Integrated IS-IS Commands

advertise-passive-only

To configure Intermediate System-to-Intermediate System (IS-IS) to advertise only prefixes that belong to passive interfaces, use the **advertise-passive-only** command in router configuration mode. To remove the restriction, use the **no** form of this command.

advertise-passive-only

no advertise-passive-only

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior.

Command Modes

Router configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is an IS-IS mechanism to exclude IP prefixes of connected networks from link-state packet (LSP) advertisements, thereby reducing IS-IS convergence time.

Configuring this command per IS-IS instance is a scalable solution to reduce IS-IS convergence time because fewer prefixes will be advertised in the router nonpseudonode LSP.

This command relies on the fact that when enabling IS-IS on a loopback interface, you usually configure the loopback as passive (to prevent sending unnecessary hello packets out through it because there is no chance of finding a neighbor behind it). Thus, if you want to advertise only the loopback and if it has already been configured as passive, configuring the **advertise-passive-only** command per IS-IS instance would prevent the overpopulation of the routing tables.

An alternative to this command is the **no isis advertise-prefix** command. The **no isis advertise-prefix** command is a small-scale solution because it is configured per interface.

Examples

The following example uses the **advertise-passive-only** command, which affects the IS-IS instance, and thereby prevents advertising the IP network of Ethernet interface 0. Only the IP address of loopback interface 0 is advertised.

```
!
interface loopback 0
 ip address 192.168.10.1 255.255.255.255
 no ip directed-broadcast
!
!
interface Ethernet0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast
 ip router isis
!.
!.
!.
!
router isis
 passive-interface Loopback0
 net 47.0004.004d.0001.0001.0c11.1111.00
 advertise-passive-only
 log-adjacency-changes
!
```

Related Commands

Command	Description
isis advertise-prefix	Allows the advertising of IP prefixes of connected networks in LSP advertisements per IS-IS interface.
passive-interface	Suppresses the sending of routing updates through the specified interface.

area-password

To configure the Intermediate System-to-Intermediate System (IS-IS) area authentication password, use the **area-password** command in router configuration mode. To disable the password, use the **no** form of this command.

area-password *password* [**authenticate snp** {**validate** | **send-only**}]

no area-password [*password*]

Syntax Description

password	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into sequence number PDUs (SNPs).
validate	Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Defaults

No area password is defined, and area password authentication is disabled.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **authenticate snp**, **validate**, and **send-only** keywords were added.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **area-password** command on all routers in an area will prevent unauthorized routers from injecting false routing information into the link-state database.

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 1 (station router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an area authentication password and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
router isis
 area-password track authenticate snp validate
```

Related Commands

Command	Description
domain-password	Configures the IS-IS routing domain authentication password.
isis password	Configures the authentication password for an interface.

authentication key-chain

To enable authentication for Intermediate System-to-Intermediate System (IS-IS), use the **authentication key-chain** command in router configuration mode. To disable such authentication, use the **no** form of this command.

authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Syntax Description

name-of-chain	Enables authentication and specifies the group of keys that are valid.
level-1	(Optional) Enables authentication for Level 1 packets only.
level-2	(Optional) Enables authentication for Level 2 packets only.

Defaults

No key chain authentication is provided for IS-IS packets at the router level.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no key chain is configured with the **key chain** command, no key chain authentication is performed.

Key chain authentication could apply to clear text authentication or MD5 authentication. The mode is determined by the **authentication mode command**.

Only one authentication key chain is applied to IS-IS at one time. That is, if you configure a second **authentication key-chain** command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the chain applies to both levels.

You can specify authentication for an individual IS-IS interface by using the **isis authentication key-chain** command.

Examples

The following example configures IS-IS to accept and send any key belonging to the key chain named site1:

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain site1 level-1
```

Related Commands

Command	Description
authentication mode	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
isis authentication key-chain	Enables authentication for an IS-IS interface.
key chain	Enables authentication for routing protocols.

authentication mode

To specify the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets for the IS-IS instance, use the **authentication mode** command in router configuration mode. To restore clear text authentication, use the **no** form of this command.

authentication mode {**md5** | **text**} [**level-1** | **level-2**]

no authentication mode

Syntax Description

md5	Message Digest 5 (MD5) authentication.
text	Clear text authentication.
level-1	(Optional) Enables the specified authentication for Level 1 packets only.
level-2	(Optional) Enables the specified authentication for Level 2 packets only.

Defaults

No authentication is provided for IS-IS packets at the router level by use of this command, although clear text (plain text) authentication could be configured by other means, such as the **area-password** command or the **domain-password** command.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

You can specify the type of authentication and the level to which it applies for a single IS-IS interface, rather than per IS-IS instance, by using the **isis authentication mode** command.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the **authentication mode** command overrides both of those commands.

If you configure the **authentication mode** command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no authentication mode** command first.

Examples

The following example configures for the IS-IS instance that Message Digest 5 (MD5) authentication is performed on Level 1 packets:

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain site1 level-1
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
authentication key-chain	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
domain-password	Configures the IS-IS routing domain authentication password.
isis authentication mode	Specifies the type of authentication used for an Intermediate System-to-Intermediate System (IS-IS) interface.
key chain	Enables authentication for routing protocols.

authentication send-only

To specify for the Intermediate System-to-Intermediate System (IS-IS) instance that authentication is performed only on IS-IS packets being sent (not received), use the **authentication send-only** command in router configuration mode. To configure for the IS-IS instance that if authentication is configured at the router level, such authentication be performed on packets being sent and received, use the **no** form of this command.

authentication send-only [**level-1** | **level-2**]

no authentication send-only

Syntax Description

level-1	(Optional) Authentication is performed only on Level 1 packets that are being sent (not received).
level-2	(Optional) Authentication is performed only on Level 2 packets that are being sent (not received).

Defaults

If authentication is configured at the router level, it applies to IS-IS packets being sent and received.

Command Modes

Router configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no** **authentication send-only** command to disable the send-only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send-only feature applies to both levels.

This command could apply to clear text authentication or Message Digest 5 (MD5) authentication. The mode is determined by the **authentication mode** command.

Examples

The following example configures IS-IS Level 1 packets to use clear text authentication on packets being sent (not received):

```
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication send-only level-1
 authentication mode text level-1
 authentication key-chain site1 level-1
```

Related Commands

Command	Description
authentication key-chain	Enables authentication for Intermediate System-to-Intermediate System (IS-IS) packets and specifies the set of keys that can be used on an interface.
authentication mode	Specifies the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets for the IS-IS instance.
key chain	Enables authentication for routing protocols.

clear isis lsp-full

To clear the LSPFULL state, use the **clear isis lsp-full** command in privileged EXEC mode.

clear isis lsp-full

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the link-state PDU (LSP) becomes full because too many routes are redistributed, use the **clear isis lsp-full** command to clear the state after the problem has been resolved.

Examples

This example clears the LSPFULL state:

```
Router# clear isis lsp-full
```

Related Commands

Command	Description
lsp-full suppress	Controls which routes are suppressed when the link-state PDU becomes full.

clear isis rib redistribution

To clear some or all prefixes in the Intermediate System-to-Intermediate System (IS-IS) redistribution cache, use the **clear isis rib redistribution** command in privileged EXEC mode.

clear isis rib redistribution [**level-1** | **level-2**] [*network-prefix*] [*network-mask*]

Syntax Description

level-1	(Optional) Clears Level 1 IS-IS redistributed prefixes from the redistribution cache.
level-2	(Optional) Clears Level 2 IS-IS redistributed prefixes from the redistribution cache.
network-prefix	(Optional) The network ID in the A.B.C.D format for the specific network prefix you want to clear from the redistribution Routing Information Base (RIB). If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.
network-mask	(Optional) The network ID in the A.B.C.D format for the network mask for the specific network prefix you want to clear from the RIB. If you do not provide a network mask for the prefix, the major net of the prefix will be used for the network mask.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

We recommend that you use this command in a troubleshooting situation only when a Cisco Technical Assistance Center representative requests you to do so following a software error.

Examples

The following example clears the network prefix 10.1.0.0 from the IP local redistribution cache:

```
Router# clear isis rib redistribution 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
debug isis rib redistribution	Debugs the local redistribution cache event.
show isis rib redistribution	Displays the prefixes in the IS-IS redistribution cache.

default-information originate (IS-IS)

To generate a default route into an Intermediate System-to-Intermediate System (IS-IS) routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]

no default-information originate [**route-map** *map-name*]

Syntax Description

route-map *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a router configured with this command has a route to 0.0.0.0 in the routing table, IS-IS will originate an advertisement for 0.0.0.0 in its link-state packets (LSPs).

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.
- Advertise 0/0 conditionally.

With a **match ip address** *standard-access-list* command, you can specify one or more IP routes that must exist before the router will advertise 0/0.

Examples

The following example forces the software to generate a default external route into an IS-IS domain:

```
router isis
! BGP routes will be distributed into IS-IS
redistribute bgp 120
```

```
! access list 2 is applied to outgoing routing updates
distribute-list 2 out
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show isis database	Displays the Intermediate System-to-Intermediate System (IS-IS) link-state database.

domain-password

To configure the Intermediate System-to-Intermediate System (IS-IS) routing domain authentication password, use the **domain-password** command in router configuration mode. To disable a password, use the **no** form of this command.

domain-password *password* [**authenticate snp** {**validate** | **send-only**}]

no domain-password [*password*]

Syntax Description

password	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into SNP protocol data units (PDUs).
validate	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	(Optional) Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Defaults

No domain password is specified and no authentication is enabled for exchange of Level 2 routing information.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **authenticate snp**, **validate**, and **send-only** keywords were added.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 2 (area router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an authentication password to the routing domain and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
router isis
 domain-password users2j45 authenticate snp validate
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
isis password	Configures the authentication password for an interface.

fast-flood

To fill Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs), use the **fast-flood** command in router configuration mode. To disable the fast flooding, use the **no** form of this command.

fast-flood [*lsp-number*]

no fast-flood [*lsp-number*]

Syntax Description

lsp-number	(Optional) The number of LSPs from 1 to 15 to be flooded before shortest path first (SPF) is started. The default is 5 LSPs.

Command Default

Fast flooding is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T. This command replaces the **ip fast-convergence** command.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The **fast-flood** command sends a specified number of LSPs from the router. If no LSP number value is specified, the default it 5. The LSPs invoke SPF before running SPF. When you speed up the LSP flooding process, you improve overall network convergence time.

If you are running SPF and if you have configured values shorter than 40 milliseconds for the initial delay that is set by the *seconds* argument of the **incremental-spf** command, the SPF computation might start before the LSP that triggered SPF is flooded to neighbors. The router should always flood, at least, the LSP that triggered SPF before the router runs the SPF computation.

We recommend that you enable the fast flooding of LSPs before the router runs the SPF computation, in order to achieve a faster convergence time.

Note Beginning with Cisco IOS Release 12.3(7)T, the **ip fast-convergence** command is replaced with the **fast-flood** command.

Examples

In the following example, the **fast-flood** command is entered to configure the router to fill the first seven LSPs that invoke SPF, before the SPF computation is started. When the **show running-configuration** command is entered, the output confirms that fast flooding has been enabled on the router.

```
Router# clear isis rib redistribution 10.1.0.0 255.255.0.0
Router> enable
Router# configure terminal
Router(config)# router isis first
Router(config-router)# fast-flood 7
Router(config-router)# end
Router# show running-config

fast-flood 7
```

Related Commands

Command	Description
incremental-spf	Enables incremental SPF.

fast-reroute load-sharing disable

To disable Fast Reroute (FRR) load sharing of prefixes, use the **fast-reroute load-sharing disable** command in router configuration mode. To restore the default setting, use the **no** form of this command.

fast-reroute load-sharing {**level-1** | **level-2**} **disable**

no fast-reroute load-sharing {**level-1** | **level-2**} **disable**

Syntax Description

level-1	Specifies Level 1 packets.
level-2	Specifies Level 2 packets.

Command Default

Load sharing of prefixes is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

You must configure the **router isis** command before you can configure the **fast-reroute load-sharing disable** command.

Load sharing equally distributes the prefixes that use the same protected primary path over the available loop-free alternates (LFAs). An LFA is a next hop that helps a packet reach its destination without looping back.

Examples

The following example shows how to disable load sharing of Level 2 prefixes:

```
Router(config)# router isis
Router(router-config)# fast-reroute load-sharing level-2 disable
Router(router-config)# end
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

fast-reroute per-prefix

To enable Fast Reroute (FRR) per prefix, use the **fast-reroute per-prefix** command in router configuration mode. To disable the configuration, use the **no** form of this command.

fast-reroute per-prefix {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*}

no fast-reroute per-prefix {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*}

Syntax Description

level-1	Enables per-prefix FRR of Level 1 packets.
level-2	Enables per-prefix FRR of Level 2 packets.
all	Enables FRR of all primary paths.
route-map	Specifies the route map for selecting primary paths for protection.
route-map-name	Route map name.

Command Default

Fast Reroute per prefix is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

You must configure the **router isis** command before you can configure the **fast-reroute per-prefix** command.

You must configure the **all** keyword to protect all prefixes or configure the **route-map** *route-map-name* keyword and argument pair to protect a selected set of prefixes. When you specify the **all** keyword, all paths are protected, except paths that use interfaces, which are not supported, or interfaces, which are not enabled for protection. Using the **route-map** *route-map-name* keyword and argument pair to specify protected routes provides you with the flexibility to select protected routes, including using administrative tags.

Repair paths forward traffic during a routing transition. Repair paths are precomputed in anticipation of failures so that they can be activated when a failure is detected.

Examples

The following example shows how to enable FRR for all Level 2 prefixes:

```
Router(config)# router isis
Router(router-config)# fast-reroute per-prefix level-2 all
Router(router-config)# end
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

fast-reroute tie-break

To configure the Fast Reroute (FRR) tiebreaking priority, use the **fast-reroute tie-break** command in router configuration mode. To disable the configuration, use the **no** form of this command.

fast-reroute tie-break {**level-1** | **level-2**} {**downstream** | **linecard-disjoint** | **lowest-backup-path-metric** | **node-protecting** | **primary-path** | **secondary-path** | **srlg-disjoint**} *priority-number*

no fast-reroute tie-break {**level-1** | **level-2**} {**downstream** | **linecard-disjoint** | **lowest-backup-path-metric** | **node-protecting** | **primary-path** | **secondary-path** | **srlg-disjoint**}

Syntax Description

level-1	Configures tiebreaking for Level 1 packets.
level-2	Configures tiebreaking for Level 2 packets.
downstream	Configures loop-free alternates (LFAs) whose metric to the protected destination is lower than the metric of the protecting node to the destination.
linecard-disjoint	Configures LFAs that use interfaces that do not exist on the line card of the interface used by the primary path. The default is 40.
lowest-backup-path-metric	Configures LFAs with the lowest metric to the protected destination. The default is 30.
node-protecting	Configures LFAs that protect the primary next hop. The default is 50.
primary-path	Configures the repair path from the Equal Cost Multipath (ECMP) set. The default is 20.
secondary-path	Configures the non-ECMP repair path.
srlg-disjoint	Configures LFAs that do not share the same Shared Risk Link Group (SRLG) ID as the primary path. The default is 10.
priority-number	Priority number. Valid values are from 1 to 255.

Command Default

Tiebreaking is enabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.

Usage Guidelines

You must configure the **router isis** command before you can configure the **fast-reroute tie-break** command.

Tiebreaking configurations are applied per IS-IS instance per address family. The lower the configured priority value, the higher the priority of the rule. The same attribute cannot be configured more than once in the same address family.

The default tiebreaking rules have a priority value of 256. Hence, the tiebreaking rules that you configure will always have a higher priority than the default rule.

Load sharing equally distributes the prefixes that use the same protected primary path over the available LFAs. An LFA is a next hop that helps a packet reach its destination without looping back.

Examples

The following example shows how to set a tiebreaking priority of 5 for Level 2 packets:

```
Router(config)# router isis
Router(router-config)# fast-reroute load-sharing level-2 all
Router(router-config)# end
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

hello padding

To reenable IS-IS hello padding at the router level, enter the **hello padding** command in router configuration mode. To disable IS-IS hello padding, use the **no** form of this command.

hello padding

no hello padding

Syntax Description

This command has no arguments or keywords.

Defaults

IS-IS hello padding is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding in order to avoid wasting network bandwidth in case the MTU of both interfaces is the same or, in case of translational bridging. While hello padding is disabled, Cisco routers still send the first five IS-IS hellos padded to the full MTU size, in order to maintain the benefits of discovering MTU mismatches.

To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the **no hello padding** command in router configuration mode. To selectively disable hello padding for a specific interface, enter the **no isis hello padding** command in interface configuration mode.

Examples

In the following example the **no hello padding** command is used to turn off hello padding at the router level:

```
Router(config)# router isis
Router(config-router)# no hello padding
Router(config-router)# end
```

The **show clns interfaces** command is entered to show that hello padding has been turned off at router level:

```
Router# show clns interface e0/0

Ethernet0/0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 4 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: Router_B.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: Router_B.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 6 seconds
!   No hello padding
    Next IS-IS LAN Level-2 Hello in 2 seconds
!   No hello padding
```

When the **debug isis adj packets** command is entered, the output will show the IS-IS hello protocol data unit (PDU) length when a hello packet has been sent to or received from an IS-IS adjacency. In the following example the IS-IS hello PDU length is 1497:

```
Router# debug isis adj packets e0/0

IS-IS Adjacency related packets debugging is on
Router_A#
*Oct 11 18:04:17.455: ISIS-Adj: Sending L1 LAN IIH on Ethernet0/0, length 55
*Oct 11 18:04:19.075: ISIS-Adj: Rec L2 IIH from aabb.cc00.6600 (Ethernet0/0), cir type
L1L2, cir id 0000.0000.000B.01, length 1497
```

Related Commands

Command	Description
debug isis adj packets	Displays information on all adjacency-related activity such as hello packets sent and received and IS-IS adjacencies going up and down.
isis hello padding	Reenables IS-IS hello padding at the interface level.
show clns interface	Lists the CLNS-specific information about each interface.

hostname dynamic

To enable IS-IS dynamic hostname capability on the router, use the **hostname dynamic** command in router configuration mode. To disable the dynamic hostname feature, use the **no** form of this command.

hostname dynamic

no hostname dynamic

Syntax Description

This command has no arguments or keywords.

Command Default

The dynamic hostname feature is enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.
12.0S	This command was integrated into Cisco IOS Release 12.0(S).

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname** command displays the entries in the system-ID-to-router-name mapping table.

The dynamic hostname mechanism uses link-state protocol (LSP) flooding to distribute the router-name-to-system-ID mapping information across the entire network. Every router on the network will try to install the system ID-to-router name mapping information in its routing table.

If a router that has been advertising the dynamic name type, length, value (TLV) on the network suddenly stops the advertisement, the mapping information last received will remain in the dynamic host mapping table for up to one hour, allowing the network administrator to display the entries in the mapping table during a time when the network experiences problems. Entering the **show isis hostname** command displays the entries in the mapping table.

Note Locally defined mappings are always preferred over dynamically learned mappings. If you have already configured the **clns host** command to overwrite network advertised name mappings from LSPs, the **clns host** command will take precedence over the dynamic hostname feature.

Examples

The following example changes the hostname from Router to RouterA and assigns the NET 49.0001.0000.0000.000b.00 to RouterA. The dynamic hostname feature is disabled by entering the **no hostname dynamic** command. The dynamic hostname feature is then reeanabled by entering the **hostname dynamic** command.

```
Router> enable
Router# configure terminal
Router(config)# hostname RouterA
RouterA(config)# router isis CompanyA
RouterA(config-router)# net 49.0001.0000.0000.000b.00
RouterA(config-router)# hostname dynamic
RouterA(config-router)# end
```

Entering the **show isis hostname** command displays the dynamic host mapping table. The * symbol signifies that this is the hostname for the local router. The dynamic host mapping table confirms that system ID 0000.0000.000B belongs to a router with the dynamic hostname RouterA. This router is running the IS-IS process named CompanyA.

```
Router# show isis hostname

Level  System ID      Dynamic Hostname    (CompanyA)
     * 0000.0000.000B RouterA
```

Related Commands

Command	Description
clns host	Defines a name-to-NSAP mapping that can then be used with commands that require NSAPs.
hostname	Specifies or modifies the hostname for the network server.
net	Configures an IS-IS NET for a CLNS or IS-IS routing process.
show isis hostname	Displays the entries of the dynamic host mapping table.

ip fast-convergence

To reduce packet loss when the metric of a path is changed, or to fast-flood Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs), use the **ip fast-convergence** command in router configuration mode. To disable packet loss reduction or fast-flooding, use the **no** version of this command.

ip fast-convergence

no ip fast-convergence

Note Effective with Release 12.3(7)T, the **ip fast-convergence** command is replaced by the **fast-flood** command. See the **fast-flood** command for more information.

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(8)T	This command was introduced to reduce packet loss.
12.2(10)T	This command was modified to enable fast-flooding.
12.3(7)T	This command was replaced by the **fast-flood** command.

Usage Guidelines

To reduce packet loss when the metric of a path is changed, use the **ip fast-convergence** command. Entering the **ip fast-convergence** command is especially helpful when Multiprotocol Label Switching (MPLS) traffic engineering with Fast Reroute (FRR) is deployed.

If you are running Cisco IOS Release 12.2(11)T or a later release, you can enter the **ip fast-convergence** command to configure the router to flood the first five LSPs that invoke shortest path first (SPF) before running SPF. When you speed up the LSP flooding process, you improve overall network convergence time. We recommend that you enable the fast-flooding of LSPs before the router runs the SPF computation, in order to achieve a faster convergence time.

Examples

In the following example, the **ip fast-convergence** command is entered to configure the router to flood the first five LSPs that invoke SPF, before the SPF computation is started. When the **show running-configuration** command is entered, the output confirms that fast-flooding has been enabled on the router.

```
Router> enable
Router# configure terminal
Router(config)# router isis
```

```
Router(config-router)# ip fast-convergence
Router(config-router)# end
Router# show running-config

fast-flood
```

Related Commands

Command	Description
incremental-spf	Enables incremental SPF.

ip route priority high

To assign a high priority to an Integrated Intermediate System-to-Intermediate System (IS-IS) IP prefix, use the **ip route priority high** command in router configuration mode. To remove the IP prefix priority, use the **no** form of this command.

ip route priority high tag *tag-value*

no ip route priority high tag *tag-value*

Syntax Description

tag *tag-value*	Assigns a high priority to IS-IS IP prefixes with a specific route tag in a range from 1 to 4294967295.

Defaults

No IP prefix priority is set.

Command Modes

Router configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you use the **ip route priority high** command to tag higher priority IS-IS IP prefixes for faster processing and installation in the global routing table, you can achieve faster convergence. For example, you can help Voice over IP (VoIP) gateway addresses get processed first to help VoIP traffic get updated faster than other types of packets.

Examples

The following example uses the **ip route priority high** command to assign a tag value of 100 to the IS-IS IP prefix:

```
Router> enable
Router# configure terminal
Router(config)# interface Ethernet 0
Router(config-if)# ip router isis
Router(config-if)# isis tag 100
!
Router(config)# router isis
Router(config-router)# ip route priority high tag 100
!
```

Related Commands

Command	Description
debug isis rib	Displays debug information for IP Version 4 routes within the global or IS-IS local RIB.
show isis rib	Displays paths for routes in the IP Version 4 IS-IS local RIB.

ip router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IP on an interface and to attach an area designator to the routing process, use the **ip router isis** command in interface configuration mode. To disable IS-IS for IP, use the **no** form of the command.

ip router isis *area-tag*

no ip router isis *area-tag*

Syntax Description

area-tag	Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. **Note** Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area.

Defaults

No routing processes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Multiarea functionality was added, changing the way the *tag* argument (now *area-tag*) is used.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	Support for IPv6 was added.

Usage Guidelines

Before the IS-IS routing process is useful, a network entity title (NET) must be assigned with the **net** command and some interfaces must have IS-IS enabled.

If you have IS-IS running and at least one International Organization for Standardization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one process to perform Level 2 (interarea) routing. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform intra-area (Level 1) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. Use the **is-type** command to remove Level 2 routing from a router instance. You can then use the **is-type** command to enable Level 2 routing on some other IS-IS router instance.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

Examples

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows an IS-IS configuration with two Level 1 areas and one Level 1-2 area:

```
ip routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02


.
.
.

! Defaults to "is-type level-1-2"
router isis BB
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

Related Commands

Command	Description
is-type	Configures the routing level for an IS-IS routing process.
net	Configures an IS-IS NET for a CLNS routing process.
router isis	Enables the IS-IS routing protocol.

isis advertise-prefix

To allow the advertising of IP prefixes of connected networks in link-state packet (LSP) advertisements per Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis advertise-prefix** command in interface configuration mode. To prevent IP prefixes of connected networks from being advertised, use the **no** form of this command.

isis advertise-prefix

no isis advertise-prefix

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled; IP prefixes are advertised.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **no isis advertise-prefix** command is an IS-IS mechanism to exclude IP prefixes of connected networks from LSP advertisements, thereby reducing IS-IS convergence time.

Configuring the **no** form of this command per IS-IS interface is a small-scale solution to reduce IS-IS convergence time because fewer prefixes will be advertised in the router nonpseudonode LSP.

An alternative the **isis advertise-prefix** command is the **advertise-passive-only** command. The latter command is a scalable solution because it is configured per IS-IS instance.

Examples

The following example uses the **no isis advertise-prefix** command on Ethernet interface 0. Only the IP address of loopback interface 0 is advertised.

```
!
interface loopback 0
 ip address 192.168.10.1 255.255.255.255
 no ip directed-broadcast
!
```

```
interface Ethernet 0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast
 ip router isis
 no isis advertise-prefix
!
.
.
.
!
router isis
 passive-interface loopback 0
 net 47.0004.004d.0001.0001.0c11.1111.00
 log-adjacency-changes
!
```

Related Commands

Command	Description
advertise-passive-only	Configures the IS-IS instance to advertise only prefixes that belong to passive interfaces.

isis authentication key-chain

To enable authentication for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis authentication key-chain** command in interface configuration mode. To disable such authentication, use the **no** form of this command.

isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

no isis authentication key-chain *name-of-chain* [**level-1** | **level-2**]

Syntax Description

name-of-chain	Enables authentication and specifies the group of keys that are valid.
level-1	(Optional) Enables authentication for Level 1 packets only.
level-2	(Optional) Enables authentication for Level 2 packets only.

Defaults

No key chain authentication is configured for a specific IS-IS interface, although it might be configured at the IS-IS instance level.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no key chain is configured with the **key chain** command, no key chain authentication is performed.

Only one authentication key chain is applied to an IS-IS interface at one time. That is, if you configure a second **isis authentication key-chain** command, the first is overridden.

If neither the **level-1** nor **level-2** keyword is configured, the chain applies to both levels.

You can specify authentication for an entire instance of IS-IS instead of at the interface level by using the **authentication key-chain** command.

Examples

The following example configures Ethernet interface 0 to accept and send any key belonging to the key chain named second:

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.252
```

```
ip router isis real_secure_network
isis authentication mode md5 level-1
isis authentication key-chain second level-1
```

Related Commands

Command	Description
authentication key-chain	Enables authentication for IS-IS at the instance level.
key chain	Enables authentication for routing protocols.

isis authentication mode

To specify the type of authentication used for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis authentication mode** command in interface configuration mode. To restore clear text authentication, use the **no** form of this command.

isis authentication mode {**md5** | **text**} [**level-1** | **level-2**]

no isis authentication mode

Syntax Description

md5	Message Digest 5 (MD5) authentication.
text	Clear text authentication.
level-1	(Optional) Enables the specified authentication on the interface for Level 1 packets only.
level-2	(Optional) Enables the specified authentication on the interface for Level 2 packets only.

Defaults

No authentication is provided for IS-IS packets on an interface level, although authentication could be provided at the IS-IS instance level by several means.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If neither the **level-1** nor **level-2** keyword is configured, the mode applies to both levels.

If you had clear text authentication configured by using the **area-password** or **domain-password** command, the **authentication mode** command overrides both of those commands.

If you configure the **isis authentication mode** command and subsequently try to configure the **area-password** or **domain-password** command, you will not be allowed to do so. If you truly want to configure clear text authentication using the **area-password** or **domain-password** command, you must use the **no isis authentication mode** command first.

You can specify the type of authentication and the level to which it applies for the entire IS-IS instance, rather than per interface, by using the **authentication mode** command.

Examples

The following example configures IS-IS Level 2 packets to use MD5 authentication on Ethernet interface 0:

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication mode md5 level-2
 isis authentication key-chain cisco level-2
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
authentication mode	Specifies the type of authentication used in IS-IS packets for the IS-IS instance.
domain-password	Configures the IS-IS routing domain authentication password.
key chain	Enables authentication for routing protocols.

isis authentication send-only

To specify that authentication is performed only on packets being sent (not received) on a specified Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis authentication send-only** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis authentication send-only [**level-1** | **level-2**]

no **isis authentication send-only**

Syntax Description

level-1	(Optional) Authentication is performed only on Level 1 packets that are being sent (not received).
level-2	(Optional) Authentication is performed only on Level 2 packets that are being sent (not received).

Defaults

If MD5 authentication is configured at the interface level, it applies to IS-IS packets being sent and received over all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command before configuring the authentication mode and authentication key chain so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all of the routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then specify the **no isis authentication send-only** command to disable the send-only feature.

If neither the **level-1** nor **level-2** keyword is configured, the send-only feature applies to both levels.

Examples

The following example configures IS-IS Level-1 packets to use MD5 authentication on packets being sent (not received) on Ethernet interface 0:

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
```

```
isis authentication send-only level-1
isis authentication mode md5 level-1
isis authentication key-chain cisco level-1
```

Related Commands

Command	Description
isis authentication key-chain	Enables authentication for IS-IS packets and specifies the set of keys that can be used on an interface.
isis authentication mode	Specifies the type of authentication used in IS-IS packets for the interface.
key chain	Enables authentication for routing protocols.

isis bfd

To enable or disable Bidirectional Forwarding Detection (BFD) on a specific interface configured for Intermediate System-to-Intermediate System (IS-IS), use the **isis bfd** command in interface configuration mode. To disable BFD on the IS-IS interface, use the **disable** keyword. To remove the **isis bfd** command, use the **no** form of this command.

isis bfd [**disable**]

no isis bfd

Syntax Description

disable	(Optional) Disables BFD for IS-IS on a specified interface.

Defaults

When the **disable** keyword is not used, the default behavior is to enable BFD support for IS-IS on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Enter the **isis bfd** command in interface mode to configure an IS-IS interface to use BFD for failure detection. If you have used the **bfd-all interfaces** command in router configuration mode to globally configure all IS-IS interfaces for an IS-IS process to use BFD, you can enter the **isis bfd** command with the **disable** keyword in interface configuration mode to disable BFD for a specific IS-IS interface.

Entering the **no isis bfd** command will remove the command. In that case, whether or not an IS-IS interface for a particular IS-IS process is registered with the BFD protocol will depend on whether or not you have entered the **bfd all-interfaces** command in router configuration mode for the specific IS-IS process.

Examples

In the following example, the interface associated with OSPF, Fast Ethernet interface 3/0, is configured for BFD:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 3/0
Router(config-if)# isis bfd
Router(config-if)# end
```

Related Commands

Command	Description
bfd all-interfaces	Enables BFD for all interfaces for a BFD peer.

isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** command in interface configuration mode. To reset the circuit type to Level l and Level 2, use the **no** form of this command.

isis circuit-type [**level-1 | level-1-2 | level-2-only**]

no isis circuit-type

Syntax Description

level-1	(Optional) Configures a router for Level 1 adjacency only.
level-1-2	(Optional) Configures a router for Level 1 and Level 2 adjacency.
level-2-only	(Optional) Configures a router for Level 2 adjacency only.

Defaults

A Level 1 and Level 2 adjacency is established.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Normally, this command need not be configured. The proper way is to configure a router as a Level 1-only, Level 1-2, or Level 2-only system. Only on routers that are between areas (Level 1-2 routers) should you configure some interfaces to be Level 2-only to prevent wasting bandwidth by sending out unused Level 1 hello packets. Note that on point-to-point interfaces, the Level 1 and Level 2 hellos are in the same packet.

A Level 1 adjacency may be established if there is at least one area address in common between this system and its neighbors. Level 2 adjacencies will never be established over this interface.

A Level 1 and Level 2 adjacency is established if the neighbor is also configured as **level-1-2** and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.

Level 2 adjacencies are established if the other routers are Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies will never be established over this interface.

Examples

In the following example, other routers on Ethernet interface 0 are in the same area. Other routers on Ethernet interface 1 are in other areas, so the router will stop sending Level 1 hellos.

```
interface ethernet 0
ip router isis
interface ethernet 1
 isis circuit-type level-2-only
```

isis csnp-interval

To configure the Intermediate System-to-Intermediate System (IS-IS) complete sequence number PDUs (CSNPs) interval, use the **isis csnp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis csnp-interval *seconds* [**level-1** | **level-2**]

no isis csnp-interval [**level-1** | **level-2**]

Syntax Description

seconds	Interval of time between transmission of CSNPs on multiaccess networks. This interval only applies for the designated router. The default is 10 seconds. The range is from 0 to 65535.
level-1	(Optional) Configures the interval of time between transmission of CSNPs for Level 1 independently.
level-2	(Optional) Configures the interval of time between transmission of CSNPs for Level 2 independently.

Defaults

10 seconds
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

It is very unlikely you will need to change the default value of this command.

This command applies only for the designated router (DR) for a specified interface. Only DRs send CSNP packets in order to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2. Configuring the CSNP interval does not apply to serial point-to-point interfaces. It does apply to WAN connections if the WAN is viewed as a multiaccess meshed network.

For multiaccess WAN interfaces such as ATM, Frame Relay, and X.25, we highly recommend that you configure the nonbroadcast multiaccess (NBMA) cloud as multiple point-to-point subinterfaces. Doing so will make routing much more robust if one or more permanent virtual circuits (PVCs) fails.

The **isis csnp-interval** command on point-to-point subinterfaces should be used only in combination with the IS-IS mesh-group feature.

Examples

The following example configures Ethernet interface 0 for sending CSNPs every 30 seconds:

```
interface ethernet 0
 isis csnp-interval 30 level-1
```

isis display delimiter

To make output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information, use the **isis display delimiter** command in global configuration mode. To disable this output format, use the **no** form of the command.

isis display delimiter [**return** *count* | *character count*]

no isis display delimiter [**return** *count* | *character count*]

Syntax Description

return	(Optional) Delimit with carriage returns.
count	(Optional) Number of carriage returns or length of string to use for the delimiter.
character	(Optional) Character to use for the delimiter string.

Defaults

The **isis display delimiter** command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to customize display output when the IS-IS multiarea feature is used. The **isis display delimiter** command displays the output from different areas as a string or additional white space.

Examples

The following command causes different areas in multiarea displays (such as **show** command output) to be delimited by a string of dashes (-):

```
isis display delimiter - 14
```

With three IS-IS neighbors configured, this command displays the following output from the **show clns neighbors** command:

```
Router# show clns neighbors

--------------
Area L2BB:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0009 Tu529       172.21.39.9     Up     25        L1L2 IS-IS
--------------
```

```
Area A3253-01:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0053 Et1         0060.3e58.ccdb  Up     22        L1   IS-IS
0000.0000.0003 Et1         0000.0c03.6944  Up     20        L1   IS-IS
--------------
Area A3253-02:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 Et2         0000.0c03.6bc5  Up     27        L1   IS-IS
0000.0000.0053 Et2         0060.3e58.ccde  Up     24        L1   IS-IS
```

Related Commands

Command	Description
show clns es-neighbors	Lists the ES neighbors that this router knows.
show clns is-neighbors	Displays IS-IS related information for IS-IS router adjacencies.
show clns neighbors	Displays both ES and IS neighbors.
show isis database	Displays the IS-IS link-state database.
show isis routes	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
show isis spf-log	Displays how often and why the router has run a full SPF calculation.
show isis topology	Displays a list of all connected routers in all areas.

isis hello padding

To reenable Intermediate System-to-Intermediate System (IS-IS) hello padding at the interface level, enter the **isis hello padding** command in interface configuration mode. To disable IS-IS hello padding, use the **no** form of this command.

isis hello padding

no isis hello padding

Syntax Description

This command has no arguments or keywords.

Defaults

IS-IS hello padding is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

You can disable hello padding in order to avoid wasting network bandwidth in case the MTU of both interfaces is the same or, in case of translational bridging. While hello padding is disabled, Cisco routers still send the first five IS-IS hellos padded to the full MTU size, in order to maintain the benefits of discovering MTU mismatches.

To selectively disable hello padding for a specific interface, enter the **no isis hello padding** command in interface configuration mode. To disable hello padding for all interfaces on a router for the IS-IS routing process, enter the **no hello padding** command in router configuration mode.

Examples

To turn off hello padding at the interface level for the Ethernet interface 0/0, enter the **no isis hello padding** command in interface configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface e0/0
```

```
Router(config-if)# no isis hello padding
Router(config-if)# end
```

When the **show clns neighbor** command is entered for Ethernet interface 0/0, the output confirms that hello padding has been turned off for both Level 1 and Level 2 circuit types:

```
Router# show clns interface e0/0

Ethernet0/0 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 47 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: Router_B.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: Router_B.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
!   No hello padding
    Next IS-IS LAN Level-2 Hello in 2 seconds
!   No hello padding
```

When the **debug isis adj packets** command is entered, the output will show the IS-IS hello protocol data unit (PDU) length when a hello packet has been sent to or received from an IS-IS adjacency. In the following example the IS-IS hello PDU length is 1497:

```
Router# debug isis adj packets e0/0

IS-IS Adjacency related packets debugging is on
Router#
*Oct 11 18:04:17.455: ISIS-Adj: Sending L1 LAN IIH on Ethernet0/0, length 55
*Oct 11 18:04:19.075: ISIS-Adj: Rec L2 IIH from aabb.cc00.6600 (Ethernet0/0), cir type
L1L2, cir id 0000.0000.000B.01, length 1497
```

Related Commands

Command	Description
hello padding	Reenables IS-IS hello padding at the router level.
debug isis adj packets	Displays information on all adjacency-related activity such as hello packets sent and received and IS-IS adjacencies going up and down.
show clns interface	Lists the CLNS-specific information about each interface.

isis hello-interval

To specify the length of time between hello packets that the Cisco IOS software sends, use the **isis hello-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis hello-interval {*seconds* | **minimal**} [**level-1** | **level-2**]

no isis hello-interval [**level-1** | **level-2**]

Syntax Description

seconds	Length of time between hello packets, in seconds. By default, a value three times the hello interval *seconds* is advertised as the hold time in the hello packets sent. (Change the multiplier of 3 by specifying the **isis hello-multiplier** command.) With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. The default is 10. The range is from 0 to 65535. **Note** On designated intermediate system (DIS) interfaces, only one third of the configured value is used. The full value of the configured hello intervals is used only by non-DIS interfaces.
minimal	Causes the system to compute the hello interval based on the hello multiplier (specified by the **isis hello-multiplier** command) so that the resulting hold time is 1 second.
level-1	(Optional) Configures the hello interval for Level 1 independently. Use this on X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay multiaccess networks.
level-2	(Optional) Configures the hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.

Command Default

The hello interval is 10 seconds for non-DIS interfaces, and 3.333 seconds for DIS interfaces. The hello interval is configured for both Level 1 and Level 2.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **minimal** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 packet 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 on LAN interfaces.

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.

It makes more sense to tune the hello interval and hello multiplier on point-to-point interfaces than on LAN interfaces.

Examples

The following example configures serial interface 0 to advertise hello packets every 5 seconds. The router is configured to act as a station router. This configuration will cause more traffic than the traffic generated by configuring a longer interval, but topological changes will be detected earlier.

```
interface serial 0
 isis hello-interval 5 level-1
```

Related Commands

Command	Description
isis hello-multiplier	Specifies the number of IS-IS hello packets that a neighbor must miss before the router should declare the adjacency as down.

isis hello-multiplier

To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the **isis hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis hello-multiplier *multiplier* [**level-1** | **level-2**]

no isis hello-multiplier [**level-1** | **level-2**]

Syntax Description

multiplier	Integer value from 3 to 1000. The advertised hold time in IS-IS hello packets will be set to the hello multiplier times the hello interval. Neighbors will declare an adjacency to this router down after not having received any IS-IS hello packets during the advertised hold time. The hold time (and thus the hello multiplier and the hello interval) can be set on a per-interface basis, and can be different between different routers in one area. Using a smaller hello multiplier will give fast convergence, but can result in more routing instability. Increment the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier lower than the default value of 3.
level-1	(Optional) Configures the hello multiplier independently for Level 1 adjacencies.
level-2	(Optional) Configures the hello multiplier independently for Level 2 adjacencies.

Defaults

multiplier: 3
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The “holding time” carried in an IS-IS hello packet determines how long a neighbor waits for another hello packet before declaring the neighbor to be down. This time determines how quickly a failed link or neighbor is detected so that routes can be recalculated.

Use the **isis hello-multiplier** command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval (**isis hello-interval** command) correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

On point-to-point links, there is only one hello for both Level 1 and Level 2, so different hello multipliers should be configured only for multiaccess networks such as Ethernet and FDDI. Separate Level 1 and Level 2 hello packets are also sent over nonbroadcast multiaccess (NBMA) networks in multipoint mode, such as X.25, Frame Relay, and ATM. However, we recommend that you run IS-IS over point-to-point subinterfaces over WAN NBMA media.

Examples

In the following example, the network administrator wants to increase network stability by making sure an adjacency will go down only when many (ten) hello packets are missed. The total time to detect link failure is 60 seconds. This configuration will ensure that the network remains stable, even when the link is fully congested.

```
interface serial 1
 ip router isis
 isis hello-interval 6 level-1
 isis hello-multiplier 10 level-1
```

Related Commands

Command	Description
isis hello-interval	Specifies the length of time between hello packets that the Cisco IOS software sends.

isis lsp-interval

To configure the time delay between successive Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) transmissions, use the **isis lsp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis lsp-interval *milliseconds*

no isis lsp-interval

Syntax Description

milliseconds	Time delay between successive LSPs (in milliseconds).

Defaults

The default time delay is 33 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In topologies with a large number of IS-IS neighbors and interfaces, a router may have difficulty with the CPU load imposed by LSP transmission and reception. This command allows the LSP transmission rate (and by implication the reception rate of other systems) to be reduced.

Examples

The following example causes the system to send LSPs every 100 milliseconds (10 packets per second) on serial interface 0:

```
interface serial 0
 isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Configures the time between retransmission of each LSP (IS-IS link-state PDU) over point-to-point links.

isis mesh-group

To optimize link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies, use the **isis mesh-group** command in interface configuration mode. To remove a subinterface from a mesh group, use the **no** form of this command.

isis mesh-group [*number* | **blocked**]

no isis mesh-group [*number* | **blocked**]

Syntax Description

number	(Optional) A number identifying the mesh group of which this interface is a member.
blocked	(Optional) Specifies that no LSP flooding will take place on this subinterface.

Defaults

The interface performs normal flooding.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LSPs that are first received on subinterfaces that are not part of a mesh group are flooded to all other subinterfaces in the usual way.

LSPs that are first received on subinterfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group. If the **blocked** keyword is configured on a subinterface, then a newly received LSP is not flooded out over that interface.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally, you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios no router will be logically disconnected from the rest of the network. In other words, blocking flooding on all links permits the best scaling performance, but there is no flooding. Permitting flooding on all links results in very poor scaling performance.

Examples

In the following example six interfaces are configured in three mesh groups. LSPs received are handled as follows:

- LSPs received first via ATM 1/0.1 are flooded to all interfaces except ATM 1/0.2 (which is part of the same mesh group) and ATM 1/2.1, which is blocked.
- LSPs received first via ATM 1/1.2 are flooded to all interfaces except ATM 1/1.1 (which is part of the same mesh group) and ATM 1/2.1, which is blocked.
- LSPs received first via ATM 1/2.1 are not ignored, but flooded as usual to all interfaces. LSPs received first via ATM 1/2.2 are flooded to all interfaces, except ATM 1/2.1, which is blocked.

```
interface atm 1/0.1
ip router isis
isis mesh-group 10

interface atm 1/0.2
ip router isis
isis mesh-group 10

interface atm 1/1.1
ip router isis
isis mesh-group 11

interface atm 1/1.2
ip router isis
isis mesh-group 11

interface atm 1/2.1
ip router isis
isis mesh-group blocked

interface atm 1/2.2
ip router isis
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

isis metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) metric, use the **isis metric** command in interface configuration or subinterface mode. To restore the default metric value, use the **no** form of this command.

isis metric {*metric-value* | **maximum**} [**level-1** | **level-2**]

no isis metric {*metric-value* | **maximum**} [**level-1** | **level-2**]

Syntax Description

metric-value	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 1to 16777214. The default value is 10.
maximum	Excludes a link or adjacency from the shortest path first (SPF) calculation.
level-1	(Optional) Specifies that this metric should be used only in the SPF calculation for Level 1 (intra-area) routing. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.
level-2	(Optional) Specifies that this metric should be used only in the SPF calculation for Level 2 (interarea) routing. If no optional keyword is specified, the metric is enabled on routing Level 1 and Level 2.

Command Default

The default metric value is set to 10.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **maximum** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(13)	The **maximum** keyword was made available under subinterface configuration mode.
12.4(13)T	The **maximum** keyword was made available under subinterface configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Specifying the **level-1** or **level-2** keyword resets the metric only for Level 1 or Level 2 routing, respectively.

We highly recommend that you configure metrics on all interfaces. If you do not do so, the IS-IS metrics are similar to hop-count metrics.

It is strongly recommended to use the **metric-style wide** command to configure IS-IS to use the new-style type, length, value (TLV) because TLVs that are used to advertise IPv4 information in link-state packets (LSPs) are defined to use only extended metrics. Cisco IOS software provides support of a 24-bit metric field, the so-called "wide metric." Using the new metric style, link metrics now have a maximum value of 16777214 with a total path metric of 4261412864.

Cisco IOS Release 12.4(13) and 12.4(13)T

Entering the **maximum** keyword will exclude the link from the SPF calculation. If a link is advertised with the maximum link metric, the link will not be considered during the normal SPF calculation. When the link is excluded from the SPF, it will not be advertised for calculating the normal SPF. An example would be a link that is available for traffic engineering, but not for hop-by-hop routing. If a link, such as one that is used for traffic engineering, should not be included in the SPF calculation, enter the **isis metric** command with the **maximum** keyword.

Note The **isis metric maximum** command applies only when the **metric-style wide** command has been entered. The **metric-style wide** command is used to configure IS-IS to use the new-style TLV because TLVs that are used to advertise IPv4 information in link-state packets (LSPs) are defined to use only extended metrics.

Examples

The following example configures serial interface 0 for a link-state metric cost of 15 for Level 1:

```
Router(config)# interface serial 0
Router(config-if)# isis metric 15 level-1
```

The following example sets the IS-IS metric for the link to maximum. SPF will ignore the link for both Level 1 and Level 2 routing because neither the **level-1** keyword nor the **level-2** keyword was entered.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# isis metric maximum
```

Cisco IOS Release 12.4(13) and 12.4(13)T

The following example configures the **isis metric maximum** command on Ethernet subinterface 1/1.9.

```
Router(config)# interface Ethernet 1/1.9
Router(config-subif)# isis metric maximum
```

Related Commands

Command	Description
metric-style wide	Configures a router running IS-IS so that it generates and accepts only new-style TLVs.

isis network point-to-point

To configure a network of only two networking devices that use broadcast media and the integrated Intermediate System-to-Intermediate System (IS-IS) routing protocol to function as a point-to-point link instead of a broadcast link, use the **isis network point-to-point** command in interface configuration mode. To disable the point-to-point usage, use the **no** form of this command.

isis network point-to-point

no isis network point-to-point

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command only on broadcast media in a network of only two networking devices. The command will cause the system to issue packets point-to-point rather than as broadcasts. Configure the command on both networking devices in the network.

Examples

The following example configures a Fast Ethernet interface to act as a point-to-point interface:

```
interface fastethernet 1/0
 isis network point-to-point
```

isis password

To configure the authentication password for an interface, use the **isis password** command in interface configuration mode. To disable authentication for Intermediate System-to-Intermediate System (IS-IS), use the **no** form of this command.

isis password *password* [**level-1** | **level-2**]

no isis password [**level-1** | **level-2**]

Syntax Description

password	Authentication password you assign for an interface.
level-1	(Optional) Configures the authentication password for Level 1 independently. For Level 1 routing, the router acts as a station router only.
level-2	(Optional) Configures the authentication password for Level 2 independently. For Level 2 routing, the router acts as an area router only.

Defaults

This command is disabled by default.

If no keyword is specified, the default is **level-1-2**.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables you to prevent unauthorized routers from forming adjacencies with this router, and thus protects the network from intruders.

The password is exchanged as plain text and thus provides only limited security.

Different passwords can be assigned for different routing levels using the **level-1** and **level-2** keywords.

Specifying the **level-1** or **level-2** keyword disables the password only for Level 1 or Level 2 routing, respectively.

Examples

The following example configures a password for Ethernet interface 0 at Level 1:

```
interface ethernet 0
 isis password analyst level-1
```

isis priority

To configure the priority of designated routers, use the **isis priority** command in interface configuration mode. To reset the default priority, use the **no** form of this command.

isis priority *number-value* [**level-1** | **level-2**]

no isis priority [**level-1** | **level-2**]

Syntax Description

number-value	Sets the priority of a router and is a number from 0 to 127. The default value is 64.
level-1	(Optional) Sets the priority for Level 1 independently.
level-2	(Optional) Sets the priority for Level 2 independently.

Defaults

Priority of 64
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Priorities can be configured for Level 1 and Level 2 independently. Specifying the **level-1** or **level-2** keyword resets priority only for Level 1 or Level 2 routing, respectively.

The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.

In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

Examples

The following example shows Level 1 routing given priority by setting the priority level to 80. This router is now more likely to become the DIS.

```
interface ethernet 0
 isis priority 80 level-1
```

isis protocol shutdown

To disable the Intermediate System-to-Intermediate System (IS-IS) protocol so that it cannot form adjacencies on a specified interface and place the IP address of the interface into the link-state packet (LSP) that is generated by the router, use the **isis protocol shutdown** command in interface configuration mode. To reenable the IS-IS protocol, use the **no** form of this command.

isis protocol shutdown

no isis protocol shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **isis protocol shutdown** command allows you to disable the IS-IS protocol for a specified interface without removing the configuration parameters. The IS-IS protocol will not form any adjacencies for the interface for which the **isis protocol shutdown** command has been configured, and the IP address of the interface will be put into the LSP that is generated by the router.

If you do not want IS-IS to form any adjacency on any interface and clear the IS-IS LSP database, you can enter the **protocol shutdown** command.

Examples

The following example disables the IS-IS protocol on Ethernet interface3/1:

```
Router(config)# interface Ethernet 3/1
Router(config-if)# isis protocol shutdown
```

Related Commands

Command	Description
protocol shutdown	Disables the IS-IS protocol so that it cannot form any adjacency on any interface and clears the IS-IS LSP database.

isis retransmit-interval

To configure the amount of time between retransmission of each Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) on a point-to-point link, use the **isis retransmit-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-interval *seconds*

no isis retransmit-interval *seconds*

Syntax Description

seconds	Time (in seconds) between retransmission of each LSP. It is an integer that should be greater than the expected round-trip delay between any two routers on the attached network. The default is 5 seconds. The range is from 0 to 65535.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The setting of the *seconds* argument should be conservative, or needless retransmission will result.

This command has no effect on LAN (multipoint) interfaces. On point-to-point links, the value can be increased to enhance network stability.

Retransmissions occur only when LSPs are dropped. So setting the *seconds* argument to a higher value has little effect on reconvergence. The more neighbors routers have, and the more paths over which LSPs can be flooded, the higher this value can be made.

The value should be higher for serial lines.

Examples

The following example configures serial interface 0 for retransmission of IS-IS LSP, every 60 seconds for a large serial line:

```
interface serial 0
 isis retransmit-interval 60
```

Related Commands

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of any IS-IS LSPs on a point-to-point interface.

isis retransmit-throttle-interval

To configure the amount of time between retransmissions on each Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) on a point-to-point interface, use the **isis retransmit-throttle-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-throttle-interval *milliseconds*

no isis retransmit-throttle-interval

Syntax Description

milliseconds	Minimum delay (in milliseconds) between LSP retransmissions on the interface.

Defaults

The delay is determined by the **isis lsp-interval** command.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command may be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be re-sent on the interface.

The **isis retransmit-throttle-interval** command is distinct from the rate at which LSPs are sent on the interface (controlled by the **isis lsp-interval** command) and the period between retransmissions of a single LSP (controlled by the **isis retransmit-interval** command). These commands may all be used in combination to control the offered load of routing traffic from one router to its neighbors.

Examples

The following example configures serial interface 0 to limit the rate of LSP retransmissions to one every 300 milliseconds:

```
interface serial 0
 isis retransmit-throttle-interval 300
```

Related Commands

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSPs over a point-to-point link.

isis tag

To set a tag on the IP address configured for an interface when this IP prefix is put into an Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP), use the **isis tag** command in interface configuration mode. To stop tagging the IP address, use the **no** form of this command.

isis tag *tag-number*

no isis tag *tag-number*

Syntax Description

tag-number	Integer that serves as a tag on an IS-IS route.

Command Default

No route tag is associated for IP addresses configured for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

No action occurs on a tagged route until the tag is used, for example, to redistribute routes or summarize routes.

Configuring the **isis tag** command triggers the router to generate new LSPs because the tag is a new piece of information in the packet.

Examples

In this example, two interfaces are tagged with different tag values. By default, these two IP addresses would have been put into the IS-IS Level 1 and Level 2 database. However, if you use the **redistribute** command with a route map to match tag 110, only IP address 172.16. 0.0 is put into the Level 2 database.

```
interface ethernet 1/0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
 isis tag 120
interface ethernet 1/1
 ip address 172.16.0.0
 ip router isis
 isis tag 110
```

```
router isis
 net 49.0001.0001.0001.0001.00
 redistribute isis ip level-1 into level-2 route-map match-tag
 route-map match-tag permit 10
 match tag 110
```

ispf

To enable incremental shortest path first (SPF), use the **ispf** command in router configuration mode. To disable incremental SPF, use the **no** form of this command.

ispf {**level-1** | **level-2** | **level-1-2**} [*seconds*]

no ispf

Syntax Description

level-1	Enables incremental SPF for Level 1 packets only. The **level-1** keyword applies only when you have enabled Intermediate System-to-Intermediate System (IS-IS).
level-2	Enables incremental SPF for Level 2 packets only. The **level-2** keyword applies only when you have enabled IS-IS.
level-1-2	Enables incremental SPF for Level 1 and Level 2 packets. The **level-1-2** keyword applies only when you have enabled IS-IS.
seconds	(Optional) Number of seconds after configuring this command that incremental SPF is activated. Value can be in the range from 1 to 600. The default value is 120 seconds. The *seconds* argument applies only when you have enabled IS-IS.

Command Default

Incremental SPF is disabled.
seconds: 120

Command Modes

Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) use Dijkstra's SPF algorithm to compute the shortest path tree (SPT). During the computation of the SPT, the shortest path to each node is discovered. The topology tree is used to populate the routing table with routes to IP networks. When changes to a Type 1 or Type 2 link-state advertisement (LSA) occur in an area, the entire SPT is recomputed. In many cases, the entire SPT need not be recomputed because most of the tree remains unchanged. Incremental SPF allows the system to recompute only the affected part of the tree.

Recomputing only a portion of the tree rather than the entire tree results in faster OSPF convergence and saves CPU resources. Note that if the change to a Type 1 or Type 2 LSA occurs in the calculating router itself, then the full SPT is performed.

Incremental SPF computes only the steps needed to apply the changes in the network topology diagram. That process requires that the system keep more information about the topology in order to apply the incremental changes. Also, more processing must be done on each node for which the system receives a new link-state packet (LSP). However, incremental SPF typically reduces demand on CPU.

Incremental SPF is scheduled in the same way as the full SPF. Routers enabled with incremental SPF and routers not enabled with incremental SPF can function in the same internetwork.

Incremental SPF works only for IPv4.

Even if incremental SPF is configured, there are some cases where full SPF is executed; for example, periodic SPF, a calculation change for the routing calculation (such as a change in metric, is-type, and so on), the configuration of the **clear ip route** or **clear isis** commands, or adjacency changes.

Examples

The following example enables OSPF incremental SPF:

```
Router(config)# router ospf 1
Router(config-router)# ispf level-1
```

The following examples enables IS-IS incremental SPF for Level 1 and Level 2 packets:

```
Router(config)# router isis
Router(config-router)# ispf level-1-2
```

is-type

To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the **is-type** command in router configuration mode. To reset the default value, use the **no** form of this command.

is-type [**level-1** | **level-1-2** | **level-2-only**]

no is-type [**level-1** | **level-1-2** | **level-2-only**]

Syntax Description

level-1	(Optional) Router performs only Level 1 (intra-area) routing. This router learns only about destinations inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.
level-1-2	(Optional) Router performs both Level 1 and Level 2 routing. This router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
level-2-only	(Optional) Routing process acts as a Level 2 (interarea) router only. This router is part of the backbone, and does not communicate with Level 1-only routers in its own area.

Defaults

In conventional IS-IS configurations, the router acts as both a Level 1 (intra-area) and a Level 2 (interarea) router.

In multiarea IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and interarea) router. The remaining instances of the IS-IS process configured by default are Level 1 routers.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	This command was modified to include multiarea IS-IS routing.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

We highly recommend that you configure the type of IS-IS routing process. If you are configuring multiarea IS-IS, you *must* configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the **router isis** command is a Level 1-2 router.

If only one area is in the network, there is no need to run both Level 1 and Level 2 routing algorithms. If IS-IS is used for Connectionless Network Service (CLNS) routing (and there is only one area), Level 1 only must be used everywhere. If IS-IS is used for IP routing only (and there is only one area), you can run Level 2 only everywhere. Areas you add after the Level 1-2 area exists are by default Level 1 areas.

If the router instance has been configured for Level 1-2 (the default for the first instance of the IS-IS routing process in a Cisco device), you can remove Level 2 (interarea) routing for the area using the **is-type** command. You can also use the **is-type** command to configure Level 2 routing for an area, but it must be the only instance of the IS-IS routing process configured for Level 2 on the Cisco device.

Examples

The following example specifies an area router:

```
router isis
 is-type level-2-only
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.
show clns neighbor areas	Displays information about IS-IS neighbors and the areas to which they belong.