-IS is registered for BFD support:

Router A

RouterA# **show bfd neighbors details**

OurAddr	NeighAddr	LD/RD	RH	Holdown(mult)	State	Int
172.16.10.1	172.16.10.2	1/8	1	536 (3)	Up	Fa0/1

```

Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(23543)
Rx Count: 13877, Rx Interval (ms) min/max/avg: 200/448/335 last: 64 ms ago
Tx Count: 23546, Tx Interval (ms) min/max/avg: 152/248/196 last: 32 ms ago
Registered protocols: ISIS
Uptime: 01:17:09
Last packet: Version: 0           - Diagnostic: 0
              I Hear You bit: 1    - Demand bit: 0
              Poll bit: 0          - Final bit: 0
              Multiplier: 3        - Length: 24
              My Discr.: 8         - Your Discr.: 1
              Min tx interval: 50000 - Min rx interval: 1000
              Min Echo interval: 0

```

The output from the **show bfd neighbors details** command from the line card on Router B verifies that a BFD session has been created:



Note

Router B is a Cisco 12000 series router. The **show bfd neighbors details** command must be run on the line cards. The **show bfd neighbors details** command will not display the registered protocols when it is entered on a line card.

Router B

RouterB# **attach 6**

Entering Console for 8 Port Fast Ethernet in Slot: 6

Type "exit" to end this session

Press RETURN to get started!

LC-Slot6> **show bfd neighbors details**

Cleanup timer hits: 0

```

OurAddr      NeighAddr    LD/RD RH  Holdown(mult)  State    Int
172.16.10.2  172.16.10.1  8/1  1  1000 (5 )     Up      Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0           - Diagnostic: 0
              I Hear You bit: 1    - Demand bit: 0
              Poll bit: 0          - Final bit: 0
              Multiplier: 5        - Length: 24
              My Discr.: 1         - Your Discr.: 8
              Min tx interval: 200000 - Min rx interval: 200000
              Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
IPC Tx Failure Count: 0
IPC Rx Failure Count: 0
Total Adjs Found: 1

```

Configuring IS-IS to Achieve Fast Convergence by Reducing Failure Detection Times: Example

The following example configures Ethernet interface 0/0 to use IP event dampening, setting the half life to 30 seconds, the reuse threshold to 1500, the suppress threshold to 10,000, and the maximum suppress time to 120 seconds. The IS-IS hello parameters have also been tuned for more rapid failure detection

```
enable
configure terminal
interface Ethernet 0/0
dampening 30 1500 10000 120
isis hello-interval minimal
isis hello-multiplier 2
```

Where to Go Next

To configure additional features to improve IS-IS network convergence times, complete the optional tasks in one or more of the following modules:

- [“Setting Best Practice Parameters for IS-IS Fast Convergence”](#)
- [“Reducing Link Failure and Topology Change Notification Times in IS-IS Networks”](#)
- [“Reducing Alternate-Path Calculation Times in IS-IS Networks”](#)

Additional References

The following sections provide references related to reducing failure detection times in IS-IS networks.

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	Cisco IOS IP Routing Protocols Command Reference
Roadmap of IS-IS features	“Integrated IS-IS Features Roadmap” module
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	“Integrated IS-IS Routing Protocol Overview” module

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Reducing Failure Detection Times in IS-IS Networks

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1), 12.0(3)S, or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Integrated IS-IS Features Roadmap](#)” module.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Reducing Failure Detection Times in IS-IS Networks

Feature Name	Software Releases	Feature Information
IS-IS Support for BFD over IPv4	12.4(4)T	<p>Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and convergence time will be consistent and predictable.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Using Bidirectional Forwarding Failure Detection to Decrease Failure Detection Times, page 2
Integrated IS-IS Point-to-Point Adjacency over Broadcast Media	12.2(8)T	<p>When a network consists of only two networking devices connected to broadcast media and uses the integrated IS-IS protocol, it is better for the system to handle the link as a point-to-point link instead of as a broadcast link. This feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring an IS-IS Point-to-Point Adjacency over Broadcast Media to Reduce Link Failure Detection Times, page 10

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS,

Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.

