IP Routing: ISIS Configuration Guide, Cisco IOS Release 12.2SY

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Last Updated: July 19, 2011

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Integrated IS-IS Routing Protocol Overview

This module provides a technical overview of the Integrated Intermediate System-to-Intermediate System (IS-IS) routing protocol. IS-IS is a link-state Interior Gateway Protocol (IGP). Link-state protocols are characterized by the propagation of the information required to build a complete network connectivity map on each participating router. That map is then used to calculate the shortest path to destinations.

The IS-IS protocol was developed in the late 1980s by Digital Equipment Corporation (DEC) and was standardized by the International Standards Organization (ISO) in ISO/IEC 10589. The current version of this standard is ISO/IEC 10589:2002.

ISO/IEC 10589 defines support for the ISO Connectionless Network Protocol (CLNP) as defined in ISO 8473. However, the protocol was designed to be extensible to other network protocols. RFC 1195 defined IS-IS support for IP, and additional IETF extensions have defined IS-IS support for IPv6. Integration of support for multiple network layer protocols has led to the term Integrated IS-IS. The Cisco IOS IS-IS implementation supports CLNP, IPv4, and IPv6. This module and its related modules use the term IS-IS to refer to the Integrated IS-IS that is implemented by Cisco IOS software.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for the Integrated IS-IS Routing Protocol

This document assumes knowledge of CLNS, IPv4, and IPv6. The amount of knowledge required for each technology is dependent on your deployment.

Information About the Integrated IS-IS Routing Protocol

IS-IS Functional Overview

A routing domain may be divided into one or more subdomains. Each subdomain is referred to as an area and is assigned an area address. Routing within an area is referred to as Level-1 routing. Routing between Level-1 areas is referred to as Level-2 routing. A router in OSI terminology is referred to as an Intermediate System (IS). An IS may operate at Level 1, Level 2, or both. ISs that operate at Level 1 exchange routing information with other Level-1 ISs in the same area. ISs that operate at Level 2 exchange routing information with other Level-2 routers regardless of whether they are in the same Level-1 area. The set of Level-2 routers and the links that interconnect them form the Level-2 subdomain, which must not be partitioned in order for routing to work properly.

IS Address Assignment

An IS is identified by an address known as a Network Entity Title (NET). The NET is the address of a Network Service Access Point (NSAP), which identifies an instance of the IS-IS routing protocol running on an IS. The NET may be 8 to 20 octets in length and consists of three parts:

- Area address--This field is 1 to 13 octets in length and is composed of high-order octets of the address.

Note An IS-IS instance may be assigned multiple area addresses. When this is the case, all area addresses are considered synonymous. Multiple synonymous area addresses are useful when merging or splitting areas in the domain. In normal operation, for example, once the merge or split has been completed, there is no need to assign more than one area address to an IS-IS instance.

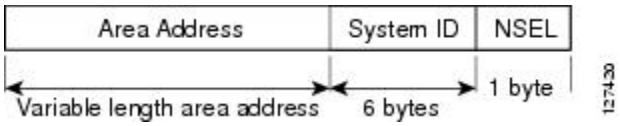
- System ID--This field is 6 octets long and immediately follows the area address. When the IS operates at Level 1, the system ID must be unique among all the Level-1 routers in the same area. When the IS operates at Level 2, the system ID must be unique among all routers in the domain.

Note An IS instance is assigned exactly one system ID.

- NSEL--The N-selector field is 1 octet in length and immediately follows the system ID. It must be set to "00".

The figure below shows the format for the NET.

Figure 1



IS-IS PDU Types

ISs exchange routing information with their peers using protocol data units (PDUs). The following types of PDUs are used:

- IIHs, page 3
- LSPs, page 3
- SNPs, page 4

IIHs

Intermediate System-to-Intermediate System Hello PDUs (IIHs) are exchanged between IS neighbors on circuits on which the IS-IS protocol is enabled. IIHs include the system ID of the sender, the assigned area address(es), and the identity of neighbors on that circuit that are known to the sending IS. Additional optional information may also be included.

There are three types of IIHs:

- Point-to-Point IIHs--These are sent on point-to-point circuits.
- Level-1 LAN IIHs--These are sent on multiaccess circuits when the sending IS operates as a Level-1 router on that circuit.
- Level-2 LAN IIHs--These are sent on multiaccess circuits when the sending IS operates as a Level-2 router on that circuit.

LSPs

An IS generates Link-State PDUs (LSPs) to advertise its neighbors and the destination that are directly connected to the IS. An LSP is uniquely identified by the following:

- System ID of the IS that generated the LSP
- pseudonode ID--This is always 0 except when the LSP is a pseudonode LSP (see Operation of IS-IS on Multiaccess Circuits, page 4)
- LSP number (0 to 255)
- 32-bit sequence number

Whenever a new version of an LSP is generated, the sequence number is incremented.

Level-1 LSPs are generated by ISs that support Level 1. The Level-1 LSPs are flooded throughout the Level-1 area. The set of Level-1 LSPs generated by all Level-1 ISs in an area is the Level-1 LSP Database (LSPDB). All Level-1 ISs in an area will have an identical Level-1 LSPDB and will therefore have an identical network connectivity map for the area.

Level-2 LSPs are generated by ISs that support Level 2. Level-2 LSPs are flooded throughout the Level-2 subdomain. The set of Level-2 LSPs generated by all Level-2 ISs in the domain is the Level-2 LSP

Database (LSPDB). All Level-2 ISs will have an identical Level-2 LSPDB and will therefore have an identical connectivity map for the Level-2 subdomain.

SNPs

Sequence Number PDUs (SNPs) contain a summary description of one or more LSPs. There are two types of SNPs--complete and partial--for both Level 1 and Level 2.

- Complete Sequence Number PDUs (CSNPs) are used to send a summary of the LSPDB that an IS has for a given level.
- Partial Sequence Number PDUs (PSNPs) are used to send a summary of a subset of the LSPs for a given level that an IS either has in its database or needs to obtain.

For more information about how SNPs are used, see the IS-IS Supported Circuit Types, page 4.

IS-IS Supported Circuit Types

IS-IS supports two generic circuit types:

- Point-to-point circuits
- Multiaccess circuits

Operation of IS-IS on Point-to-Point Circuits

A point-to-point circuit has exactly two ISs on the circuit. An IS forms a single adjacency to the other IS on the point-to-point circuit. The adjacency type describes what level(s) are supported on that circuit.

If both ISs support Level 1 on that circuit and the ISs are configured with at least one matching address, the adjacency supports Level 1. Level-1 LSPs and SNPs will be sent on that circuit.

If both ISs support Level 2 on that circuit, the adjacency supports Level 2. Level-2 LSPs and SNPs will be sent on that circuit.

The adjacency then can be Level 1, Level 2, or Level 1-2.

ISs send point-to-point IIHs on point-to-point circuits. These IIHs allow each IS to discover the identity of the neighbor, the configured area address(es), and the supported levels.

When an adjacency is first established, each IS sends a set of CSNPs for each level that is supported on the circuit. A CSNP set describes the current contents of the LSPDB at that level. By comparing the contents of the set of received CSNPs with the contents of the local LSPDB, each IS can determine where the databases differ and initiate procedures to exchange the necessary LSPs so that the databases are efficiently and reliably synchronized.

PSNPs are sent to acknowledge the receipt of an updated LSP.

Operation of IS-IS on Multiaccess Circuits

Multiaccess circuits support multiple ISs, for example, two or more operating on the circuit. The ability to address multiple systems utilizing a multicast or broadcast address is assumed.

An IS that supports Level 1 on a multiaccess circuit sends Level-1 LAN IIHs on the circuit. An IS that supports Level 2 on a multiaccess circuit sends Level-2 LAN IIHs on the circuit.

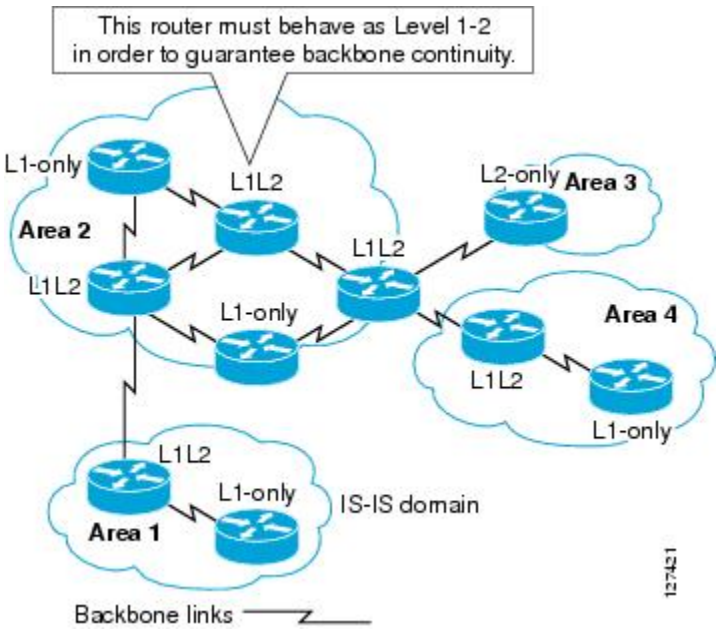
ISs form separate adjacencies for each level with neighbor ISs on the circuit.

An IS will form a Level-1 adjacency with other ISs that support Level 1 on the circuit and will have a matching area address. It is a misconfiguration to have two ISs with disjoint sets of area addresses supporting Level 1 on the same multiaccess circuit.

An IS will form a Level-2 adjacency with other ISs that support Level 2 on the circuit.

The routers in the IS-IS network topology in the figure below perform Level 1, Level 2, or Level 1 and 2 routing along the backbone of the network.

Figure 2



IS-IS Election of the Designated Intermediate System

If each IS advertised all of its adjacencies on a multiaccess circuit in its LSPs, the total number of advertisements required would be N 2 --where N is the number of ISs that operate at a given level on the circuit. To address this scalability issue, IS-IS defines a pseudonode to represent the multiaccess circuit. All ISs that operate on the circuit at a given level elect one of the ISs to act as the Designated Intermediate System (DIS) on that circuit. A DIS is elected for each level that is active on the circuit.

The DIS is responsible for issuing pseudonode LSPs. The pseudonode LSPs include neighbor advertisements for all of the ISs that operate on that circuit. All ISs that operate on the circuit (including the DIS) provide a neighbor advertisement to the pseudonode in their non-pseudonode LSPs and do not advertise any of their neighbors on the multiaccess circuit. In this way the total number of advertisements required varies as a function of N--the number of ISs that operate on the circuit.

A pseudonode LSP is uniquely classified by the following identifiers:

- System ID of the DIS that generated the LSP
- pseudonode ID--ALWAYS NON-ZERO
- LSP number (0 to 255)
- 32-bit sequence number

The nonzero pseudonode ID is what differentiates a pseudonode LSP from a nonpseudonode LSP and is chosen by the DIS to be unique among any other LAN circuits for which it is also the DIS at this level.

The DIS is also responsible for sending periodic CSNPs on the circuit. This provides a complete summary description of the current contents of the LSPDB on the DIS. Other ISs on the circuit can then perform the following activities:

- Flood LSPs that they have that are absent from or are newer than those that are described in the CSNPs sent by the DIS.
- Request an LSP by sending a PSNP for LSPs that are described in the CSNPs sent by the DIS that are absent from the local database or older than what is described in the CSNP set.

In this way, the LSPDBs of all ISs on a multiaccess circuit are efficiently and reliably synchronized.

IS-IS Overview of LSPDB Synchronization

Proper operation of IS-IS requires a reliable and efficient process to synchronize the LSPDBs on each IS. In IS-IS this process is called the update process. This section provides a brief overview of the operation of the update process. The update process operates independently at each supported level.

LSPs may be locally generated, in which case they always are new LSPs. LSPs may also be received from a neighbor on a circuit, in which case they may be generated by some other IS or may be a copy of an LSP generated by the local IS. Received LSPs may be older, the same age, or newer than the current contents of the local LSPDB.

- Handling of Newer LSPs, page 6
- Handling of Older LSPs, page 6
- Handling LSPs That Are the Same, page 7

Handling of Newer LSPs

A newer LSP is added to the local LSPDB. If an older copy of the same LSP currently exists in the LSPDB, it is replaced. The newer LSP is marked to be sent on all circuits on which the IS currently has an adjacency in the UP state at the level associated with the newer LSP--excluding the circuit on which the newer LSP was received.

On point-to-point circuits, the newer LSP will be flooded periodically until the neighbor acknowledges its receipt by sending a PSNP or by sending an LSP that is the same or newer than the LSP being flooded.

On multiaccess circuits, the IS will flood the newer LSP once. The IS examines the set of CNSPs that are sent periodically by the DIS for the multiaccess circuit. If the local LSPDB contains one or more LSPs that are newer than what is described in the CSNP set (this includes LSPs that are absent from the CSNP set) those LSPs are reflooded over the multiaccess circuit. If the local LSPDB contains one or more LSPs that are older than what is described in the CSNP set (this includes LSPs described in the CSNP set that are absent from the local LSPDB), a PSNP is sent on the multiaccess circuit with descriptions of the LSPs that require updating. The DIS for the multiaccess circuit responds by sending the requested LSPs.

Handling of Older LSPs

An IS may receive an LSP that is older than the copy in the local LSPDB. An IS may receive an SNP (complete or partial) that describes an LSP that is older than the copy in the local LSPDB. In both cases the IS marks the LSP in the local database to be flooded on the circuit on which the older LSP or SNP that contained the older LSP was received.

At this point, the actions taken are identical to the actions that are described in the previous Handling of Newer LSPs, page 6, after a new LSP has been added to the local database.

Handling LSPs That Are the Same

Because of the distributed nature of the update process, it is possible than an IS may receive copies of an LSP that is the same as the current contents of the local LSPDB.

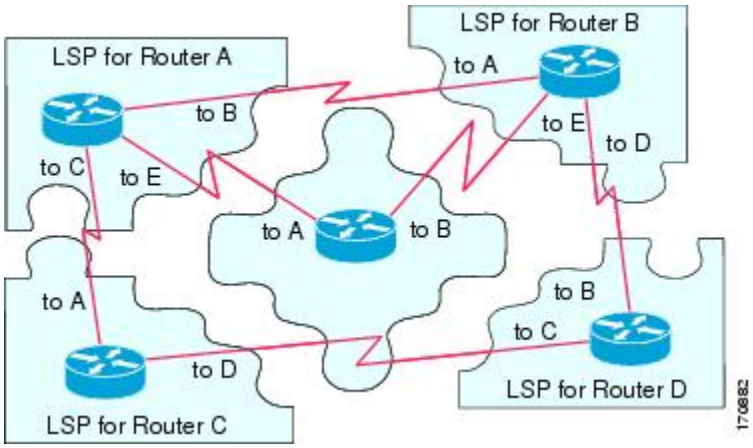
On a point-to-point circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

In a multiaccess circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

The figure below shows how the LSPs are used to create a network map. Imagine the network topology as a jigsaw puzzle. Each LSP (representing an IS) is considered one of the jigsaw pieces.

Note The figure below is applicable to all Level-1 routers in an area or to all Level-2 routers in a Level-2 subdomain.

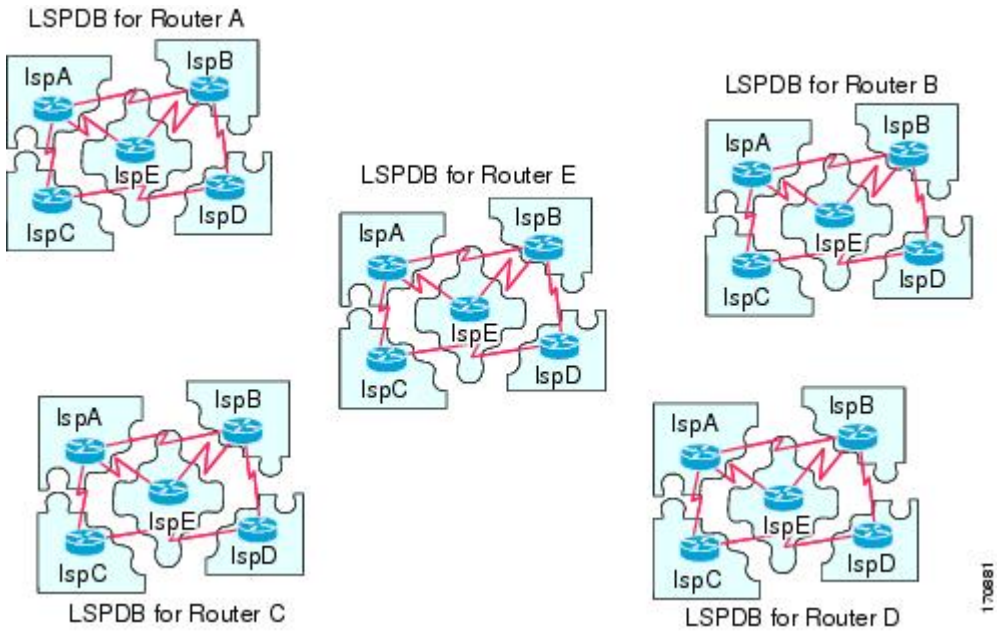
Figure 3



The figure below shows each router in the IS-IS network with its fully updated link-state database, after the adjacencies have been formed among the neighbor routers.

Note The figure below is applicable to all Level-1 routers in an area or to all Level-2 routers in a Level-2 subdomain.

Figure 4



IS-IS Overview of the Shortest Path Calculation

When the contents of the LSPDB change, each IS independently reruns a shortest path calculation. The algorithm is based on the well-known Dijkstra algorithm for finding the shortest paths along a directed graph where the ISs are the vertices of the graph and the links between the ISs are edges with a nonnegative weight. A two-way connectivity check is performed before considering a link between two ISs as part of the graph. This prevents the use of stale information in the LSPDB, for example, when one IS is no longer operating in the network but did not purge the set of LSPs that it generated before ceasing operation.

The output of the SPF is a set of tuples (destination, next hop). The destinations are protocol-specific; for example, they would be prefixes when the supported protocol is IP, NSAPs of end systems when the supported protocol is CLNP. Multiple equal-cost paths are supported, in which case multiple next hops would be associated with the same destination.

Independent SPFs are performed for each level supported by the IS. In cases in which the same destination is reachable by both Level-1 and Level-2 paths, the Level-1 path is preferred.

A Level-2 IS that indicates that it has one or more Level-2 neighbors in other areas may be used by Level-1 routers in the same area as the path of last resort, also called the default route. The Level-2 IS indicates its attachment to other areas by setting an attached bit (ATT) in its Level-1 LSP 0.

Note An IS can generate up to 256 LSPs at each level. The LSPs are identified by the numbers 0 through 255. LPS 0 has special properties, including the significance of the setting of the ATT bit to indicate attachment to other areas. When LPSs that are numbered 1 though 255 have the ATT bit set, it is not of significance.

Where to Go Next

- To initially configure and enable IS-IS, see the "Configuring a Basic IS-IS Network" module.
- To customize IS-IS for your network design, see the "Customizing IS-IS for Your Network Design" module.
- To customize IS-IS for achieving fast convergence and scalability, see the following modules:
  - "Overview of IS-IS Fast Convergence"
  - "Setting Best Practice Parameters for IS-IS Fast Convergence"
  - "Reducing Failure Detection Times in IS-IS Networks"
  - "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"
  - "Reducing Alternate-Path Calculation Times in IS-IS Networks"
- To enhance IS-IS network security, see the "Enhancing Security in an IS-IS Network" module.

Additional References

Standards

Standard	Title
ISO 8473	*CLNP, Connectionless Network Protocol*
ISO 9542	*ES-IS Routing Information Exchange Protocol*
ISO/IEC 10589	IS-IS Protocol

MIBs

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

RFCs

RFC	Title
RFC 1195	http://www.ietf.org/rfc/rfc1195.txt Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Glossary

area --A physically connected portion of a routing domain in which all routers are assigned a common area address. Also known as the Level-1 subdomain. A routing domain may consist of multiple areas that are reachable by traversing the Level-2 subdomain.

area address --The high-order octets of the Network Entity Title (NET) assigned to an IS. All ISs in the same Level-1 area are assigned the same area address.

CLNP --ISO Connectionless Network Protocol as defined in ISO 8473.

DIS --Designated Intermediate System. An IS elected by all the ISs operating on a multiaccess circuit at a given level to represent the multiaccess circuit. The DIS sends pseudonode LSPs on behalf of the circuit advertising adjacencies to all the ISs operating on that circuit.

domain --The portion of a network on which the IS-IS protocol is configured to operate. The routing domain consists of all Level-1 areas and the Level-2 subdomain.

ES --end system. An ES is any nonrouting host or node.

Integrated IS-IS --Extended form of IS-IS that supports multiple network protocols. Extensions have been defined in IETF documents, especially RFC 1195.

IS --intermediate system. OSI term for a router.

IP --Internet Protocol Version 4, also known as IPv4.

IPv6 --Internet Protocol Version 6.

IS-IS --Intermediate System-to-Intermediate System. Routing protocol as defined in ISO/IEC 10589.

Level-1 router --An IS that supports Level-1 routing for its assigned area.

Level-2 router --An IS that supports Level-2 routing.

Level-2 subdomain --All Level-2 capable routers in a domain and the links that interconnect them. Level-1 areas are interconnected via the Level-2 subdomain. For routing in a domain to work properly, the Level-2 subdomain must not be partitioned.

NET --Network Entity Title. An address assigned to an instance of the IS-IS protocol. The NET includes an area address, a system ID, and an N-selector. When multiple NETs are assigned to an IS-IS instance, only the area address portion of the NET may differ.

NSEL --N-selector. The least significant octet of a Network Entity Title. It is always assigned the value 00.

system ID --The part of the NET that immediately follows the area address. The field is 6 octets long.

Configuring a Basic IS-IS Network

This module describes the tasks to configure and monitor a basic Intermediate System-to-Intermediate System (IS-IS) network. The IS-IS process and adjacency formation is also explained. IS-IS is link-state protocol that allows the network designer to organize the network into a group of flooding domains. Often deployed as the Interior Gateway Protocol (IGP) for an ISP network backbone, IS-IS is capable of handling large topologies and large numbers of routing changes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Configuring a Basic IS-IS Network

- Before performing the tasks in this module, you should be familiar with the concepts described in the "Integrated IS-IS Routing Protocol Overview" module.
- You should know your network design and how you want traffic to flow through it before configuring IS-IS. Define areas, prepare an addressing plan for the routers (including defining the NETs), and determine the interfaces that will run Integrated IS-IS. To facilitate verification, a matrix of adjacencies should be prepared before you configure your routers, showing what neighbors should be expected in the adjacencies table. For more information on verifying IS-IS configuration and formed adjacencies, see "Monitoring IS-IS".

Information About the IS-IS Routing Protocol

IS-IS Process and Adjacencies

IS-IS requires some configuration on both the router and the interface. An IS-IS process is created when you enable IS-IS on a router and define a specific tag to identify that routing process. Interfaces configured with a specific tag will be part of the corresponding router process. More than one IS-IS process can run on a router for Connectionless Network Service (CLNS), but only one IS-IS process can run for IP.

Small IS-IS networks are built as a single area that includes all the routers in the network. As the network grows larger, it is usually reorganized into a backbone area made up of the connected set of all Level 2 routers from all areas. The areas are connected to local areas. Within a local area, routers know how to reach all system IDs. Between areas, routers know how to reach the backbone, and the backbone routers know how to reach other areas.

Routers establish Level 1 adjacencies to perform routing within a local area (intra-area routing). Routers establish Level 2 adjacencies to perform routing between Level 1 areas (inter-area routing).

If the network administrator does not specify Level 1 or Level 2 routing for the routing process being configured, the default routing behavior for the routing process will be Level 1-2.

If Level 2 routing is configured on any process, additional processes are automatically configured as Level 1, with the exception of previously configured Level 2 process, which will remain Level 2. You can have only one Level-2 process. You can configure the Level-2 process to perform Level-1 routing at the same time. If Level-2 routing is not desired for a router instance, use the **is-type** command in router configuration mode to remove the Level-2 capability. You can also use the **is-type** command to configure a different router instance as a Level-2 router.

Some networks use legacy equipment that supports only Level 1 routing. These devices are typically organized into many small areas that cannot be aggregated due to performance limitations. Cisco routers are used to interconnect each area to the Level 2 backbone.

Network entity titles (NETs) define the area addresses and the system ID of the router. See the "Configuring ISO CLNS" module in the *Cisco IOS ISO CLNS Configuration Guide* for a more detailed discussion of NETs.

PDU Packet Types in IS-IS Routing

The OSI stack defines a unit of data as a protocol data unit (PDU). A frame therefore is regarded by OSI as a data-link PDU, and a packet is regarded as a network PDU. There are four types of PDU packets, and each type can be Level 1 or Level 2:

- LSP--Link-state PDU. Used to distribute link-state information.
- IIH PDU--For IS-IS this is called the IS-IS Hello PDU. Used to establish and maintain adjacencies.

Note On point-to-point links, IIH PDUs will be the same for Level 1 and Level 2. Both Level-1 and Level-2 IIH use the same type of PDU, but they carry different circuit types.

- PSNP--partial sequence numbers protocol data unit (PDU). Used to acknowledge and request link-state information.
- CSNP--complete sequence number protocol data unit (PDU). Used to distribute the complete link-state database of a router.

IS-IS LSPs include specific information about the router's attachments. The following information is included in multiple TLV fields in the main body of the LSP:

- The links to neighbor router intermediate systems (ISs), including the metrics of those interfaces
- The links to the neighbor end systems (ESs)

How to Create Monitor and Make Changes to a Basic IS-IS Network

Enabling IS-IS as an IP Routing Protocol on the Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **net** *network-entity-title*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis`	Assigns a tag to an IS-IS process. Enters router configuration mode. • Configure tags to identify multiple IS-IS processes by giving a meaningful name for each routing process. If the tag is not specified, a null tag (0) is assumed and the process is referenced with a null tag. The tag name must be unique among all IP router processes for the router.
Step 4	**net** *network-entity-title* **Example:** `Router(config-router)# net 49.0001.0000.0000.000b.00`	Configures the NET on the router. • The NET identifies the router for IS-IS.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Enabling IS-IS as an IP Routing Protocol on the Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [*secondary*]
5. **ip router isis [** *area - tag* **]**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 4/0`	Enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [*secondary*] **Example:** `Router(config-if)# ip address 172.16.1.27 255.255.255.0`	Sets the primary IP address on the interface.
Step 5	**ip router isis [** *area - tag* **]** **Example:** `Router(config-if)# ip router isis company1`	Enables IS-IS on the interfaces that are to use IS-IS to distribute their IP information (and additionally that might be used to establish IS-IS adjacencies). • Use the *area-tag* argument to specify to which IS-IS process the router belongs. • If there is more than one IS-IS process on the router, repeat the **ip router isis** command for each interface, specifying an area tag for each interface to associate each interface with the specific process to which it belongs.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring IS-IS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isis display delimiter** [**return** *count* | **character** *count*]
4. **exit**
5. **show ip protocols**
6. **show clns is** *area-tag* **neighbors** [*type number*] [**detail**]
7. **show clns interface** [*type number*]
8. **show clns** *area-tag* **neighbors** [*type number*] [**area**] [**detail**]
9. **show clns** *area-tag* **traffic**
10. **show ip route** [*ip-address* [*mask*]] [[**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]]
11. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
12. **show isis database verbose**
13. **show isis lsp-log**
14. **show isis** [*area-tag*] [**ipv6** | *****] **spf-log**
15. **show isis** [*process-tag*] [**ipv6** | *****] **topology**
16. **show isis** [*area-tag*] **neighbors**[**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**isis display delimiter** [**return** *count*	**character** *count*] **Example:** `Router(config)# isis display delimiter return 15`	Makes output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show ip protocols** **Example:** `Router# show ip protocols`	Displays the parameters and current state of the active routing protocol process. • You can use this command to learn what protocols are active, what interfaces they are active on, what networks they are routing for, and other parameters that relate to the routing protocols.
Step 6	**show clns is** *area-tag* **neighbors** [*type number*] [**detail**] **Example:** `Router# show clns is tag3 neighbors detail`	Displays IS-IS information for IS-IS router adjacencies.
Step 7	**show clns interface** [*type number*] **Example:** `Router# show clns interface`	List the CLNS-specific information about each interface.
Step 8	**show clns** *area-tag* **neighbors** [*type number*] [**area**] [**detail**] **Example:** `Router# show clns area3 neighbors`	Displays both ES and IS neighbors. • The **show clns neighbor** command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your routers, showing what neighbors should be expected in the adjacencies table, to facilitate verification.

	Command or Action	Purpose
Step 9	**show clns** *area-tag* **traffic** **Example:** `Router# show clns area3 traffic`	Displays traffic statistics. To monitor IS-IS for stability once it has been deployed across your network, enter the **show clns traffic** command to check the following important statistics: high numbers of SPFs, checksum errors, and retransmissions. To troubleshoot IS-IS behavior, you can use the output from the **show clns traffic** command to check for the following indicators: • The number of link-state PDUs (LSPs) can help you determine the stability of the IS-IS network. The number of LSPs should never be zero. However, an LSP count that keeps increasing over a short time period indicates a network issue. • LSP retransmissions should stay low. A later execution of the **show clns traffic** command that shows an increase in LSP retransmissions, as compared to an earlier execution of the command, can indicate instability or traffic problems. • To check for partial route calculations (PRCs), enter the **show clns traffic** command. PRCs are flooded when a change that does not affect topology is reported through an LSP; typical examples include the addition or removal of a prefix or metric changes for external or passive interfaces. A PRC update queue that remains full or increases to the maximum value for long periods of time indicates network instability. • LSP checksum errors indicate a problem. • The update queue should not stay full and should not drop much.
Step 10	**show ip route** [*ip-address* [*mask*]] [[**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]] **Example:** `Router# show ip route 172.16.0.21`	Displays the current state of the routing table.
Step 11	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Router# show isis database detail`	Displays additional information about the IS-IS database. • Displays the link-state database for Level-1 and Level-2, the contents for each LSP, and the link-state protocol PDU identifier.

	Command or Action	Purpose
Step 12	**show isis database verbose** **Example:** `Router# show isis database verbose`	Displays additional information about the IS-IS database such as the sequence number, checksum, and holdtime for LSPs.
Step 13	**show isis lsp-log** **Example:** `Router# show isis lsp-log`	Displays a log of LSPs including time of occurrence, count, interface, and the event that triggered the LSP.
Step 14	**show isis** [*area-tag*] [**ipv6** | *****] **spf-log** **Example:** `Router# show isis spf-log`	Displays how often and why the router has run a full shortest path first (SPF) calculation. • If the router continues to run SPF without ceasing, there might be an issue regarding a change in the network (intra-area). The cause for the continued SPF calculations could be an interconnecting link that is transitioning up/down/up/down or a metric change. It is normal for the SPF calculation to run a few times when a network change occurs, but then it should cease.
Step 15	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **Example:** `Router# show isis topology`	Displays a list of all connected routers in all areas.
Step 16	**show isis** [*area-tag*] **neighbors**[**detail**] **Example:** `Router# show isis neighbors detail`	Displays IS-IS adjacency information. • The **show isis neighbor detail**command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your routers, showing what neighbors should be expected in the adjacencies table, to facilitate verification.

Example

When the **show isis neighbors** command is entered with the **detail** keyword, the output provides information on the IS-IS adjacencies that have formed.

```
Router1# show isis neighbors detail
System Id      Type Interface IP Address      State Holdtime Circuit Id
Router2         L2   Et1/0     10.1.1.0        UP   255      Circuit3.01
  Area Address(es): 32
  SNPA: aabb.cc00.2001
  State Changed: 00:00:14
  LAN Priority: 64
  Format: Phase V
```

• Troubleshooting Tips, page 22

Troubleshooting Tips

You can use the following two system debugging commands to check your IS-IS IPv4 implementation.

- If adjacencies are not coming up properly, use the **debug isis adj-packets** command.
- To display a log of significant events during an IS-IS SPF calculation, use the **debug isis spf-events** command.

Shutting Down IS-IS to Make Changes to Your IS-IS Network

You can shut down IS-IS (placing it in an administrative down state) to make changes to the IS-IS protocol configuration, without losing your configuration parameters. You can shut down IS-IS at the interface level or at the global IS-IS process level. If the router was rebooted when the protocol was turned off, the protocol would be expected to come back up in the disabled state. When the protocol is set to the administrative down state, network administrators are allowed to administratively turn off the operation of the IS-IS protocol without losing the protocol configuration, to make a series of changes to the protocol configuration without having the operation of the protocol transition through intermediate--and perhaps undesirable--states, and to then reenable the protocol at a suitable time.

Before the introduction of the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature, there was no nondestructive way to disable IS-IS operation. The only way to disable IS-IS at the router level was to issue the **no router isis** command, which removes the IS-IS configuration. At the interface level there are two ways to disable IS-IS operation. You can enter the **no ip router isis** command to remove IS-IS from the specified interface, or you can put the interface into passive mode such that the IP address of the specified interface will still be advertised. In either case, the current IS-IS configuration will be removed.

- Shutting Down IS-IS in Interface Mode, page 22
- Shutting Down IS-IS in Router Mode, page 23

Shutting Down IS-IS in Interface Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isis protocol shutdown**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0`	Configures an interface and enters interface configuration mode.
Step 4	**isis protocol shutdown** **Example:** `Router(config-if)# isis protocol shutdown`	Disables the IS-IS protocol so that it cannot form adjacencies on a specified interface and places the IP address of the interface into the LSP that is generated by the router.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Shutting Down IS-IS in Router Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **protocol shutdown**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis 1`	Enables the IS-IS routing protocol and specifies an IS-IS process. • Enters router configuration mode.
Step 4	**protocol shutdown** **Example:** `Router(config-router)# protocol shutdown`	Prevents IS-IS from forming any adjacency on any interface and clears the IS-IS LSP database, without actually removing the IS-IS configuration.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for a Basic IS-IS Network

Example Configuring a Basic IS-IS Network

The following example shows how to configure three routers to run IS-IS as an IP routing protocol. The figure below illustrates the sample configuration.

Router A Configuration

```
router isis
 net 49.0001.0000.0000.000a.00
interface ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
interface serial 2/0
 ip router isis
 ip address 192.168.1.2 255.255.255.0
```

Router B Configuration

```
router isis
 net 49.0001.0000.0000.000b.00
interface ethernet0/0
 ip router isis
 ip address 172.17.1.1 255.255.255.0
interface serial2/0
 ip router isis
 ip address 192.168.1.1 255.255.255.0
interface serial5/0
 ip router isis
 ip address 172.21.1.1 255.255.255.0
```

Router C Configuration

```
router isis
 net 49.0001.0000.0000.000c.00
interface ethernet2/0
 ip router isis
 ip address 172.21.1.2 255.255.255.0
interface serial5/0
 ip router isis
 ip address 172.22.1.1 255.255.255.0
```

The **show isis topology** command displays the following information about how the routers are connected within the IS-IS network:

```
RouterB# show isis topology
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
RouterA              10         RouterA              Se2/0       *HDLC*
RouterB              --
RouterC              10         RouterC              Se5/0       *HDLC*
IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
RouterA              10         RouterA              Se2/0       *HDLC*
RouterB              --
RouterC              10         RouterC              Se5/0       *HDLC*
```

The **show isis database** command displays following information for the Level 1 and Level 2 LSPs for each router in the IS-IS network.

```
RouterB# show isis database
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
RouterA.00-00           0x00000005   0x1A1D        1063              0/0/0
RouterB.00-00         * 0x00000006   0xD15B        1118              0/0/0
RouterC.00-00           0x00000004   0x3196        1133              1/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
RouterA.00-00           0x00000008   0x0BF4        1136              0/0/0
RouterB.00-00         * 0x00000008   0x1701        1137              0/0/0
RouterC.00-00           0x00000004   0x3624        1133              0/0/0
```

The **show ip route** command displays information about the interfaces of each router, including their IP addresses and how they are connected to Router B:

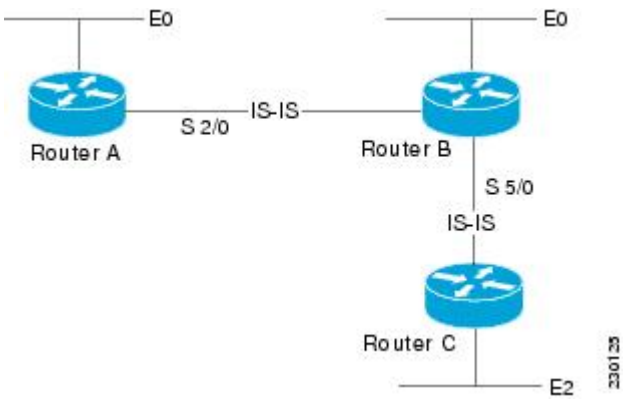
```
RouterB# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     172.17.0.0/24 is subnetted, 1 subnets
```

```
C       172.17.1.0 is directly connected, Ethernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial4/0
     172.21.0.0/24 is subnetted, 1 subnets
C       172.21.1.0 is directly connected, Serial5/0
     172.22.0.0/24 is subnetted, 1 subnets
i L1    172.22.1.0 [115/20] via 172.21.1.2, Serial5/0
     10.0.0.0/24 is subnetted, 1 subnets
i L1    10.1.1.0 [115/20] via 192.168.1.2, Serial2/0
C    192.168.1.0/24 is directly connected, Serial2/0
C    192.168.3.0/24 is directly connected, Serial3/0
```

The **show isis spf-log** command displays logs of Level 1 and Level 2 LSPs including time of occurrence, duration, count, and the event that triggered the LSP.

```
RouterB## show isis spf-log
   level 1 SPF log
  When   Duration  Nodes  Count    First trigger LSP   Triggers
00:01:30       0      3      7        RouterB.00-00  PERIODIC NEWADJ NEWLSP TLVT
   level 2 SPF log
  When   Duration  Nodes  Count    First trigger LSP   Triggers
00:01:31       0      3      7        RouterB.00-00  PERIODIC NEWADJ NEWLSP TLVT
```

Figure 5



Example Shutting Down IS-IS in Interface Mode

The following router output shows that the router has two IS-IS adjacencies:

```
Router# show clns neighbors
System Id  Interface  SNPA            State  Holdtime  Type      Protocol
first      Et3/1      0002.7dd6.1c21  Up     25        L1L2      IS-IS
second     Et3/2      0004.6d25.c056  Up     29        L1L2      IS-IS
```

When the **isis protocol shutdown** command is entered for Ethernet interface 3/1, the IS-IS protocol will be disabled for the specified interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet3/1
Router(config-if)# isis protocol shutdown
Router(config-if)# end
```

The following router output shows that the adjacency for Ethernet interface 3/1 has not formed:

```
Router# show clns neighbors
System Id  Interface  SNPA            State  Holdtime  Type      Protocol
second     Et3/2      0004.6d25.c056  Up     27        L1L2      IS-IS
```

Example Shutting Down IS-IS in Router Mode

The following router output shows that the router has two IS-IS adjacencies:

```
Router# show clns neighbors
System Id  Interface  SNPA            State  Holdtime  Type      Protocol
south      Et3/1      0002.7dd6.1c21  Up     29        L1L2      IS-IS
north      Et3/2      0004.6d25.c056  Up     28        L1L2      IS-IS
```

The **protocol shutdown** command is entered so that IS-IS is disabled and no adjacencies will be formed on any interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router isis area1
Router(config-router)# protocol shutdown
Router(config-router)# end
```

The following router output now shows that both adjacencies are gone.

```
Router# show clns neighbors
System Id  Interface  SNPA            State  Holdtime  Type      Protocol
```

When the **no protocol shutdown** command is entered, the adjacencies will again be formed on both interfaces:

```
Router(config)# router isis area1
Router(config-router)# no protocol shutdown
Router(config-router)# end
Router# show clns neighbors
System Id  Interface  SNPA            State  Holdtime  Type      Protocol
south      Et3/1      0002.7dd6.1c21  Up     24        L1L2      IS-IS
north      Et3/2      0004.6d25.c056  Up     24        L1L2      IS-IS
```

Where to Go Next

- To customize IS-IS for your network design, see the "Customizing IS-IS for Your Network Design" module.
- To customize IS-IS for achieving fast convergence and scalability, see the following modules:
  - "Overview of IS-IS Fast Convergence"
  - "Setting Best Practice Parameters for IS-IS Fast Convergence"
  - "Reducing Failure Detection Times in IS-IS Networks"
  - "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"
  - "Reducing Alternate-Path Calculation Times in IS-IS Networks"
- To enhance IS-IS network security, see the "Enhancing Security in an IS-IS Network" module.

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of IS-IS concepts	"Integrated IS-IS Routing Protocol Overview" module
Customizing IS-IS for achieving fast convergence and scalability	"Overview of IS-IS Fast Convergence" module

Standards

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

MIBs

MIB	MIBs Link
• CISCO-IETF-IP-FORWARD-MIB • CISCO-IETF-IP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1195	http://www.ietf.org/rfc/rfc1195.txt Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring a Basic IS-IS Network

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

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

Table 1 Feature Information for Configuring a Basic IS-IS Network

Feature Name	Releases	Feature Information
Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	12.0(27)S 12.2(25)S 12.3(4)T	The Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature allows you to disable the Integrated Intermediate System-to-Intermediate System (IS-IS) protocol at the interface level or at the global IS-IS process level without removing the IS-IS configuration parameters.

Customizing IS-IS for Your Network Design

This module describes optional tasks that you can perform to customize Intermediate System-to-Intermediate System (IS-IS) for your network design. You can optimize network traffic flow by setting metrics, specifying an IS-IS system type, summarizing addresses, generating a default route, and configuring a global default metric.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Customizing IS-IS for Your Network Design

- Before performing the tasks in this module, you should be familiar with the concepts described in the "Integrated IS-IS Routing Protocol Overview" module.
- You should understand the concept of IP addressing. For more information on IP addressing, see the "Configuring IPv4 Addresses" module of the *Cisco IOS IP Addressing Services Configuration Guide*.
- You should know your network design and how you want traffic to flow through it before configuring IS-IS. Define areas, prepare an addressing plan for the routers (including defining the network entity titles [NETs]), and determine the interfaces that will run Integrated IS-IS.
- IS-IS must be enabled.

Restrictions for Customizing IS-IS for Your Network Design

If you have already configured a metric for a specific interface by entering the **isis metric** command, the metric that has been configured for that specific interface will take precedence over any default set by the **metric** command.

Information About Customizing IS-IS for Your Network Design

You can enhance network traffic flow by configuring IS-IS metric values for Level-1 or Level-2 routing, in order to prioritize traffic through certain paths. You can customize network traffic flow by changing the metric cost for a specified interface. All IS-IS links use the metric of 10 by default. The protocol does not automatically incorporate link attributes such as bandwidth or delay when metric values are assigned. The total cost to a destination is the sum of the costs on all outgoing interfaces along a particular path from the source to the destination. The least-cost paths are preferred.

If you want to configure a global default metric, see the Configuring an IS-IS Default Metric, page 39.

On multi-access networks, IS-IS elects a router to act as a pseudo-node representing the multi-access circuit. The elected router is known as the designated intermediate system (DIS). The DIS issues pseudo-node LSPs listing all of the routers which are reachable on the network. Each router on the network advertises in its non-pseudonode LSPs reachability to the DIS. This reduces the amount of information that needs to be advertised. A DIS is elected for each level that is operating on the network, for example both Level 1 and Level 2. By default, all routers have the same priority for being elected DIS. The MAC address of each router's interface onto the network is used as the tiebreaker. When all routers have the same priority, the addition or removal of a router onto the network can result in a chance in the DIS. This churn can be prevented by assigning a higher priority to the router which you wish to act as the DIS. Priorities can be configured individually for Level 1 and Level 2. By default the priority is 64. You can configure the priority in the range from 0 to 127.

You can configure a summary address to represent summarized (aggregate) addresses within the IS-IS routing table. This process is called route summarization. Using a summary address can enhance scalability and network stability because it reduces the amount of information that needs to be advertised and reduces the frequency of updates required. For example, a single route flap may not cause the summary advertisement to flap. The disadvantage of using the summary addresses is that routing may be sub-optimal, for example, the path to a specific destination covered by the summary address may be longer than it would have been, had all the individual addresses been advertised. Summary addresses are most commonly used to summarize routes from one Level-one area into the Level-2 subdomain. One summary address can include multiple groups of addresses for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes.

In Cisco IOS software, IS-IS has a default metric value of 10 for all active interfaces. If the interface is passive, the default value is zero. Rather than change the metric values for the active interfaces one by one, you can configure a different default metric value to be used by all interfaces. All interfaces that had the original IS-IS default metric 10 will be configured with the new default value. Besides offering the user the convenience of being able to globally configure the value for all IS-IS interfaces, the feature helps prevent errors that may occur when interfaces are individually configured to change the metric value. For example the user may remove configured metrics from an interface, thereby restoring the default metric value of 10--perhaps unintentionally making that interface a highly preferred one in the network. Such an occurrence on the wrong interface could mean the rerouting of traffic across the network on an undesirable path.

- Enhancing Your IS-IS Network Design at the Interface Level, page 33

- Enhancing Your IS-IS Network Design at the Router Level, page 35

Enhancing Your IS-IS Network Design at the Interface Level

Setting the IS-IS Link-State Metrics

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type name*
4. **isis metric** *default-metric* [**level-1** | **level-2**]
5. **end**
6. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type name* **Example:** `Router(config)# interface ethernet 0`	Enters interface configuration mode.
Step 4	**isis metric** *default-metric* [**level-1**	**level-2**] **Example:** `Router(config-if)# isis metric 15 level-1`	Configures the metric for an interface. **Note** We highly recommend that you configure the metrics on all interfaces. If you do not do so, all links will have the same cost and the cost to reach any node in the network will be logically equivalent to the number of hops.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Router# show isis database detail`	(Optional) Displays the IS-IS link-state database. • To display information about each LSP and the link-state database, enter the **detail** keyword.

Prioritizing Designated Intermediate Systems for IS-IS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type name*
4. **isis priority** *number-value* [**level-1** | **level-2**]
5. **end**
6. **show clns interface** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type name* **Example:** `Router(config)# interface ethernet 0/3`	Enters interface configuration mode.
Step 4	**isis priority** *number-value* [**level-1** | **level-2**] **Example:** `Router(config-if)# ip priority 2 level-1`	Configures the priority used in designated router election.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show clns interface** *type number* **Example:** `Router# show clns interface ethernet 0/3`	(Optional) Displays CLNS-specific information about the the interfaces running IS-IS. • The command output will display the DIS for both Level 1 and Level 2.

Enhancing Your IS-IS Network Design at the Router Level

Limiting Level 1 and Level 2 Operations on the IS-IS Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **is-type** [**level-1** | **level-1-2** | **level-2-only**]
5. **end**
6. **show isis** [**ipv6**] [*] **topology**[**level-1**] [**level-2**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol. • Enters router configuration mode.
Step 4	**is-type** [**level-1** | **level-1-2** | **level-2-only**] **Example:** `Router(config-router)# is-type level-1`	Configures the routing level for an instance of the IS-IS routing process. • By default Cisco IOS software enables both Level 1 and Level 2 operations on IS-IS routers. Specifying routers to act as Level 1, Level 2, or Level 1 and 2 can streamline your network design.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show isis** [**ipv6**] [*] **topology**[**level-1**] [**level-2**] **Example:** `Router# show isis topology level-1`	(Optional) Displays a list of all connected routers in all areas. • To confirm paths to all Level 1 or Level 2 routers in the area or areas in which this router resides, enter the **level-1** or **level-2** keywords, respectively.

Example

The following example shows output from the **show isis topology** command for a router within a dual CLNS-IP network. In this example, because neither the **level-1** nor **level-2** optional keywords were entered, information is displayed for both Level 1 and Level 2 routers.

```
Router# show isis topology
Tag L2BB:
IS-IS paths to level-2 routers
```

```
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0005  --
0000.0000.0009  10      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0017  20      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0053  30      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0068  20      0000.0000.0009  Tu529           *Tunnel*
Tag A3253-01:
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0003  10      0000.0000.0003  Et1             0000.0c03.6944
0000.0000.0005  --
0000.0000.0053  10      0000.0000.0053  Et1             0060.3e58.ccdb
```

Summarizing Address Ranges in the IS-IS Routing Table

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**}[**tag** *tag-number*] [**metric** *metric-value*]
5. **end**
6. **show isis database verbose**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol. • Enters router configuration mode.

	Command or Action	Purpose
Step 4	**summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**}[**tag** *tag-number*] [**metric** *metric-value*] **Example:** `Router(config-router)# summary-address 10.1.0.0 255.255.0.0 level-2`	Creates aggregate addresses for IS-IS. **Note** Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes. This command helps reduce the size of the routing table.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show isis database verbose** **Example:** `Router# show isis database verbose`	(Optional) Displays detailed information about the IS-IS database.

Generating an IS-IS Default Route

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **default-information originate** [**route-map** *map-name*]
5. **end**
6. **show ip route**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol. • Enters router configuration mode.
Step 4	**default-information originate** [**route-map** *map-name*] **Example:** `Router(config-router)# default-information originate`	Generates a default route into an IS-IS routing domain. • Use the route map to identify the level into which the default route is to be announced, whether a particular non-default prefix must be reachable, etc.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show ip route** **Example:** `Router# show ip route`	(Optional) Displays the current state of the routing table.

Configuring an IS-IS Default Metric

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric** *default-value* [**level-1** | **level-2**]
5. **end**
6. **show clns interface** [*type number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** **Example:** `Router(config)# router isis 1`	Enables IS-IS as an IP routing protocol. • Enters router configuration mode.
Step 4	**metric** *default-value* [**level-1** | **level-2**] **Example:** `Router(config-router)# metric 25 level-2`	Globally sets a new default metric value for all IS-IS interfaces. • The value 25 shown in the example will apply only to Level 2 IS-IS interfaces. If you do not enter the **level-1** or **level-2** keyword, the metric will be applied to both Level 1 and Level 2 IS-IS interfaces.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show clns interface** [*type number*] **Example:** `Router# show clns interface`	(Optional) Displays the CLNS-specific information about each interface. • Enter this command if you want to verify the IS-IS global default metric that is set for the interface.

Configuration Examples for Customizing IS-IS for Your Network Design

Example Configuring a Global Default Metric for IPv4

The following configuration example for an IS-IS routing process called area1 sets a global default metric of 111 for the IS-IS interfaces:

```
interface Ethernet3/1
 ip address 172.16.10.2 255.255.0.0
 ip router isis area1
 no ip route-cache
 duplex half
!
interface Ethernet3/2
 ip address 192.168.242.2 255.255.255.0
 ip router isis area1
 no ip route-cache
 duplex half
router isis area1
 net 01.0000.0309.1234.00
 metric-style wide
 metric 111
```

In the following example, the **show clns interface** command confirms that the IS-IS IPv4 interface metric for both Level 1 and Level 2 interfaces is assigned the new default metric value 111:

```
Router# show clns interface
Ethernet3/1 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 39 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 922 milliseconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
Ethernet3/2 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 20 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x1, local circuit ID 0x2
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

In the following example, the **isis metric** command is entered so that it will assign a metric value of 10. The metric value that is set with the **isis metric** command for Ethernet interface 3/1 will take precedence over the metric value that was previously set with the **metric** command.

```
interface Ethernet3/1
 ip address 172.30.10.2 255.255.0.0
```

```
 ip router isis area1
 no ip route-cache
 duplex half
 isis metric 10
!
interface Ethernet3/2
 ip address 192.168.224.2 255.255.255.0
 ip router isis area1
 no ip route-cache
 duplex half
router isis area1
 net 01.0000.0309.1234.00
 metric-style wide
 metric 111
```

When the **show clns interface**command is entered, the router output confirms that the interface has an assigned IS-IS IPv4 metric value of 10:

```
Router# show clns interface
Ethernet3/1 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 53 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: mekong.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: mekong.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 4 seconds
    Next IS-IS LAN Level-2 Hello in 4 seconds
Ethernet3/2 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 30 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x1, local circuit ID 0x2
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 922 milliseconds
```

Where to Go Next

- To customize IS-IS for achieving fast convergence and scalability, see the "Overview of IS-IS Fast Convergence" module.
- To enhance IS-IS network security, see the "Enhancing Security in an IS-IS Network" module.

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Integrated IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module
Configuring IPv6	"Implementing IPv6 Addressing and Basic Connectivity" module in the *Cisco IOS IPv6 Configuration Guide*
Configuring the IS-IS protocol for IPv6 networks	"Implementing IS-IS for IPv6" module in the *Cisco IOS IPv6 Configuration Guide*

RFCs

RFCs	Title
RFC 1195	http://www.ietf.org/rfc/rfc1195.txt Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Customizing IS-IS for Your Network Design

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2 Feature Information for Customizing IS-IS for Your Network Design

Feature Name	Releases	Feature Information
Integrated IS-IS Global Default Metric	12.0(27)S 12.2(25)S 12.3(4)T	The Integrated IS-IS Global Default Metric feature allows you to change the global IS-IS default metric for interfaces so that you need not change the metric values for the interfaces one by one. All interfaces that had the original IS-IS default metric 10 will be configured with the new global default value.

IS-IS MIB

This feature introduces MIB support for the Intermediate System-to-Intermediate System (IS-IS) link-state routing protocol. IS-IS is used as the link-state routing protocol of choice by major service providers. The IS-IS MIB feature offers service providers an improved capability to continuously monitor the changing state of an IS-IS network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant protocol events such as an authentication failure or a mismatch in area addresses between Intermediate Systems (ISs). The protocol information collected by the IS-IS MIB objects and trap objects can be used by the network manager to derive statistics that can help monitor and improve overall network performance.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for IS-IS MIB

- Simple Network Management Protocol (SNMP) must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.
- IS-IS must be configured on the router.

Restrictions for IS-IS MIB

- All enhancements that are introduced by this feature are provided only by the Cisco private MIB CISCO-IETF-ISIS-MIB.my.
- The SNMP SET capability will not be supported for any IS-IS MIB objects. Objects with read-create or read-write access are understood to operate only as read-only.
- This feature is not supported for multiple instances of IS-IS.

Information About IS-IS MIB

- Cisco IS-IS MIB Table Object Definitions, page 46
- Cisco IS-IS MIB Trap Notifications, page 53

Cisco IS-IS MIB Table Object Definitions

The IS-IS MIB feature introduces network management support for the IS-IS routing protocol through the use of IS-IS MIB table entries, MIB objects and MIB trap notification objects that comprise the Cisco private MIB CISCO-IETF-ISIS-MIB.my. New CLI has been added to enable SNMP notifications for IS-IS MIB objects. Notifications are provided for errors and other significant event information for the IS-IS network.

The following MIB objects describe IS-IS MIB table entries:

The ciiManAreaAddrEntry table contains the set of area addresses manually configured for the IS. The ciiManAreaAddrEntry table defines the following MIB objects:

- ciiManAreaAddr
- ciiManAreaAddrExistState

The ciiAreaAddrEntry table groups sets of relevant area addresses reported in all Level 1 link-state packets (LSPs) that were generated or received by an IS from other ISs that are reachable through Level 1 routing.

Each entry contains one area address per LSP. The ciiAreaAddrEntry table defines the following MIB object:

- ciiAreaAddr

The ciiSysProtSuppEntry table contains a manually configured set of protocols supported by the IS. The supported protocol types are IPv4, IPv6 and ISO8473. The ciiSysProtSuppEntry table defines the following MIB objects:

- ciiSysProtSuppProtocol
- ciiSysProtSuppExistState

The ciiSummAddrEntry table contains a set of manually configured summary addresses used to form summarized IP TLVs originated by an ISS. This table is useful to combine and modify IP reachability announcements, and also controls leaking of L1 routes into L2. The ciiSummAddrEntry table defines the following MIB objects:

- ciiSummAddressType
- ciiSummAddress
- ciiSummAddrPrefixLen

- ciiSummAddrExistState
- ciiSummAddrMetric
- ciiSummAddrFullMetric

The ciiRedistributeAddrEntry table provides the criteria to decide if a route should be leaked from L2 to L1. When Domain Wide Prefix leaking is enabled (represented by ciiSysL2toL1Leaking), addresses that match the summary mask in the table are announced at L1 by routers. The Cisco MIB implementation also allows retrieval of routes for masked entries based on configured access lists or route maps. The ciiRedistributeAddrEntry table defines the following MIB objects:

- ciiRedistributeAddrType
- ciiRedistributeAddrAddress
- ciiRedistributeAddrPrefixLen
- ciiRedistributeAddrExistState

The ciiRouterEntry table has one entry for every peer and it tracks the hostnames and Router IDs associated with that peer. The ciiRouterEntry table defines the following MIB objects.

- ciiRouterSysID
- ciiRouterLevel
- ciiRouterHostName
- ciiRouterID

Note The IS-IS MIB defines the ciiRouterLevel object to be the level of the IS. The Cisco implementation interprets the ciiRouterLevel object to be the level of the link-state packet (LSP) in which the hostname (ciiRouterHostName) and router ID (ciiRouterID) were received.

The ciiSysLevelEntry table captures level-specific information about the IS. This information includes parameters that control how LSPs are generated, metrics for SPF computation and the decision of whether to perform traffic engineering at this level.

The ciiSysLevelEntry table defines the following MIB objects:

- ciiSysLevelIndex
- ciiSysLevelOrigLSPBuffSize
- ciiSysLevelMinLSPGenInt
- ciiSysLevelOverloadState
- ciiSysLevelSetOverload
- ciiSysLevelSetOverloadUntil
- ciiSysLevelMetricStyle
- ciiSysLevelSPFConsiders
- ciiSysLevelTEEnabled

Note For the ciiSysLevelOverloadState MIB object, the Cisco MIB follows the correct interpretation of IS state transition per the future IETF draft MIB revisions. The draft-ietf-isis-wg-16.txt did not follow the ISO 10589:2002 definition correctly. Per the ISO 10589:2002 definition, the waiting state is defined for low memory resource condition and the overloaded state is enabled by the administrator. Moreover, the Cisco implementation does not support a transition to a waiting state on low memory.

The ciiCircEntry table contains circuit-specific information about each broadcast or point-to-point interface used in this IS-IS. Each entry is associated with a corresponding interface, based on the circuit type

(broadcast or point-to-point interfaces). In other words, only interfaces that are configured as broadcast or point-to-point can be polled. The Cisco implementation of the IS-IS MIB does not support the following circuit types: staticIn, staticOut, dA (dynamically assigned). The ciiCircEntry table defines the following MIB objects:

- ciiCircIndex
- ciiCircIfIndex
- ciiCircIfSubIndex
- ciiCircAdminState
- ciiCircExistState
- ciiCircType
- ciiCircExtDomain
- ciiCircLevel
- ciiCircPassiveCircuit
- ciiCircMeshGroupEnabled
- ciiCircMeshGroup
- ciiCircSmallHellos
- ciiCircLastUpTime
- ciiCirc3WayEnabled
- ciiCircExtendedCircID

Note The ciiCircExtDomain MIB table object is not implemented because externalDomain linkage is not supported by Cisco IOS software.

The ciiNextCircIndex object, which is defined outside ciiCircTable, is used to assign a unique index value to the ciiCircIndex through a SET operation. The Cisco MIB implementation does not implement this object because the SET ability currently is not supported, and ciiCircIndex is determined uniquely through data from configured interfaces.

The ciiCircLevelEntry table contains level-specific information about IS-IS circuits. The ciiCircLevelEntry table contains the following MIB objects:

- ciiCircLevelIndex
- ciiCircLevelMetric
- ciiCircLevelWideMetric
- ciiCircLevelISPriority
- ciiCircLevelIDOctet
- ciiCircLevelID
- ciiCircLevelDesIS
- ciiCircLevelHelloMultiplier
- ciiCircLevelHelloTimer
- ciiCircLevelDRHelloTimer
- ciiCircLevelLSPThrottle
- ciiCircLevelMinLSPRetransInt
- ciiCircLevelCSNPInterval
- ciiCircLevelPartSNPInterval

The ciiSystemCounterEntry table has a sequence of entries used to track system-wide events using counters. The ciiSystemCounterEntry table defines the following MIB objects:

- ciiSysStatLevel
- ciiSysStatCorrLSPs
- ciiSysStatAuthTypeFails
- ciiSysStatAuthFails
- ciiSysStatLSPDbaseOloads
- ciiSysStatManAddrDropFromAreas
- ciiSysStatAttmptToExMaxSeqNums
- ciiSysStatSeqNumSkips
- ciiSysStatOwnLSPPurges
- ciiSysStatIDFieldLenMismatches
- ciiSysStatPartChanges
- ciiSysStatSPFRuns
- ciiSysStatLSPErrors

Note The ciiSysStatPartChanges object is not implemented because the ability to detect partition changes currently is not supported by Cisco IOS software.

The ciiCircuitCounterEntry table is used to track system-wide events specific to a circuit and level. The ciiCircuitCounterEntry table defines the following MIB objects:

- ciiCircuitType
- ciiCircAdjChanges
- ciiCircNumAdj
- ciiCircInitFails
- ciiCircRejAdjs
- ciiCircIDFieldLenMismatches
- ciiCircMaxAreaAddrMismatches
- ciiCircAuthTypeFails
- ciiCircAuthFails
- ciiCircLANDesISChanges

Note The ciiCircInitFails MIB object does not return any data because circuit initialization failures are not tracked by Cisco IOS software.

The ciiPacketCounterEntry table tracks the number of IS-IS packets sent and received over a circuit at one level. At any time, the traffic flow along one direction is recorded. All objects defined in this table are Counter objects. The ciiPacketCounterEntry table defines the following MIB objects:

- ciiPacketCountLevel
- ciiPacketCountDirection
- ciiPacketCountIIHellos
- ciiPacketCountISHellos
- ciiPacketCountESHellos
- ciiPacketCountLSPs
- ciiPacketCountCSNPs
- ciiPacketCountPSNPs
- ciiPacketCountUnknowns

Note The ciiPacketCountISHellos MIB object tracks the number of end system-Intermediate system (ES-IS) hellos only at system granularity and not at per-level or per-circuit.

- The ciiPacketCountESHellos MIB objects tracks the number of end-system (ES) hellos only at system granularity and not at per-level or per-circuit.
- The ciiPacketCountUnknowns MIB object can track only unknown packet types that are received, not those that are sent in any given level.

The ciiISAdjEntry table has one entry associated with every adjacency to an IS (in other words, a table of adjacencies).

However, this object cannot be used to track multiple adjacencies in a LAN, with each adjacency corresponding to a level. Thus the best priority level is selected among the configured objects.

The ciiISAdjEntry table defines the following MIB objects:

- ciiISAdjChanges
- ciiISAdjIndex
- ciiISAdjState
- ciiISAdj3WayState
- ciiISAdjNeighSNPAAddress
- ciiISAdjNeighSysType
- ciiISAdjNeighSysID
- ciiISAdjNbrExtendedCircID
- ciiISAdjUsage
- ciiISAdjHoldTimer
- ciiIsAdjNeighPriority
- ciiISAdjLastUpTime

Note The ciiISAdjChanges MIB object gathers information based on the best priority level that is selected among the configured objects, per the restriction against the software support of multiple adjacencies in a LAN for the ciiISAdjEntry table.

- The ciiISAdjNeighPriority MIB object gathers information based on the best priority level that is selected among the configured objects, per the restriction against the software support of multiple adjacencies in a LAN for the ciiISAdjEntry table.

The ciiISAdjAreaAddrEntry table contains entries for the sets of area addresses of neighboring ISs as reported in received IS-IS Hello protocol data units (PDU)s. The ciiISAdjAreaAddrEntry table defines the following MIB objects:

- ciiISAdjAreaAddrIndex
- ciiISAdjAreaAddress

The ciiISAdjIPAddrEntry table contains entries that are formed by a set of IP addresses of neighboring ISs as reported in received Hello PDUs. The ciiISAdjIPAddrEntry table defines the following MIB objects:

- ciiISAdjIPAddrIndex
- ciiISAdjIPAddrType
- ciiISAdjIPAddrAddress

The ciiISAdjProtSuppEntry table contains information about the protocols supported by neighboring ISs as reported in received Hello PDUs. The ciiISAdjProtSuppEntry table defines the following MIB object:

- ciiISAdjProtSuppProtocol

The ciiRAEntry table records information about a reachable NSAP or address prefix that is manually configured or learned dynamically.

The ciiRAEntry table defines the following MIB objects:

- ciiRAIndex
- ciiRAExistState
- ciiRAAdminState
- ciiRAAddrPrefix
- ciiRAMapType
- ciiRAMetric
- ciiRAMetricType
- ciiRASNPAAddress
- ciiRASNPAMask
- ciiRASNPAPrefix
- ciiRAType

Note The ciiRAMapType MIB Object supports only implicit (null) and explicit mapping types. The extractIDI and extractDSP types are not supported.

- Because the ciiRAMapType MIB Object does not support the extractIDI and extractDSP mapping types, the ciiraSNPAPrefix and ciiRASNPAMask MIB objects will hold no data, as they depend on the unsupported mapping types. The ciiRAMapType and ciiRASNPAMask MIB objects are not implemented.
- The ciiRAType MIB object does not support the manual creation of IP reachability addresses.

Each entry in the ciiIPRAEntry table records information about one IP reachable address manually configured on the IS or learned from another protocol. The ciiIPRAEntry table defines the following MIB objects:

- ciiIPRADestType
- ciiIPRADest
- ciiIPRADestPrefixLen
- ciiIPRANextHopIndex
- ciiIPRANextHopType
- ciiIPRANextHop
- ciiIPRAType
- ciiIPRAExistState
- ciiIPRAAdminState
- ciiIPRAMetric
- ciiIPRAMetricType
- ciiIPRAFullMetric
- ciiIPRASNPAAddress
- ciiIPRASourceType

Note The ciiIpRAType MIB object does not support manually created IP reachability addresses.

The ciiLSPSummaryEntry table (LSP Summary Table) provides LSP summary information.

The ciiLSPSummaryEntry table defines the following MIB objects:

- ciiLSPLevel
- ciiLSPID
- ciiLSPSeq
- ciiLSPZeroLife
- ciiLSPChecksum
- ciiLSPLifetimeRemain
- ciiLSPPDULength
- ciiLSPAttributes

The ciiLSPTLVEntry table provides a complete record of all LSPs as a sequence of {Type, Length, Value} tuples. The ciiLSPTLVEntry table defines the following MIB objects:

- ciiLSPTLVIndex
- ciiLSPTLVSeq
- ciiLSPTLVChecksum
- ciiLSPTLVType
- ciiLSPTLVLen
- ciiLSPTLVValue

Fields that are required for notifications are recorded in the ciiNotificationEntry table. The ciiNotificationEntry table is not meant for query since the MAX-ACCESS clause of the MIB objects is "accessible-for-notify." The information for notifications will be directly provided at the time of event generation. The following MIB objects are used only in trap notifications where their value is determined and directly based on input parameters for the IS-IS trap generation process.

- ciiPduLspId
- ciiPduFragment
- ciiPduFieldLen
- ciiPduMaxAreaAddress
- ciiPduProtocolVersion
- ciiPduLspSize
- ciiPduOriginatingBufferSize
- ciiPduProtocolsSupported
- ciiAdjState
- ciiErrorOffset
- ciiErrorTLVType
- ciiNotifManualAddress
- ciiNotifIsLevelIndex

Note The MIB objects ciiNotifManualAddress and ciiNotifIsLevelIndex were added separately and are not defined in draft-ietf-isis-wg-mib-16.txt. These have been provided as a replacement for ciiManAreaAddr and ciiSysLevelIndex respectively to be used only in trap notifications. They have a MAX-ACCESS clause of "accessible-for-notify."

Cisco IS-IS MIB Trap Notifications

IS-IS MIB for Generic System-Wide Errors

The following MIB trap objects are for generic, system-wide errors that can occur in the IS-IS network:

- ciiManualAddressDrops--The ciiManualAddressDrops trap is generated when one of the manually configured area addresses assigned to the system is ignored while computing routes.
- ciiAuthenticationFailure--The ciiAuthenticationFailure trap is generated when the authenticating type information field in the PDU received from a circuit is incorrect. This is an edge-triggered notification.
- ciiIDLenMismatch--When an LSP with a different value of SystemID length is received, the ciiIDLenMismatch notification is generated specific to the circuit where the LSP was detected. This is an edge-triggered notification and hence will be generated only once for PDUs received on the same circuit.
- ciiMaxAreaAddressesMismatch--When the value of Maximum Area Addresses is changed in the LSP that is received from a circuit, the ciiMaxAreaAddressesMismatch trap notification is generated. The header of the packet is used to identify the cause of the mismatch in Maximum Area Address. This trap is an edge-triggered notification and hence will be generated only once for PDUs received on the same circuit.

IS-IS MIB for LSP-Specific Errors

The following MIB trap objects are for LSP-specific errors that can occur in the IS-IS network:

- ciiCorruptedLSPDetected--When an LSP stored in memory is corrupted, the ciiCorruptedLSPDetected trap is generated.
- ciiAttemptToExceedMaxSequence--The ciiAttemptToExceedMaxSequence trap is generated each time a sequence number on a generated LSP wraps around the 32-bit sequence counter, forcing it to be purged and hence waiting for its reannouncement.
- ciiOwnLSPPurge--The ciiOwnLSPPurge trap is generated when a LSP is received from a circuit with your systemID and zero age.
- ciiSequenceNumberSkip--When an LSP is received without a SystemID or differing contents, the ciiSequenceNumberSkip trap is generated in order to increment the sequence number by 1.
- ciiAuthenticationTypeFailure--When an LSP is received from a circuit filled with a wrong authentication type field, the ciiAuthenticationTypeFailure notification is generated. This is an edge-triggered notification.
- ciiLSPTooLargeToPropagate--When an attempt is made to send an LSP over the circuit with a size greater than dataLinkBlockSize (link-specific parameter for maximum size of a data packet), the

ciiLSPTooLargeToPropagate trap is generated indicating that the LSP could not be propagated. This is an edge-triggered notification and will be generated only once for all PDUs received on the same circuit.

Note Cisco IOS software does not support the condition that leads to this event. Therefore, this trap will not be generated.

- ciiOrigLSPBuffSizeMismatch--When an L1 or L2 LSP that has been received from a circuit has a size larger than the local value of ciiOriginatingBufferSize, or when an LSP has been received with the ciiOriginatingBufferSize option and there is a mismatch between local ciiOriginatingBufferSize and value of the PDU option field, this notification is generated. This is an edge-triggered notification and will be generated only once.

Note The originating buffer size TLV that is used to advertise this condition is not currently supported in Cisco IOS software and sufficient information to determine which condition caused the trap is not available. Therefore, this trap will not be generated.

- ciiProtocolsSupportedMismatch--The ciiProtocolsSupportedMismatch trap is generated when a non-pseudonode segment 0 LSP is received that does not have any matching protocols supported. This is an edge-triggered notification.

Note Cisco IOS software does not provide checks in the IS-IS implementation for detecting matching protocols in the case of received PDUs. The generation of the ciiProtocolsSupportedMismatch trap does not indicate a mismatch in protocols supported as specified in the protocol field of the received PDU.

- ciiLSPErrorDetected--The ciiLSPErrorDetected trap is generated to indicate that an LSP with a parse error has been received.

MIB Support for IS-IS Hello PDU-Specific Errors

The following MIB trap objects are for Hello PDU-specific errors that can occur in the IS-IS network:

- ciiVersionSkew--The ciiVersionSkew trap notification is generated when a Hello PDU is received from an IS running a different version of the IS-IS protocol. This is an edge-triggered notification and will be generated once for all PDUs received on the same circuit.
- ciiAreaMismatch--When a Hello PDU is received from an IS that does not share any area address, the ciiAreaMismatch notification is generated. This is an edge-triggered notification and will be generated only once for all PDUs received on the same circuit.
- ciiRejectedAdjacency--When a correct Hello PDU is received from an IS but adjacency is not established, the ciiRejectedAdjacency notification is generated to indicate that adjacency formation was not allowed. This is an edge-triggered notification.

You can enable SNMP notifications to be sent when IS-IS errors and mismatches related to invalid field values in PDUs are detected. Errors can be classified as generic (applied to all PDUs), LPS-related, and IS-IS Hello PDU-related. When you enter the **snmp-server enable traps isis errors** command without specifying any of the optional keywords and arguments, all IS-IS traps are enabled. You can enter specific

keywords and arguments to enable certain traps. For more information on how to enable specific traps or groups of traps, refer to the **snmp-server enable traps isis**command page.

You can enable IS-IS traps for the following system-wide errors that apply to all PDUs:

- Authentication
- Authentication type
- System ID field length mismatch
- Manually-configured address drop
- Mismatch in maximum area address values

You can enable IS-IS traps for the following errors that apply specifically to IS-IS Hello PDUs:

- Adjacency creation failure
- Mismatch in the area addresses between ISs
- IS-IS protocol version mismatch

You can enable IS-IS traps for the following errors that apply specifically to LSPs:

- Mismatch in LSP and originating buffer size
- Attempt made to exceed a maximum sequence number
- LSP in-memory corruption with an invalid checksum
- Packet parse failure on a receiving circuit
- Protocol-supported mismatch for non-pseudonode LSP
- Invalid attempt to purge a the LSP of a local IS
- Propagation failure caused by an oversized LSP
- A system ID has been configured with a sequence number skip.

MIB Support for IS-IS Transition State Changes

The following MIB trap objects are used to notify the network manager when a transition state change has occurred for an IS:

- ciiDatabaseOverload--The ciiDatabaseOverload trap object is used to notify the network manager when the system enters or leaves the Overload state.
- ciiAdjacencyChange--When an IS-IS adjacency changes its state to UP or moves out of this state, it causes the ciiAdjacencyChange trap notification to be generated.

How to Enable IS-IS MIB

Configuring the Router to Send SNMP Notifications for IS-IS to a Host

SNMP must be enabled on your network.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth**| **priv**]}] *community-string* [**upd-port** *port*] [*notification-type*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration to determine if an SNMP agent is already running. • If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth**| **priv**]}] *community-string* [**upd-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 172.16.1.1 traps version 3 mycommunitystring isis`	Specifies the recipient (target host) for IS-IS SNMP notification operations. • If no *notification-type* is specified, all enabled notifications (traps or informs) will be sent to a specified host. If you want to send only IS-IS notifications to the specified host, you can use the optional **isis** keyword as the value for the *notification-type* argument. (See the example.)
Step 5	**end** **Example:** `Router(config)# end`	Ends your configuration sessions and exits global configuration mode.

Examples

The following example configures the router to send SNMP notifications for IS-IS to a host:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host 172.31.1.1 traps version 3 mycommunity string isis
```

- What to Do Next, page 57

What to Do Next

To globally enable all IS-IS traps, refer to the Enabling All IS-IS Traps, page 57. To enable groups of IS-IS traps, refer to the Enabling IS-IS Error Traps, page 59 and the Enabling IS-IS State-Change Traps, page 60.

Enabling All IS-IS Traps

SNMP notifications can be configured only after MIB support is enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps isis**
4. **no snmp-server enable traps isis** [**errors** [*error-type*]] [**state-change** [*state-change-type*]]
5. **exit**
6. **show running-config** [*options*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **snmp-server enable traps isis** **Example:** `Router(config)# snmp-server enable traps isis`	Enables all SNMP notifications defined in the IS-IS MIB. **Note** This step is required only if you wish to enable all IS-IS traps. To enable specific groups of traps, see the Enabling IS-IS Error Traps, page 59 or the Enabling IS-IS State-Change Traps, page 60. When you enter the **no snmp-server enable traps isis** command, all IS-IS traps will be disabled.
Step 4 **no snmp-server enable traps isis** [**errors** [*error-type*]] [**state-change** [*state-change-type*]] **Example:** `Router(config)# no snmp-server enable traps isis state-change database-overload`	Disables the sending of SNMP notifications for IS-IS state changes. **Note** This step is required only if you wish to disable a particular trap or set of traps. To enable specific groups of traps, see the Enabling IS-IS Error Traps, page 59 or the Enabling IS-IS State-Change Traps, page 60.
Step 5 **exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 6 **show running-config** [*options*] **Example:** `Router# show running-config | include traps`	Displays the running configuration to verify which traps have been enabled.

Examples

The following example shows how to globally enable all IS-IS traps:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps isis
```

- What to Do Next, page 58

What to Do Next

To enable some but not all IS-IS traps, refer to Enabling IS-IS Error Traps, page 59. To enable one or more IS-IS state-change traps, refer to Enabling IS-IS State-Change Traps, page 60.

Enabling IS-IS Error Traps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps isis** [**errors** [*error-type*]] [**state-change** [*state-change-type*]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps isis** [**errors** [*error-type*]] [**state-change** [*state-change-type*]] **Example:** `Router(config)# snmp-server enable traps isis errors lsp`	Enables SNMP notifications for IS-IS errors. • When you enter the **lsp** keyword for the *error-type*, only the LSP error traps are enabled. (See the **snmp-server enable traps isis** command in the *Cisco IOS IP Routing: ISIS Command Reference* for a list of *error-type* keywords.)
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration sessions and exits global configuration mode.

Examples

The following example shows how to enable only the IS-IS traps related to authentication errors:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps isis errors authentication
```

Enabling IS-IS State-Change Traps

You can enable SNMP notifications to be sent when significant IS-IS state changes occur in the system. Perform this task to enable the IS-IS trap MIB objects cliiDatabaseOverload and ciiAdjacencyChange.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps isis** [**state-change** [*state-change-type*]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps isis** [**state-change** [*state-change-type*]] **Example:** `Router(config)# snmp-server enable traps isis state-change`	Enables SNMP notifications for IS-IS state changes. **Note** When the **snmp-server enable traps isis state-change**command is entered without any of the optional keywords, both IS-IS state change traps are enabled. Entering the **no snmp-server enable traps isis state-change**command will disable both IS-IS state-change traps.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration sessions and exits global configuration mode.

Examples

The following example shows how to enable only the IS-IS traps related to adjacency transition state changes:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps isis state-change adjacency
```

Verifying IS-IS MIB Traps on the Router

SUMMARY STEPS

1. **enable**
2. **show running-config** [*options*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** [*options*] **Example:** `Router# show running-config | include traps`	Displays the contents of the currently running configuration file and includes information about enabled traps. • Verifies if the traps have been enabled.

Configuration Examples for IS-IS MIB

Example Enabling and Verifying IS-IS Error Traps

The following example enables all IS-IS error traps:

```
Router(config)# snmp-server enable traps isis
Router# end
```

The **show running-config** command is entered to verify that the traps are enabled:

```
Router# show running-config | include traps
snmp-server enable traps isis
```

Example Enabling and Verifying IS-IS State Change Traps

The following example shows how to enable the ciiDatabaseOverload and ciiManualAddressDrops traps:

```
Router(config)# snmp-server enable traps isis state-change database-overload
Router(config)# snmp-server enable traps isis errors manual-address-drop
Router(config)# end
```

The **show running-config** command is entered to verify that these traps are enabled:

```
Router# show running-config | include traps
snmp-server enable traps isis state-change database-overload
snmp-server enable traps isis errors manual-address-drop
```

Where to Go Next

For more information about SNMP and SNMP operations, refer to the "Configuring SNMP Support" section of the *Cisco IOS Network Management Configuration Guide*.

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module
SNMP configuration	"Configuring SNMP Support" section of the *Cisco IOS Network Management Configuration Guide*
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
CISCO-IETF-ISIS-MIB.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
IETF draft draft-ietf-isis-wg-mib-16.txt	*Management Information Base for IS-IS*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IS-IS MIB

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

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

Table 3 Feature Information for IS-IS MIB

Feature Name	Releases	Feature Information
IS-IS MIB	12.2(25)SG 12.2(31)SB2 12.2(33)SRB 12.2(31)SB3 15.0(1)M	This feature introduces MIB support for the Intermediate System-to-Intermediate System (IS-IS) link-state routing protocol. IS-IS is used as the link-state routing protocol of choice by major service providers. The IS-IS MIB feature offers service providers an improved capability to continuously monitor the changing state of an IS-IS network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant protocol events such as an authentication failure or a mismatch in area addresses between Intermediate Systems (ISs). The protocol information collected by the IS-IS MIB objects and trap objects can be used by the network manager to derive statistics that can help monitor and improve overall network performance. In 12.2(31)SB2, this feature was implemented on the Cisco 7000 series routers. In 12.2(31)SB3, this feature was implemented on the Cisco 10000 series routers. The following commands were introduced or modified: **snmp-server enable traps isis, snmp-server host**

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

IS-IS Support for an IS-IS Instance per VRF for IP

This module introduces support for multiple VPN routing and forwarding (VRF)-aware Intermediate System-to-Intermediate System (IS-IS) instances. The VRF functionality allows Internet service providers (ISPs) to separate routing protocol information and propagate it to the appropriate routing table and network neighbors. Using one router with VRF functionality is more cost-effective than using separate routers to separate and forward the routing information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for IS-IS Support for an IS-IS Instance per VRF for IP

- You must be running IS-IS on your network.
- The VRF configuration is a prerequisite to associating an IS-IS instance with that specific VRF. However, the VRF configuration is independent of associating it with IS-IS or any other routing protocol. An IS-IS instance cannot be referred to as being VRF-aware until it has been associated with a particular VRF.

Restrictions for IS-IS Support for an IS-IS Instance per VRF for IP

IS-IS VRF support is supported only for IPv4.

When you configure the IS-IS Support for an IS-IS Instance per VRF for IP feature, you must comply with the following nine best practices guidelines:

- IS-IS instances running Connectionless Network Services (CLNS) must have the same system ID.
- An IS-IS instance that is running CLNS or IPv6 cannot be associated with a VRF.
- You can configure only one IS-IS instance to run both CLNS and IP.
- IS-IS instances within the same VRF must have unique system IDs, although IS-IS instances located in separate VRFs can have the same system ID.
- You can associate an IS-IS instance with only one VRF.
- You can configure the **passive-interface default** command only on one IS-IS instance per VRF.
- Redistribution is allowed only within the same VRF.
- You can enable only one IS-IS instance per interface.
- An interface can belong to an IS-IS instance only if they are associated with the same VRF.

Note If you are using LDP, you cannot use the **route-target** command when configuring a VRF. The router will use BGP for Multiprotocol Label Switching (MPLS) labels.

Information About IS-IS Support for an IS-IS Instance per VRF for IP

VRF-Aware IS-IS

You can configure IS-IS to be VRF-aware. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

IS-IS Support for an IS-IS Instance per VRF for IP Feature Operation

ISPs have the capability to create multiple VRF-aware IS-IS instances that run on one router, rather than requiring duplicate hardware. IS-IS can be enabled to be VRF-aware, and ISPs can use multiple VRF-aware IS-IS instances to separate customer data while propagating the information to appropriate service providers.

For example, an ISP can create three VRFs--VRF First, VRF Second, and VRF Third--to represent three separate customers. A VRF-aware IS-IS instance is created and associated with each VRF: tagFIRST,

tagSECOND, and tagTHIRD. Each instance will have its own routing process, IS-IS database, and routing table, and will calculate its own shortest path first (SPF) tree.

How to Configure IS-IS Support for an IS-IS Instance per VRF for IP

Creating a VRF

- You must have IS-IS running on your network.
- If CEF is not enabled by default on your platform, enable CEF to associate interfaces with VRF-aware IS-IS instances.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip cef** [**distributed**] **Example:** `Router(config)# ip cef distributed`	(Optional) Enables CEF on the Route Processor card. • If CEF is not enabled by default on your particular platform, you must configure it with the **ip cef** command.
Step 4	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf vrfFirst`	Configures a VRF routing table, and enters VRF configuration mode.
Step 5	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 1:1`	Creates routing and forwarding tables for a VRF.
Step 6	**end** **Example:** `Router(config-vrf)# end`	Exits VRF configuration mode and returns to privileged EXEC mode.

Attaching an Interface to the VRF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/2`	Configures an interface type and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding vrfFirst`	Associates a VPN routing and forwarding instance (VRF) with an interface or subinterface.

Creating VRF Aware IS-IS Instances

Prerequisites

Before creating VRF-aware IS-IS instances, enable IP routing on the router.

Note Only one instance within the VRF can be configured as the passive interface default.

Creating a VRF-Aware IS-IS Instance in Interface Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [*secondary*]
5. **ip router isis** *process-tag*
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/2`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [*secondary*] **Example:** `Router(config-if)# ip address 172.16.11.1 255.255.255.255`	Sets a primary or secondary IP address for an interface.
Step 5	**ip router isis** *process-tag* **Example:** `Router(config-if)# ip router isis vrfFirst`	Configures an IS-IS routing process for IP on an interface and attaches a tag to the routing process. **Note** The configuration of the interface-mode **ip router isis** command will overwrite the prior configuration on that interface, but only if the new configuration is attempting to change the interface ownership to a different instance that is in the same VRF as the currently configured owner instance. The configuration will be rejected if the attempted change is between two instances that are associated with different VRFs.
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Restarts a disabled interface.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Creating a VRF-Aware IS-IS Instance in Router Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *process-tag*
4. **vrf** *vrf-name*
5. **net** *network-entity-title*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *process-tag* **Example:** `Router(config)# router isis tagFirst`	Enables the IS-IS routing protocol, specifies an IS-IS process, and enters router configuration mode.
Step 4	**vrf** *vrf-name* **Example:** `Router(config-router)# vrf vrfFirst`	Associates an IS-IS instance with a VRF. • It is presumed that the VRF named vrfFirst was previously created.

	Command or Action	Purpose

Step 5	**net** *network-entity-title*
	
	Example:
	
	`Router(config-router)# net 49.000b.`
	`0000.0001.0002.00`
		Configures an IS-IS NET for a CLNS routing process.

Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for IS-IS Support for an IS-IS Instance per VRF for IP

Example Configuring Multiple VRF-Aware IS-IS Instances

In the following example, the VRF Second is created and an IS-IS instance is created explicitly by entering the **router isis** command on the router:

```
Router(config)# ip cef distributed
Router(config)# ip routing
Router(config)# ip vrf Second
Router(config-vrf)# rd 1:1
Router(config-if)# router isis tagSecond
Router(config-router)# vrf Second
Router(config-router)# net 49.000b.0000.0001.0002.00
```

The VRF Third is created and a VRF-aware IS-IS instance is automatically created when the **ip router isis** command is entered:

```
Router(config)# ip vrf Third
Router(config-vrf)# rd 1:1
Router(config-if)# interface FastEthernet0/2
Router(config-if)# ip vrf forwarding Third
Router(config-if)# ip address 172.16.10.1 255.255.255.0
Router(config-if)# ip router isis tagThird
Router(config-if)# no shutdown
```

A new IS-IS instance with the process tag tagThird will automatically be created and associated with the VRF Third. When the **show running-config** command is entered, the following information for the new IS-IS instance will be displayed:

```
Router# show running-config
Building configuration...
router isis tagThird
 vrf Third
Router(config)# router isis tagThird
Router(config-router)# net 49.000b.0000.0001.0001.00
```

The following sample output verifies information for the VRF-aware IS-IS instances that were created in the previous examples:

```
Router# show isis tagThird topology
Tag tagThird:
IS-IS paths to level-2 routers
System Id             Metric  Next-Hop               Interface   SNPA
router-02             10      router-02              Fa4/3       0010.0ddc.e00b
router-03             10      router-03              Et0/2       0006.0e03.0c45
router-04             10      router-04              Fa4/0       000a.f3c3.1c70
.                             router-04              Fa4/1       000a.f3c3.1c71
.
.
.
Router# show clns tagSecond neighbors
Tag tagSecond:
System Id      Interface   SNPA                State  Holdtime  Type Protocol
router-03      Fa0/2       00d0.2b7f.9502      Up     9         L2   IS-IS
router-03      PO2/2.1     DLCI 211            Up     27        L2   IS-IS
router-02      PO2/0.1     DLCI 131            Up     29        L2   IS-IS
router-11      Fa0/4       000e.d79d.7920      Up     7         L2   IS-IS
router-11      Fa0/5       000e.d79d.7921      Up     8         L2   IS-IS
router-11      PO3/2.1     DLCI 451            Up     24        L2   IS-IS
.
.
.
Router# show isis tagThird database level-2
Tag tagThird:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
router-01.00-00       0x0000000A    0x5E73       914               0/0/0
router-01.03-00       0x00000001    0x8E41       894               0/0/0
router-01.04-00       0x00000001    0x8747       894               0/0/0
router-03.00-00     * 0x00000005    0x55AD       727               0/0/0
router-03.02-00     * 0x00000001    0x3B97       727               0/0/0
router-02.00-00       0x00000004    0xC1FB       993               0/0/0
router-02.01-00       0x00000001    0x448D       814               0/0/0
router-04.00-00       0x00000004    0x76D0       892               0/0/0
Router# show isis tagThird database level-1
Tag tagThird:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
router-03.00-00     * 0x0000000B   0xBDF6        1005              1/0/0
router-03.02-00     * 0x00000001   0xC473        940               0/0/0
router-07.00-00       0x00000006   0x403A        940               0/0/0
Router# show clns tagSecond protocol
IS-IS Router: tagSecond
  System Id: 0000.0001.0002.00  IS-Type: level-2-only
  Manual area address(es):
        49.000b
  Routing for area address(es):
        49.000b
  Interfaces supported by IS-IS:
        FastEthernet4/1 - IP
        FastEthernet4/0 - IP
        Ethernet0/2 - IP
        FastEthernet4/3 - IP
  Redistributing:
    static
  Distance: 110
```

```
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
Router# show clns tagThird protocol
IS-IS Router: tagThird
  System Id: 0000.0001.0001.00  IS-Type: level-1-2
  Manual area address(es):
        49.000b
  Routing for area address(es):
        49.000b
  Interfaces supported by IS-IS:
        POS2/2.1 - IP
        FastEthernet0/2 - IP
        FastEthernet0/4 - IP
        POS2/0.1 - IP
        FastEthernet0/5 - IP
        POS3/2.1 - IP
  Redistributing:
    static
  Distance: 110
  RRR level: none
  Generate narrow metrics: none
  Accept narrow metrics:   none
  Generate wide metrics:   level-1-2
  Accept wide metrics:     level-1-2
```

Example Creating an IS-IS Instance Without a Process Tag

In the following example, an IS-IS instance was created without the optional process tag. When an IS-IS instance is created without the optional process tag, you can display its information by entering the commands such as **show clns protocol** with "null" specified for the *process-tag* argument.

```
Router(config)# router isis
Router(config-router)# vrf first
Router(config-router)# net 49.000b.0000.0001.ffff.00
Router(config-router)# is-type level-1
Router(config)# interface POS 6/1
Router(config-if)# ip vrf forwarding first
Router(config-if)# ip address 172.16.2.1 255.255.255.0
Router(config-if)# ip router isis
Router(config-if)# no shutdown
```

Because the IS-IS instance is created without the optional process tag, its information is displayed when the **show clns protocol** command is entered with "**null" specified for the** *process-tag* **argument**:

```
Router# show clns null protocol
IS-IS Router: <Null Tag>
  System Id: 0000.0001.FFFF.00  IS-Type: level-1
  Manual area address(es):
        49.000b
  Routing for area address(es):
        49.000b
  Interfaces supported by IS-IS:
        POS6/1 - IP
  Redistributing:
    static
  Distance: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
```

Example Redistributing Routes from an IS-IS Instance

In the following sample configuration, routes have been redistributed from the IS-IS instance "null" into the IS-IS instance named tagBLUE. Routes from an OSPF process in VRF Blue have been redistributed into the IS-IS instance named tagBLUE.

```
Router(config)# router isis tagBLUE
Router(config-router)# redistribute isis null ip metric 10 route-map isisMAP1
Router(config-router)# redistribute ospf 1 vrf BLUE metric 1 metric-type external
level-1-2
.
.
.
Router(config)# route-map isisMAP1 permit 10
Router(config-route-map)# match route-type level-2 level-1
Router(config-route-map)# set level level-2
```

Example Changing the Interface Ownership

In the following sample configuration, POS interface 6/1 was originally enabled for IS-IS IP routing for a "null" instance that does not have a process tag, which is in vrfSecond. The new configuration changes the ownership of POS interface 6/1 to another instance tagSecond, which is also in vrfSecond.

Note Use of the **ip router isis**command in interface configuration mode will overwrite the prior configuration on that interface, but only if the new configuration is attempting to change the interface ownership to a different instance that is in the same VRF as the currently configured owner instance. The configuration will be rejected if the attempted change is between two instances that are associated with different VRFs.

```
Router(config)# interface POS 6/1
Router(config-if)# ip router isis tagSecond
%ISIS: Interface detached from null and to be attached to instance tagSecond.
```

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module
ISO CLNS commands	*Cisco IOS ISO CLNS Command Reference*
Command Lookup Tool	http://tools.cisco.com/Support/CLILookup

Standards

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

MIBs

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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IS-IS Support for an IS-IS Instance per VRF for IP

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

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

Table 4 Feature Information for IS-IS Support for an IS-IS Instance per VRF for IP

Feature Name	Releases	Feature Information
IS-IS Support for an IS-IS Instance per VRF for IP	12.0(29)S 12.2(33)SRB 15.0(1)M	This feature provides multiple VPN routing and forwarding (VRF)-aware Intermediate System-to-Intermediate System (IS-IS) instances. The VRF functionality allows Internet service providers (ISPs) to separate routing protocol information and propagate it to the appropriate routing table and network neighbors. Using one router with VRF functionality is more cost-effective than using separate routers to separate and forward the routing information. The following commands were introduced or modified: **show clns neighbors**, **show clns protocol**, **show isis database**, **show isis topology**, and **vrf (router configuration)**.

Overview of IS-IS Fast Convergence

This module provides information about the topics of Intermediate System-to-Intermediate System (IS-IS) fast convergence. The tasks in the modules that follow this overview can help you improve convergence times for IS-IS networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for IS-IS Fast Convergence

You should be familiar with the concepts described in the "Integrated IS-IS Routing Protocol Overview" module.

Information About IS-IS Fast Convergence

Network Convergence

Convergence is the process of all routers coming to agreement on optimal routes in a network. When a network event causes routes to become available or unavailable, routers send routing update messages through the network that cause routing algorithms to recalculate optimal routes. Eventually all the routers agree on the routes as well as the network topology. Fast convergence benefits network performance.

Routing algorithms that converge slowly may cause temporary routing loops or temporary network unavailability.

The process of network convergence can be divided into three separate stages:

1. Routing change detection: The speed at which a device on the network can detect and react to the failure or modification of one of its own components, or to a topology change caused by the failure or modification of a component on a routing protocol peer.
2. Routing change notification: The speed at which the failure or topology change in the previous stage can be communicated to other devices in the network.
3. Alternate path calculation: The speed at which all devices on the network, having been notified of the failure or topology change, can process the information and calculate an alternate path through which data can flow.

An improvement in any one of these stages provides an improvement in overall convergence. In addition to a basic configuration task that is recommended as a first step in configuring an IS-IS router with best practice parameters for achieving fast convergence, several recommended configuration tasks are grouped according to the stage of network convergence they can improve. For more information, see the following modules:

- "Setting Best Practice Parameters for IS-IS Fast Convergence"
- "Reducing Failure Detection Times in IS-IS Networks"
- "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"
- "Reducing Alternate-Path Calculation Times in IS-IS Networks"

Design Recommendations for Achieving Faster Network Convergence

A faster processor can provide better performance for network convergence.

On some Cisco routers such as the Cisco 12000, 10000, 7600 and 6500 series Internet routers, the control-plane and forwarding-plane are separated. Tasks associated with network convergence such as shortest path first (SPF) calculation, routing table updates, and server functions for information distribution to line cards are supported separately from packet forwarding tasks. By leveraging the separated control-plane CPU, network convergence tasks are handled more efficiently.

Note For the Cisco 12000 series Internet routers, we recommend that you when you configure the **process-max-time** command, do not use a value lower than 60 milliseconds.

Where to Go Next

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

- "Setting Best Practice Parameters for IS-IS Fast Convergence"
- "Reducing Failure Detection Times in IS-IS Networks"
- "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"
- "Reducing Alternate-Path Calculation Times in IS-IS Networks"

To enhance IS-IS network security, see the "Enhancing Security in an IS-IS Network" module.

Additional References

Related Documents

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

Standards

Standard	Title
ISO 8473	CLNP, Connectionless Network Protocol
ISO 9542	*ES-IS Routing Information Exchange Protocol*
ISO/IEC 10589	IS-IS Protocol

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Setting Best Practice Parameters for IS-IS Fast Convergence

This module describes how to configure an IS-IS router with parameters that are recommended as a basic step to improve network convergence.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Setting Best Practice Parameters for IS-IS Fast Convergence

- It is assumed you already have IS-IS running on your network.
- Before performing the tasks in this module, you should be familiar with the concepts described in the "Overview of IS-IS Fast Convergence" module.

Information About Setting Best Practice Parameters for IS-IS Fast Convergence

To minimize the number of adjacencies, LSDBs, and related SPF and PRC computations that are performed, it is recommended that you have configured all Level 1 routers as Level 1 by using the **is-type** command. We recommend that you use the **metric-style wide** command because some features, such as setting prefix tags and MPLS traffic engineering, require that routers that are running IS-IS generate the new-style TLVs that have wider metric fields. If you use the default narrow metric style for IS-IS, the router generates and accepts old-style type, length, and value objects (TLVs).

- General Steps for Improving Convergence Time in the IS-IS Network, page 86

General Steps for Improving Convergence Time in the IS-IS Network

The process described in this module consists of configuration commands that are recommended as general first steps for improving convergence time in any IS-IS network. Performing the steps in the following process can help you save network resources and speed up network convergence.

How to Set Best Practice Parameters for IS-IS Fast Convergence

- Setting Best Practice Parameters for IS-IS Fast Convergence, page 86

Setting Best Practice Parameters for IS-IS Fast Convergence

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [area-** *tag* **]**
4. **is-type** [**level-1** | **level-1-2** | **level-2-only**]
5. **metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**]
6. **set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] [**suppress** {**interlevel**| **external**}]
7. **no hello padding**
8. **end**
9. **show clns** [*domain* | *area-tag*] **protocol**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**is-type** [**level-1** | **level-1-2** | **level-2-only**] **Example:** `Router(config-router)# is-type level-1`	Configures the routing level for an instance of the IS-IS routing process. • It is recommended that IS-IS nodes that operate at a single level be configured as Level 1 to minimize the number of adjacencies, LDSBs, and related SPF and PRC calculations. **Note** You can also set the IS-IS level type on the interface by entering the **isis circuit-type** command.
Step 5	**metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**] **Example:** `Router(config-router)# metric-style wide`	Globally changes the metric value for all IS-IS interfaces. • Wide style metrics are required for prefix tagging.
Step 6	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] [**suppress** {**interlevel**| **external**}] **Example:** `Router(config-router)# set-overload-bit on-startup 360`	Configures the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations. • Setting the overload bit gives the router enough time to build its BGP and CEF tables prior to the router being used as a transit node.

	Command or Action	Purpose
Step 7	**no hello padding** **Example:** `Router(config-router)# no hello padding`	Disables IS-IS hello padding at the router level. • By default the IS-IS Hello PDUs are padded to the full MTU size, possibly having a negative impact on time-sensitive application traffic that travels across low-bandwidth interfaces or on interface buffer resources when frequent hellos are configured. It is recommended to globally disable hello padding.
Step 8	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 9	**show clns** [*domain* | *area-tag*] **protocol** **Example:** `Router(config-if)# show clns protocol`	Lists the protocol-specific information for each ISO IGRP or IS-IS routing process in the router.

Configuration Examples for Setting Best Practice Parameters for IS-IS Fast Convergence

Example Enabling IS-IS on a Router and Setting Best Practice Parameters for IS-IS Fast Convergence

The following example enables the IS-IS routing protocol on the interfaces for Router A, enables IS-IS on Router A, and configures Router A with the basic commands recommended to optimize IS-IS network convergence.

Router A

```
!
clns routing
process-max-time 50
ip routing protocol purge interface
router isis
 passive-interface Loopback0
 net 49.1962.XXXX.XXXX.XXXX.00
 is-type level-2-only
 ispf level-2
 log-adjacency-changes
 ignore-lsp-errors
 metric-style wide level-2
```

```
 external overload signalling !Configure on Cisco 12000 series Internet routers
 set-overload-bit on-startup 180
 max-lsp-lifetime 65535
 lsp-refresh-interval 65000
 spf-interval 5 1 50
 prc-interval 5 1 50
 lsp-gen-interval 5 1 50
 no hello padding
 authentication mode md5 level-2
 authentication key-chain ON
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
interface GigabitEthernet x/x
 negotiation auto
 ip router isis
 mtu 4470
 isis network point-to-point
 isis metric <metric> level-2
 isis circuit-type level-2-only
 isis authentication mode md5 level-2
 isis authentication key-chain ON
 carrier-delay ms 0
 dampening
interface POSx/y
 carrier-delay msec 0
 dampening
 ip router isis
 no peer neighbor-route
 isis metric 1 level-2
 isis circuit-type level-2-only
 isis authentication mode md5 level-2
 isis authentication key-chain ON
 pos ais-shut
 pos report lais
 pos report lrdi
 pos report pais
 pos report prdi
 pos report slos
 pos report slof
!
key chain ON
 key 1
  key-string mypassword
```

Where to Go Next

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

- "Reducing Failure Detection Times in IS-IS Networks"
- "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"
- "Reducing Alternate-Path Calculation Times in IS-IS Networks"

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Setting Best Practice Parameters for IS-IS Fast Convergence

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

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

Table 5 Feature Information for Setting Best Practice Parameters for IS-IS Fast Convergence

Feature Name	Software Releases	Feature Information
This table is intentionally left blank because no features were introduced or modified in this module since Cisco IOS Release 12.2T. This table will be updated when feature information is added to this module.	--	--

Reducing Failure Detection Times in IS-IS Networks

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Reducing Failure Detection Times in IS-IS Networks

You should be familiar with the concepts described in the "Overview of IS-IS Fast Convergence" module.

Information About Reducing Failure Detection Times in IS-IS Networks

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.

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

"Bidirectional Forwarding Detection"

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

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

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

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

IP event dampening introduces a configurable exponential delay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping, removing it from the network until it becomes stable again. Thus, the network becomes more stable, with a faster convergence time.

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

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

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

- Importance of Fast Network Failure Detection, page 95

Importance of Fast Network Failure Detection

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

How to Reduce Failure Detection Times in IS-IS Networks

Using Bidirectional Forwarding Failure Detection to Decrease Failure Detection Times

Configuring BFD Session Parameters on the Interface

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 6/0`	Enters interface configuration mode. • Repeat this procedure for each interface over which you want to run BFD sessions to BFD neighbors.
Step 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`	Enables BFD on the interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Configuring BFD Support for IS-IS

Prerequisites

IS-IS must be running on all participating routers.

The baseline parameters for BFD sessions on the interfaces that you want to run BFD sessions to BFD neighbors over must be configured. See the Configuring BFD Session Parameters on the Interface, page 95 for more information.

Configuring BFD Support for IS-IS for All Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **bfd all-interfaces**
5. **exit**
6. **interface** *type number*
7. **isis bfd** [**disable**]
8. **end**
9. **show bfd neighbors** [**details**]
10. **show clns interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis tag1`	Specifies an IS-IS process and enters router configuration mode.
Step 4	**bfd all-interfaces** **Example:** `Router(config-router)# bfd all-interfaces`	Enables BFD globally on all interfaces associated with the IS-IS routing process.
Step 5	**exit** **Example:** `Router(config-router)# exit`	(Optional) Returns the router to global configuration mode. Enter this command only if you want to follow Step 6 and Step 7 to disable BFD for one or more interfaces.

	Command or Action	Purpose
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastethernet 6/0`	(Optional) Enters interface configuration mode.
Step 7	**isis bfd** [**disable**] **Example:** `Router(config-if)# isis bfd`	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. **Note** You should use the **disable** keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the **bfd all-interfaces** command in router configuration mode.
Step 8	**end** **Example:** `Router(config-if)# end`	Returns the router to privileged EXEC mode.
Step 9	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	Displays information that can be used to verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details**commandwhen it is entered on a line card.
Step 10	**show clns interface** **Example:** `Router# show clns interface`	Displays information that can be used to verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 6/0`	Enters interface configuration mode.
Step 4	**isis bfd** [**disable**] **Example:** `Router(config-if)# isis bfd`	Enables or disables BFD on a per-interface basis for one or more interfaces associated with the IS-IS routing process. **Note** You should use the **disable** keyword only if you enabled BFD on all of the interfaces that IS-IS is associated with using the **bfd all-interfaces** command in router configuration mode.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns the router to privileged EXEC mode.
Step 6	**show bfd neighbors** [**details**] **Example:** `Router# show bfd neighbors details`	Displays information that can help verify if the BFD neighbor is active and displays the routing protocols that BFD has registered. **Note** In order to display the full output of the **show bfd neighbors details** command on a Cisco 12000 series router, you must enter the command on the line card. Enter the **attach** *slot-number* command to establish a CLI session with a line card. The registered protocols are not shown in the output of the **show bfd neighbors details**commandwhen it is entered on a line card.

	Command or Action	Purpose
Step 7	**show clns interface** **Example:** `Router# show clns interface`	Displays information that can help verify if BFD for IS-IS has been enabled for a specific IS-IS interface that is associated.

Using IP Event Dampening to Decrease Failure Detection Times

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/1`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**dampening** [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress-time* [*restart-penalty*]] **Example:** `Router(config-if)# dampening`	Enables interface dampening. • Entering the **dampening** command without any keywords or arguments enables interface dampening with the default configuration parameters. **Note** The default values for the *half-life-period*, *reuse-threshold*, *suppress-threshold*, *max-suppress-time*, and *restart-penalty* arguments are 5, 1000, 2000, 20, and 2000, respectively. • When the timer for the *restart-penalty* argument is manually configured, the values must be manually entered for all arguments.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show dampening interface** **Example:** `Router# show dampening interface`	Displays a summary of dampened interfaces.
Step 7	**show interface dampening** **Example:** `Router# show interface dampening`	Displays dampened interfaces on the local router.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface Ethernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**isis hello-interval** {*seconds* | **minimal**} [**level-1** | **level-2**] **Example:** `Router(config-if)# isis hello-interval 5 level-1`	Specifies the length of time between the sending of IS-IS hello PDUs. • The default value is 10. The hello interval multiplied by the hello multiplier equals the hold time. If the minimal keyword is specified, the hold time is 1 second and the system computes the hello interval based on the hello multiplier. • The hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because only a single type of hello PDU is sent on serial links, it is independent of Level 1 or Level 2.) The level-1 and level-2 keywords are used on X.25, SMDS, and Frame Relay multiaccess networks or LAN interfaces. **Note** A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network, due to false failure detection events. A slower hello interval saves bandwidth and CPU. Especially when used in combination with a higher hello multiplier, this configuration may increase overall network stability, but has typical slower network convergence as a consequence.
Step 5	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**] **Example:** `Router(config-if)# isis hello-multiplier 6 level-1`	Specifies the number of IS-IS hello PDUs a neighbor must miss before the router should declare the adjacency as down. • The default value is 3. A multiplier value of 1 is very aggressive--we recommend a value of at least 3.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

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

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

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

>

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface Fastethernet 4/0`	Configures an interface type and enters interface configuration mode.
Step 4	**isis network point-to-point** **Example:** `Router(config-if)# isis network point-to-point`	Configures a network of only two networking devices that use broadcast media and the integrated IS-IS routing protocol to function as a point-to-point link instead of a broadcast link.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Monitoring IS-IS Network Convergence Time

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**isis display delimiter** [**return** *count* | **character** *count*] **Example:** `Router(config)# isis display delimiter return 2`	Makes output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Router# show isis database detail`	Displays the IS-IS link-state database.
Step 6	**show isis** [*process-tag*] **routes** **Example:** `Router# show isis financetag routes`	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	**show isis spf-log** **Example:** `Router# show isis spf-log`	Displays how often and why the router has run a full SPF calculation.

	Command or Action	Purpose
Step 8	**show isis** [*process-tag*] **topology** **Example:** `Router# show isis financetag topology`	Displays a list of all connected routers in all areas. • If a process tag is specified, output is limited to the specified routing process. When "null" is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.

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

Example Configuring BFD in an IS-IS Network

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

Configuration for Router A

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

Configuration for Router B

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

```
 bfd all-interfaces
!
```

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

```
Router A
RouterA# show bfd neighbors details

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.1   172.16.10.2    1/8  1   536  (3 )      Up        Fa0/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 1000, Received Multiplier: 3
Holdown (hits): 600(0), Hello (hits): 200(23543)
Rx Count: 13877, Rx Interval (ms) min/max/avg: 200/448/335 last: 64 ms ago
Tx Count: 23546, Tx Interval (ms) min/max/avg: 152/248/196 last: 32 ms ago
Registered protocols: ISIS
Uptime: 01:17:09
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 8          - Your Discr.: 1
             Min tx interval: 50000    - Min rx interval: 1000
             Min Echo interval: 0
```

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

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

```
Router B
RouterB# attach 6
Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
Press RETURN to get started!
LC-Slot6> show bfd neighbors details
Cleanup timer hits: 0
OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    8/1  1   1000 (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(5995)
Rx Count: 10126, Rx Interval (ms) min/max/avg: 152/248/196 last: 0 ms ago
Tx Count: 5998, Tx Interval (ms) min/max/avg: 204/440/332 last: 12 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 8
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 00:33:13
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 239103 min/max/avg: 8/16/8 last: 0 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
```

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

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

```
enable
configure terminal
interface Ethernet 0/0
 dampening 30 1500 10000 120
 isis hello-interval minimal
 isis hello-multiplier 3
```

Where to Go Next

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

- "Setting Best Practice Parameters for IS-IS Fast Convergence"
- "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"
- "Reducing Alternate-Path Calculation Times in IS-IS Networks"

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview"

Standards

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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

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

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

Table 6 Feature Information for Reducing Failure Detection Times in IS-IS Networks

Feature Name	Software Releases	Feature Information
IS-IS Support for BFD over IPv4	12.4(4)T	Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.
Integrated IS-IS Point-to-Point Adjacency over Broadcast Media	12.2(8)T Cisco IOS XE 3.1.0 SG	When a network consists of only two networking devices connected to broadcast media and uses the integrated IS-IS protocol, it is better for the system to handle the link as a point-to-point link instead of as a broadcast link. This feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices.

Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

The tasks in this module explain how to customize Intermediate System-to-Intermediate System (IS-IS) to reduce the amount of time required for routers to send link failure and topology change information to neighbors. You can adjust the IS-IS timers and thereby decrease the time required for a device to send routing updates.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

Before performing the tasks in this module, you should be familiar with the concepts described in the "Overview of IS-IS Fast Convergence" module.

Information About Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

IS-IS LSP Generation Interval and Lifetime

If you increase the link-state Protocol Data Unit (PDU) LSP tuning values to their maximum, flooding will be significantly reduced, as will resource consumption by the flooding mechanism. The maximum period a router is allowed to wait before regenerating its LSP is approximately 18.7 hours.

SPF, PRC, and LSP generation exponential backoff timers need to be tuned according to the level of stability of the network and the stability required in the routing domain. For instance, setting low values will trigger a fast convergence with a potential risk of high resource utilization if flapping routes cause network churn. Setting high values will keep the network stable with slower convergence.

It is recommended to leave the default value for the LSP generation interval at 5 seconds and also to increase the maximum lifetime for LSPs to 65,535 seconds, in order to conserve CPU usage for generation and refreshing of LSPs.

IS-IS Throttling Timers That Affect Fast Convergence

You can configure IS-IS to react more rapidly to isolated events that are likely to be real link failures and to react more stably to frequent events that are unlikely to be actual link failures. The convergence speed and stability of IS-IS is affected by the values that you set for various throttling timers. The throttling timers impose a trade-off between reaction time to external events and the amount of resources dedicated to maintaining the information in the Routing Information Base (RIB). You should become familiar with the following.

IS-IS PDUs

IS-IS encapsulates data into a data-link protocol data unit (PDU). There are four different PDU types and each can be Level 1 or Level 2:

- **LSP** --An LSP is a PDU that is sent between two IS-IS neighbors. The LSP contains information about neighbors and path costs, including adjacencies to neighbors, connected IP prefixes, Open Systems Interconnection (OSI) end systems, and area addresses. LSPs are used by the receiving routers to maintain their routing tables.
- **IIH** --An IS-IS Hello PDU is used to establish and maintain adjacencies. By default, an Intermediate-to-Intermediate Hello (IIH) is padded to the maximum transmission unit (MTU) size.
- **PSNP** --A partial sequence number PDU (PSNP) contains summaries of only a subset of known LSPs. A PSNP is used to acknowledge and request link-state information by soliciting newer versions of a complete LSP, or acknowledging receipt of an updated LSP, respectively.
- **CSNP** --A complete sequence number PDU (CSNP) contains summaries of all LSPs known by the issuing router.

LSP-Related Intervals and Exponential Backoff Timers

The following timers and intervals relate to LSPs that are generated by the IS-IS router.

- **LSP refresh interval** --Specifies the number of seconds (0 to 65535) the router will wait before refreshing (re-creating and reflooding) its own LSP.
- **Maximum LSP lifetime** --Specifies the value of the lifetime in the LSP header. Lifetime is used by all IS-IS routers in order to age out and purge old LSPs.

The following exponential backoff timers have been implemented in IS-IS to control the events of SPF calculation, Partial Route Calculations (PRC) computation, and LSP generation:

- **PRC interval** --Specifies the number of seconds between two consecutive PRCs. When changes that do not affect the topology, such as advertised external prefixes, are detected, the PRC is triggered.
- **LSP generation interval** --Specifies the number of seconds between creating new versions of a given LSP on a per-node basis.
- **SPF interval** --Specifies the number of seconds between two consecutive SPF calculations.

The purpose of these exponential backoff timers is to react quickly to the first events but, under constant churn, to slow down in order to prevent the CPU of the router from collapsing. The exponential backoff algorithm operates as follows:

1. An initial event triggers the SPF, PRC, or LSP generation.
2. The initial wait time that is configured for the interval determines the time between the initial event and the start of the SPF, PRC, or LSP generation.
3. The incremental wait time that is configured for the interval determines the amount of time that the router will wait in between the consecutive SPF execution, PRC execution, or LSP generation. This incremental value will increase exponentially between the incremental events until the maximum value is reached. For example, the incremental value will be (1x incremental value) between the first and second events, (2 x incremental value) between the second and third event, (4 x incremental value) between the third and fourth event, (8 x incremental value) between the fourth and fifth event, and so on, until the configured maximum interval--amount of time in seconds that the router will wait in between consecutive SPF execution, PRC execution, or LSP generation--has been reached.
4. If no new triggers have been received after two times the configured maximum wait-interval value, the network stabilizes, returning to a steady state and fast behavior. The initial wait-time interval will be reinstated.

See the to configure the recommended settings for the SPF, PRC and LSP generation timers.

IS-IS Hello PDU Timers

The different IS-IS Hello timers need to be adapted according to the adjacency convergence time required for each subnet. Where a rapid adjacency loss has been detected, the timers need to be reduced. These timers should be modified if necessary after deployment and after an accurate monitoring of the network stability and convergence has occurred.

- **Hello interval** --Number of seconds during two consecutive transmissions of IIH PDUs.
- **Hello interval minimum** --When the hello interval is configured, the hold time is set to one second. The significance of the hello multiplier changes if Fast Hellos are used; the hello multiplier becomes the number of hellos that will be sent per second.
- **Hello multiplier** --An integer from 1 to 300 that is used to calculate the hold time. The hold time is the number of seconds during which the router will wait for an IIH before declaring that its neighbor is lost. The router multiplies the hello interval by the hello multiplier to determine the hold time. To avoid unnecessary adjacency resets, increase the default value of 3 on interfaces where frequent losses of IIH PDUs are detected.
- **IS-IS retransmit interval** --Specifies the number of seconds between the resending of IS-IS link-state PDU transmissions for point-to-point links.

CSNP Interval

TheCSNP interval specifies the number of seconds between the two consecutive transmissions of CSNP PDUs. CSNP are generated by the designated router (DIS) in order for all routers connected to a broadcast media to synchronize their databases and by adjacent routers on a point-to-point network while setting up an adjacency. CSNPs are used to keep all router databases up to date. The lower the value of the CSNP interval, the faster the speed of the sychronization. However, a CSNP interval that is too low will trigger intensive PSNP PDU transmissions. All routers that are not synchronized with the DIS (Designated Intermediate System) and that, therefore, need additional LSPs in their database send PSNPs.

SPF, PRC, and LSP generation exponential backoff timers need to be tuned according to the level of stability of the network and the stability required in the routing domain. For instance, setting low values will trigger a fast convergence with a potential risk of high resource utilization if flapping routes cause network churn. Setting high values will keep the network stable with slower convergence.

It is recommended to leave the default value for the LSP generation interval at 5 seconds and also to increase the maximum lifetime for LSPs to 65,535 seconds, in order to conserve CPU usage for generation and refreshing of LSPs.

If you are using a routing algorithm based on SPF and if you use values for the initial required delay that are fewer than 40 milliseconds, SPF may 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. LSP flooding is required in order to guarantee that the network update in the LSP is propagated around the network as quickly as possible.

How to Reduce Link Failure and Topology Change Notification Times in IS-IS Networks

Tuning SPF PRC and LSP Generation Exponential Backoff Timers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]
5. **prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*]
6. lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*]
7. **max-lsp-lifetime** [**hours**] *value*
8. **lsp-refresh-interval** *seconds*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*] **Example:** `Router(config-router)# spf-interval 5 1 20`	Customizes IS-IS throttling of SPF calculations. **Note** The recommended values for the *spf-max-wait*, *spf-initial-wait*, and *spf-second-wait* arguments are 5, 1, and 20, respectively.
Step 5	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] **Example:** `Router(config)# prc-interval 5 1 20`	Customizes IS-IS throttling of PRC calculations. **Note** The recommended values for the *prc-max-wait*, *prc-initial-wait*, and *prc-second-wait* arguments are 5, 1, and 20, respectively.
Step 6	lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*] **Example:** `Router(config-router)# lsp-gen-interval 5 1 20`	Sets the minimum interval at which link-state PDUs (LSPs) are generated. **Note** The recommended values for the *lsp-max-wait*, *lsp-initial-wait*, and *lsp-second-wait* arguments are 5, 1, and 20, respectively.
Step 7	**max-lsp-lifetime** [**hours**] *value* **Example:** `Router(config-router)# max-lsp-lifetime 65535`	Sets the maximum time for which LSPs persist without being refreshed. • To reduce network resources used for LSP generation, increase the LSP maximum lifetime value of 65535.

	Command or Action	Purpose
Step 8	**lsp-refresh-interval** *seconds* **Example:** `Router(config-router)# lsp-refresh-interval 65535`	Sets the minimum interval at which LSPs are refreshed. • To reduce network resources used for LSP refresh, increase the value to the LSP refresh interval to maximum value of 65535 seconds.
Step 9	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

Enabling IS-IS Fast-Flooding of LSPs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **fast-flood** *lsp-number*
5. **end**
6. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required, and enters router configuration mode.
Step 4	**fast-flood** *lsp-number* **Example:** `Router(config-router)# fast-flood 20`	Fast-floods LSPs. • Keep the default values for the **isis retransmit-interval** and **isis retransmit-throttle-interval** commands when you configure the **fast-flood** command.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies that fast-flooding has been enabled.

Monitoring IS-IS Network Convergence Time

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**isis display delimiter** [**return** *count* | **character** *count*] **Example:** `Router(config)# isis display delimiter return 2`	(Optional) Makes output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Router# show isis database detail`	(Optional) Displays the IS-IS link-state database.
Step 6	**show isis** [*area-tag*] **routes** **Example:** `Router# show isis financetag routes`	(Optional) Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	**show isis spf-log** **Example:** `Router# show isis spf-log`	(Optional) Displays how often and why the router has run a full SPF calculation.

	Command or Action	Purpose
Step 8	**show isis** [*process-tag*] **topology** **Example:** `Router# show isis financetag topology`	(Optional) Displays a list of all connected routers in all areas. • If a process tag is specified, output is limited to the specified routing process. When "null" is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.

Configuration Examples for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

Example Tuning IS-IS LSP Generation

The following example configures the router to reduce LSP flooding and the consequent resource consumption by tuning the LSP values to their maximums. Adjusting the IS-IS timers will decrease the time required for the router to send routing updates.

```
Router> enable
Router# configure terminal
Router(config)# router isis
Router(config-router)# isis tag 200
Router(config-router)# lsp-gen-interval 5
Router(config-router)# max-lsp-lifetime 65535
Router(config-router)# lsp-refresh-interval 65000
```

Example Tuning IS-IS Fast Flooding of LSPs

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

```
Router> enable
Router# configure terminal
Router(config)# router isis first
Router(config-router)# fast-flood 7
Router(config-router)# end
Router# show running-config | include fast-flood

fast-flood 7
```

Where to Go Next

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

- "Setting Best Practice Parameters for IS-IS Fast Convergence"
- "Reducing Failure Detection Times in IS-IS Networks"
- "Reducing Alternate-Path Calculation Times in IS-IS Networks"

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module
Customizing IS-IS for fast convergence and scalability	"Overview of IS-IS Fast Convergence" module

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 7 Feature Information for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

Feature Name	Software Releases	Feature Information
IS-IS Fast-Flooding of LSPs Using the **fast-flood** Command	12.0(27)S 12.3(7)T	The IS-IS Fast-Flooding of LSPs Using the **fast-flood** Command feature improves Intermediate System-to-Intermediate System (IS-IS) convergence time when new link-state PDUs (LSPs) are generated in the network and shortest path first (SPF) is triggered by the new LSPs. The following command was introduced by this feature: **fast-flood**.

Reducing Alternate-Path Calculation Times in IS-IS Networks

The tasks in this module explain how to tune IS-IS and enable routers to more quickly respond to topology changes and network failures when they receive routing updates that advertise topology changes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Reducing Alternate-Path Calculation Times in IS-IS Networks

You should be familiar with the concepts described in the "Overview of IS-IS Fast Convergence" module.

Information About Reducing Alternate-Path Calculation Times in IS-IS Networks

IS-IS uses 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 occur, 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 IS-IS convergence and saves CPU resources.

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 LSP. However, incremental SPF typically reduces demand on CPU.

Route Redistribution

Routers are allowed to redistribute external prefixes, or routes, that are learned from any other routing protocol, static configuration, or connected interfaces. The redistributed routes are allowed in either a Level 1 router or a Level 2 router. When Level 2 routes are injected as Level 1 routes, this is called route leaking.

IS-IS Caching of Redistributed Routes

Beginning with Cisco IOS Release 12.0(27)S, and later releases, IS-IS caches routes that are redistributed from other routing protocols or from another IS-IS level into a local redistribution cache that is maintained by IS-IS. Caching occurs automatically and requires no configuration. The caching of redistributed routes improves IS-IS convergence time when routes are being redistributed into IS-IS. IS-IS caching of redistributed routes increases the performance of LSP generation, significantly improving network scalability.

Prioritizing the Update of IP Prefixes in the RIB to Reduce Alternate-Path Calculation Time

The time needed for the IS-IS Routing Information Base (RIB) or routing table to update depends on the number of changed IS-IS prefixes or routes that must be updated. You can tag important IS-IS IP prefixes and configure the router to give priority to the tagged prefixes so that high-priority prefixes are updated first in the RIB. For example, the loopback addresses for the routers in an MPLS VPN environment are considered high priority prefixes.

IS-IS Priority-Driven IP Prefix RIB Installation

In a network where routers run the IS-IS protocol, convergence is achieved by distributing a consistent view of the topology to all routers in the network. When a network event causes a topology change, a number of steps must occur in order for convergence to occur. The router that initially detects the topology change (for example, an interface state change) must inform other routers of the topology change by

flooding updated routing information (in the form of link-state PDUs) to other routers. All routers, including the router that detected the topology change, must utilize the updated topology information to recompute shortest paths (run an SPF), providing the updated output of the SPF calculation to the router's RIB, which will eventually cause the updated routing information to be used to forward packets. Until all routers have performed these basic steps, some destinations may be temporarily unreachable. Faster convergence benefits the network performance by minimizing the period of time during which stale topology information--the previous routing information that will be obsoleted by the updated routing information--is used to forward packets.

After performing an SPF, IS-IS must install updated routes in the RIB. If the number of prefixes advertised by IS-IS is large, the time between the installation of the first prefix and the last prefix is significant. Priority-driven IP prefix RIB installation allows a subset of the prefixes advertised by IS-IS to be designated as having a higher priority. Updates to the paths to these prefixes will be installed before updates to prefixes that do not have this designation. This reduces the convergence time for the important IS-IS IP prefixes and results in faster updating for routes that are dependent on these prefixes. This in turn shortens the time during which stale information is used for forwarding packets to these destinations.

Prefixes are characterized as having one of three levels of importance:

1. High priority prefixes--prefixes that have been tagged with a tag designated for fast convergence.
2. Medium priority prefixes--any /32 prefixes that have not been designated as high priority prefixes.
3. Low priority prefixes--all other prefixes.

When IS-IS updates the RIB, prefixes are updated in the order based on the associated level of importance.

When you assign a high priority tag to some IS-IS IP prefixes, those prefixes with the higher priority are updated in the routing tables before prefixes with lower priority. In some networks, the high priority prefixes will be the provider edge (PE) loopback addresses. The convergence time is reduced for the important IS-IS IP prefixes and results in reduced convergence time for the update processes that occur in the global RIB and Cisco Express Forwarding (CEF).

Tagging IS-IS Routes to Control Their Redistribution

You can control the redistribution of IS-IS routes by tagging them. The term "route leaking" refers to controlling distribution through tagging of routes.

How Route Summarization Can Enhance Scalability in IS-IS Networks

Summarization is a key factor that affects the scalability of a routing protocol. Summarization reduces the number of routing updates that are flooded across areas or routing domains. Especially for multi-area IS-IS, a good addressing scheme can optimize summarization by not allowing an overly large Level 2 database that is unnecessarily populated with updates that have come from Level 1 areas.

A router can summarize prefixes on redistribution whether the prefixes have come from internal prefixes, local redistribution, or Level 1 router redistribution. Routes that have been leaked from Level 2 to Level 1 and routes that are advertised into Level 2 from Level 1 can also be summarized.

Benefits of IS-IS Route Tags

- The IS-IS Support for Route Tags feature allows you to tag IP addresses of an interface and use the tag to apply administrative policy with a route map.
- You can tag IS-IS routes to control their redistribution. You can configure a route map to set a tag for an IS-IS IP prefix (route) and/or match on the tag (perhaps on a different router) to redistribute IS-IS routes. Although the **match tag** and **set tag** commands existed for other protocols before this feature, they were not implemented for IS-IS, so they did nothing when specified in an IS-IS network until now.
- You can tag a summary route and then use a route map to match the tag and set one or more attributes for the route.

IS-IS Route Tag Characteristics

An IS-IS route tag number can be up to 4 bytes long. The tag value is set into a sub-TLV 1 for TLV (Type Length Value) Type 135. For more information about TLV Type 135, see the *Intermediate System-to-Intermediate System (IS-IS) TLVs* **document referenced in the " Related Documents " section.**

Only one tag can be set to an IS-IS IP route (prefix). The tag is sent out in link-state PDUs (LSPs) advertising the route. Setting a tag to a route alone does nothing for your network. You can use the route tag at area or Level 1/Level 2 boundaries by matching on the tag and then applying administrative policies such as redistribution, route summarization, or route leaking.

Configuring a tag for an interface (with the **isis tag** command) triggers the generation of new LSPs from the router because the tag is new information for the PDUs.

IS-IS Route Leaking Based on a Route Tag

You can tag IS-IS routes to configure route leaking (redistribution). Since only the appropriate routes are redistributed--or leaked--the results is network scalability and faster convergence for the router update. If you configure route leaking and you want to match on a tag, use a route map (not a distribute list). For more information on route leaking, see the *IS-IS Route Leaking* document referenced in the IS-IS Route Leaking Based on a Route Tag, page 126 section.

There are two general steps to using IS-IS route tags: tagging routes and referencing the tag to set values for the routes and/or redistribute routes.

There are three ways to tag IS-IS routes: tag routes for networks directly connected to an interface, set a tag in a route map, or tag a summary route. All three methods are described in this section. The tagging method is independent of how you use the tag.

After you tag the routes, you can use the tag to set values (such as a metric, or next hop, and so on) and/or redistribute routes. You might tag routes on one router, but reference the tag on other routers, depending on what you want to achieve. For example, you could tag the interface on Router A with a tag, match the tag on Router B to set values, and redistribute routes on Router C based on values using a route map.

Limiting the Number of Routes That Are Redistributed into IS-IS

If someone mistakenly injects a large number of IP routes into IS-IS, perhaps by redistributing Border Gateway Protocol (BGP) into IS-IS, the network can be severely flooded. Limiting the number of redistributed routes prevents this potential problem. You can either configure IS-IS to stop allowing routes to be redistributed once your maximum configured value has been reached or configure the software to generate a system warning once the number of redistributed prefixes has reached the maximum value. Before configuring the tasks in this section, you should be familiar with the following concept.

LSP Full State

In some cases when a limit is not placed on the number of redistributed routes, the LSP may become full and routes may be dropped. A user can specify which routes should be suppressed in that event so that the consequence of an LSP full state is handled in a graceful and predictable manner.

Redistribution is usually the cause of the LSP full state. By default, external routes redistributed into IS-IS are suppressed if the LSP full state occurs. IS-IS can have 255 fragments for an LSP in a level. When there is no space left in any of the fragments, an LSPFULL error message is generated.

Once the problem that caused the LSP full state is resolved, a user can clear the LSPFULL state.

This section contains the following procedures, which are mutually exclusive. That is, you cannot both limit redistributed prefixes and also choose to be warned only.

Streamlining the Routing Table Update Process by Excluding Connected IP Prefixes from LSP Advertisements

In order to speed up IS-IS convergence, the number of IP prefixes carried in LSPs needs to be limited. Configuring interfaces as unnumbered would limit the prefixes. However, for network management reasons, you might want to have numbered interfaces and also want to prevent advertising interface addresses into IS-IS. There are two alternative methods to avoid the overpopulation of routing tables and thereby reduce IS-IS convergence time. In order to choose the method that will work best for your network, you should become familiar with the following concepts.

- Small-Scale Method to Reduce IS-IS Convergence Time, page 127
- Large-Scale Method to Reduce IS-IS Convergence Time, page 127
- Benefit of Excluding IP Prefixes of Connected Networks in LSP Advertisements, page 127

Small-Scale Method to Reduce IS-IS Convergence Time

You can explicitly configure an IS-IS interface not to advertise its IP network to the neighbors (by using the **no isis advertise-prefix**command).This method is feasible for a small network; it does not scale well. If you have dozens or hundreds of routers in your network, with possibly ten times as many physical interfaces involved, it would be difficult to add this command to each router's configuration.

Large-Scale Method to Reduce IS-IS Convergence Time

An easier way to reduce IS-IS convergence is to configure the IS-IS instance on a router to advertise only passive interfaces (by using the **advertise-passive-only** command). 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 PDUs 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.

Benefit of Excluding IP Prefixes of Connected Networks in LSP Advertisements

Whether you choose to prevent the advertising of IS-IS interface subnetworks or to advertise only the IS-IS prefixes that belong to passive (loopback) interfaces, you will reduce IS-IS convergence time. The IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements feature is recommended in any case where fast convergence is required.

How to Reduce Alternate-Path Calculation Times in IS-IS Networks

Configuring Incremental SPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **ispf** [**level-1** | **level-2** | **level-1-2**][*seconds*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router isis** *area-tag* **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**ispf** [**level-1** | **level-2** | **level-1-2**][*seconds*] **Example:** `Router(config-router)# ispf level-1-2 60`	Enables incremental SPF. • The seconds argument represents the 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.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

Assigning a High Priority Tag to an IS-IS IP Prefix

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip router isis** [*area-tag*]
5. **isis tag** *tag-value*
6. **exit**
7. **router isis** [*area-tag*]
8. **ip route priority high tag** *tag-value*
9. **end**
10. **show isis rib** [*ip-address* | *ip-address-mask*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip router isis** [*area-tag*] **Example:** `Router(config-if)# ip router isis tag13`	Enables IS-IS as an IP routing protocol, and assigns a tag to a process, if required. **Note** If the *area-tag* argument 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.
Step 5	**isis tag** *tag-value* **Example:** `Router(config-if)# isis tag 17`	Sets a tag on the IP address configured for an interface when this IP prefix is put into an IS-IS LSP. • The *tag-value* argument requires an interger in a range from 1 to 4294967295 and serves as a tag on an IS-IS route.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**router isis** [*area-tag*] **Example:** `Router(config)# router isis marketing`	Enables the IS-IS routing protocol and specifies an IS-IS process. Enters router configuration mode. **Note** If the *area-tag* argument 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 CLNS router processes for a given router.
Step 8	**ip route priority high tag** *tag-value* **Example:** `Router(config-router)# ip route priority high tag 17`	Assigns a high priority to prefixes associated with the specified tag value. • Assigns a high priority to IS-IS IP prefixes with a specific route tag in a range from 1 to 4294967295 that you specify for the *tag-value* argument.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-router)# end`	(Optional) Saves configuration commands to the running configuration file and returns to privileged EXEC mode.
Step 10	**show isis rib** [*ip-address* | *ip-address-mask*] **Example:** `Router# show isis rib 255.255.255.0`	Displays paths for a specific route in the IP Version 4 IS-IS local RIB. • IS-IS maintains a local database for all IS-IS routing information. This local database is referred to as the IS-IS local RIB. It contains additional attributes that are not maintained in the global IP routing table. Access to the contents of the local RIB is used to support the **show isis rib** command, which is used here to verify routing information related to the Priority-Driven IP Prefix RIB Installation feature.

• Troubleshooting Tips, page 131

Troubleshooting Tips

You can enter the **debug isis rib local** command to verify whether the IP prefixes that are advertised by IS-IS link-state PDUs (LSPs) are being updated correctly in the IS-IS local RIB.

Tagging Routes for Networks Directly Connected to an Interface

- Because the IS-IS route tag will be used in a route map, you must understand how to configure a route map.
- In order to use the route tag, you must configure the **metric-style wide command. (The metric-style narrow**command is configured by default**). The tag value is set into sub-TLV 1 for TLV (Type Length Value) Type 135.**
- You must understand the task for which you are using the route tag, such as route redistribution, route summarization, or route leaking.

Before you tag any IS-IS routes, you need to decide on the following:

1. Your goal to set values for routes or redistribute routes (or both).
2. Where in your network you want to tag routes.
3. Where in your network you want to reference the tags.
4. Which tagging method you will use, which determines which task in this section to perform.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip address** *ip-address mask* **secondary**
6. **isis tag** *tag-value*
7. **end**
8. **show isis database verbose**
9. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	Sets a primary IP address for an interface. • In this example, the network 10.1.1.0 will be tagged.

	Command or Action	Purpose
Step 5	**ip address** *ip-address mask* **secondary** **Example:** `Router(config-if)# ip address 10.2.2.1 255.255.255.0 secondary`	(Optional) Sets a secondary IP address for an interface. • In this example, the network 10.2.2.0 will be tagged.
Step 6	**isis tag** *tag-value* **Example:** `Router(config-if)# isis tag 120`	Sets a tag on the IP addresses configured under this interface when those IP prefixes are put into an IS-IS LSP. • The tag must be an integer.
Step 7	**end** **Example:** `Router(config-if)# end`	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 8	**show isis database verbose** **Example:** `Router# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.
Step 9	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*]] **Example:** `Router# show ip route 10.1.1.1 255.255.255.0`	(Optional) Displays the current state of the routing table. • Perform this step if you want to verify the tag.

• What to Do Next, page 133

What to Do Next

Applying the tag does nothing of value for your network until you use the tag by referencing it in a route map, either to set values, to redistribute routes, or to do both. Proceed to the section, "Using the Tag to Set Values and or Redistribute Routes, page 137."

Tagging Routes Using a Route Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match tag** *tag-value* [*...tag-value*]
5. Use an additional **match** command for each match criterion that you want.
6. **set tag** *tag-value*
7. Set another value, depending on what else you want to do with the tagged routes.
8. Repeat Step 7 for each value that you want to set.
9. Repeat Steps 3 through 8 for each route-map statement that you want.
10. **end**
11. **show isis database verbose**
12. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** *access-list-number* | [*access-list-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** `Router(config)# route-map static-color permit 15`	Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another. • This command causes the router to enter route-map configuration mode.
Step 4	**match tag** *tag-value* [*...tag-value*] **Example:** `Router(config-route-map)# match tag 15`	(Optional) Matches routes tagged with the specified tag numbers. • If you are setting a tag for the first time, you cannot match on tag; this step is an option if you are changing tags.

	Command or Action	Purpose
Step 5	Use an additional **match** command for each match criterion that you want.	(Optional) See the appropriate **match** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference* • Repeat this step for each match criterion you that want.
Step 6	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 10`	Specifies the tag number to set.
Step 7	Set another value, depending on what else you want to do with the tagged routes.	(Optional) See the following **set** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference* • **set level** • **set metric** • **set metric-type**
Step 8	Repeat Step 7 for each value that you want to set.	(Optional)
Step 9	Repeat Steps 3 through 8 for each route-map statement that you want.	(Optional)
Step 10	**end** **Example:** `Router(config-route-map)# end`	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 11	**show isis database verbose** **Example:** `Router# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.
Step 12	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** *access-list-number* | [*access-list-name*]] **Example:** `Router# show ip route 10.1.1.1 255.255.255.0`	(Optional) Displays the current state of the routing table. • Perform this step if you want to verify the tag.

• What to Do Next, page 135

What to Do Next

Applying the tag does nothing of value for your network until you use the tag by referencing it in a route map, either to set values, to redistribute routes, or to do both. Proceed to the Using the Tag to Set Values and or Redistribute Routes, page 137.

Tagging a Summary Address

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [** *area-tag* **]**
4. **metric-style wide**
5. **summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**} [**tag** *tag-value*] [**metric** *metric-value*]
6. **end**
7. **show isis database verbose**
8. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** *access-list-number* | [*access-list-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis [** *area-tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**metric-style wide** **Example:** `Router(config-router)# metric-style wide`	Configures a router running IS-IS so that it generates and accepts type, length, and value object (TLV) 135 for IP addresses.

	Command or Action	Purpose
Step 5	**summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**} [**tag** *tag-value*] [**metric** *metric-value*] **Example:** `Router(config-router)# summary-address 192.168.0.0 255.255.0.0 tag 12345 metric 321`	Creates aggregate addresses for IS-IS. **Note** If a tagged route is summarized and the tag is not explicitly configured in the **summary-address** command, then the tag is lost.
Step 6	**end** **Example:** `Router(config-router)# end`	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 7	**show isis database verbose** **Example:** `Router# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.
Step 8	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** *access-list-number* | [*access-list-name*]] **Example:** `Router# show ip route 10.1.1.1 255.255.255.0`	(Optional) Displays the current state of the routing table. • Perform this step if you want to verify the tag.

• What to Do Next, page 137

What to Do Next

Applying the tag does nothing of value for your network until you use the tag by referencing it in a route map to set values. It is unlikely that you will redistribute summary routes. Proceed to the "Using the Tag to Set Values and/or Redistribute Routes" section.

Using the Tag to Set Values and or Redistribute Routes

You must have already applied a tag on the interface, in a route map, or on a summary route. See the Tagging IS-IS Routes to Control Their Redistribution, page 125.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match tag** *tag-value*
5. Specify a **match** command for each match criterion that you want.
6. Set a value, depending on what you want to do with the tagged routes.
7. Repeat Step 6 for each value that you want to set.
8. Repeat Steps 3 through 7 for each route-map statement that you want.
9. **exit**
10. **router isis**
11. **metric-style wide**
12. **redistribute** *protocol* [*process-id*] [**level-1**| **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** `Router(config)# route-map static-color permit 15`	Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another. • This command causes you to enter route-map configuration mode.
Step 4	**match tag** *tag-value* **Example:** `Router(config-route-map)# match tag 120`	(Optional) Applies the subsequent **set** commands to routes that match routes tagged with this tag number.
Step 5	Specify a **match** command for each match criterion that you want.	(Optional) Reference the appropriate **match** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference*.

	Command or Action	Purpose
Step 6	Set a value, depending on what you want to do with the tagged routes.	(Optional) See the following **set** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference*. • **set level** • **set metric** • **set metric-type**
Step 7	Repeat Step 6 for each value that you want to set.	(Optional)
Step 8	Repeat Steps 3 through 7 for each route-map statement that you want.	(Optional)
Step 9	**exit** **Example:** `Router(config-route-map)# exit`	(Optional) Returns to global configuration mode.
Step 10	**router isis** **Example:** `Router(config)# router isis`	(Optional) Enables the IS-IS routing protocol and specifies an IS-IS process.
Step 11	**metric-style wide** **Example:** `Router(config-router)# metric-style wide`	Configures a router running IS-IS so that it generates and accepts type, length, and value object (TLV) 135 for IP addresses.
Step 12	**redistribute** *protocol* [*process-id*] [**level-1**| **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*] **Example:** `Router(config-router)# redistribute static ip metric 2 route-map static-color`	(Optional) Redistributes routes from one routing domain into another routing domain.

Limiting the Number of IS-IS Redistributed Routes

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [** *area-tag* **]**
4. **redistribute** *protocol* [*process-id*]{**level-1**| **level-1-2**| **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*]
5. **redistribute maximum-prefix** *maximum* [*percentage*] [**warning-only** | **withdraw**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis [** *area-tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**redistribute** *protocol* [*process-id*]{**level-1**| **level-1-2**| **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] **Example:** `Router(config-router)# redistribute eigrp 10 level-1`	Redistributes routes from one routing domain into another routing domain.

	Command or Action	Purpose
Step 5	**redistribute maximum-prefix** *maximum* [*percentage*] [**warning-only** | **withdraw**] **Example:** `Router(config-router)# redistribute maximum-prefix 1000 80`	Sets a maximum number of IP prefixes that are allowed to be redistributed into IS-IS. • There is no default value for the *maximum* argument. • The *percentage* value defaults to 75 percent. • If the **withdraw** keyword is specified and the maximum number of prefixes is exceeded, IS-IS rebuilds the link-state protocol data unit (PDU) fragments without the external IP prefixes. That is, the redistributed prefixes are removed from the PDUs. **Note** If the **warning-only** keyword had been configured in this command, no limit would be enforced; a warning message is simply logged.
Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Requesting a Warning About the Number of Prefixes Redistributed into IS-IS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [area-** *tag* **]**
4. **redistribute** *protocol* [*process-id*]{**level-1**| **level-1-2**| **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*]
5. **redistribute maximum-prefix** *maximum* [*percentage*] [**warning-only** | **withdraw**]
6. **lsp-full suppress** {[**external**] [**interlevel**] | **none**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**redistribute** *protocol* [*process-id*]{**level-1**| **level-1-2**| **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] **Example:** `Router(config-router)# redistribute eigrp 10 level-1`	Redistributes routes from one routing domain into another routing domain.
Step 5	**redistribute maximum-prefix** *maximum* [*percentage*] [**warning-only** | **withdraw**] **Example:** `Router(config-router)# redistribute maximum-prefix 1000 80 warning-only`	Causes a warning message to be logged when the maximum number of IP prefixes has been redistributed into IS-IS. • Because the **warning-only** keyword is included, no limit is imposed on the number of redistributed prefixes into IS-IS. • There is no default value for the *maximum* argument. • The *percentage* value defaults to 75 percent. • In this example configuration, two warnings are generated: one at 80 percent of 1000 (800 prefixes redistributed) and another at 1000 prefixes redistributed.
Step 6	**lsp-full suppress** {[**external**] [**interlevel**] | **none**} **Example:** `Router(config-router)# lsp-full suppress external interlevel`	(Optional) Controls which routes are suppressed when the link-state PDU becomes full. • The default is **external**(redistributed routes are suppressed). • The **interlevel** keyword causes routes from another level to be suppressed. • The **external** and **interval** keywords can be specified together or separately. • See the Requesting a Warning About the Number of Prefixes Redistributed into IS-IS, page 141".

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Excluding Connected IP Prefixes on a Small Scale

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address netmask*
5. **no ip directed-broadcast**
6. **ip router isis [area-** *tag* **]**
7. **no isis advertise-prefix**
8. **exit**
9. Repeat Steps 3 through 8 for each interface on which you do not want to advertise IP prefixes.
10. **router isis [area-** *tag* **]**
11. **net** *network-entity-title*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address netmask* **Example:** `Router(config-if)# ip address 192.168.20.1 255.255.255.0`	Sets a primary IP address for an interface. • The network mask can be indicated as a 4-part dotted decimal address or as a prefix. This example uses a 4-part dotted decimal number.
Step 5	**no ip directed-broadcast** **Example:** `Router(config-if)# no ip directed-broadcast`	(Optional) Disables the translation of a directed broadcast to physical broadcasts.
Step 6	**ip router isis [area-** *tag* **]** **Example:** `Router(config-if)# ip router isis`	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
Step 7	**no isis advertise-prefix** **Example:** `Router(config-if)# no isis advertise-prefix`	Prevents the advertising of IP prefixes of connected networks in LSP advertisements per IS-IS interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 9	Repeat Steps 3 through 8 for each interface on which you do not want to advertise IP prefixes.	(Optional)
Step 10	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.

	Command or Action	Purpose
Step 11	**net** *network-entity-title* **Example:** `Router(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00`	Configures an IS-IS network entity title (NET) for the routing process.
Step 12	**end** **Example:** `Router(config-router)# end`	(Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode.

Excluding Connected IP Prefixes on a Large Scale

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *number*
4. **ip address** *ip-address netmask*
5. **no ip directed-broadcast**
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address netmask*
9. **no ip directed-broadcast**
10. **ip router isis [area-** *tag* **]**
11. **exit**
12. **router isis [area-** *tag* **]**
13. **passive-interface** [**default**] *type number*
14. **net** *network-entity-title*
15. **advertise-passive-only**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface loopback** *number* **Example:** `Router(config)# interface loopback 0`	Configures a loopback interface and enters interface configuration mode.
Step 4	**ip address** *ip-address netmask* **Example:** `Router(config-if)# ip address 192.168.10.1 255.255.255.255`	Sets a primary IP address for an interface. • The network mask can be indicated as a 4-part dotted decimal address or as a prefix. This example uses a 4-part dotted decimal number.
Step 5	**no ip directed-broadcast** **Example:** `Router(config-if)# no ip directed-broadcast`	(Optional) Disables the translation of a directed broadcast to physical broadcasts.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 8	**ip address** *ip-address netmask* **Example:** `Router(config-if)# ip address 192.168.20.1 255.255.255.0`	Sets a primary IP address for an interface. • The network mask can be indicated as a 4-part dotted decimal address or as a prefix. This example uses a 4-part dotted decimal number.
Step 9	**no ip directed-broadcast** **Example:** `Router(config-if)# no ip directed-broadcast`	(Optional) Disables the translation of a directed broadcast to physical broadcasts.
Step 10	**ip router isis [area-** *tag* **]** **Example:** `Router(config-if)# ip router isis`	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 12	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 13	**passive-interface** [**default**] *type number* **Example:** `Router(config-router)# passive-interface loopback 0`	Disables sending routing updates on an interface.
Step 14	**net** *network-entity-title* **Example:** `Router(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00`	Configures an IS-IS NET for the routing process.

	Command or Action	Purpose
Step 15	**advertise-passive-only** **Example:** `Router(config-router)# advertise-passive-only`	Configures IS-IS to advertise only prefixes that belong to passive interfaces.
Step 16	**end** **Example:** `Router(config-router)# end`	(Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode.

Monitoring IS-IS Network Convergence Time

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isis display delimiter** [**return** *count* | **character** *count*]
4. **exit**
5. **show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
6. **show isis** [*area-tag*] **routes**
7. **show isis** [*area-tag*] [**ipv6** | *****] **spf-log**
8. **show isis** [*process-tag*] **topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**isis display delimiter** [**return** *count* | **character** *count*] **Example:** `Router(config)# isis display delimiter return 2`	Makes output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Router# show isis database detail`	Displays the IS-IS link-state database.
Step 6	**show isis** [*area-tag*] **routes** **Example:** `Router# show isis financetag routes`	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	**show isis** [*area-tag*] [**ipv6** | *****] **spf-log** **Example:** `Router# show isis spf-log`	Displays how often and why the router has run a full SPF calculation.
Step 8	**show isis** [*process-tag*] **topology** **Example:** `Router# show isis financetag topology`	Displays a list of all connected routers in all areas. • If a process tag is specified, output is limited to the specified routing process. When "null" is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.

Examples

The following sample output from the **show isis spf-log** command displays the following important information:

- At what time the SPFs have been executed
- Total elapsed time for the SPT computation, LRIB update, and RIB and FIB update
- Number of nodes in the graph
- Number of triggers that caused the SPF calculation

- Information regarding what triggered the SPF calculation

```
Router# show isis spf-log

   Level 1 SPF log

  When   Duration  Nodes  Count     Last trigger LSP   Triggers

00:15:46    3124     40      1          milles.00-00  TLVCODE

00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP

00:15:19    3096     41      1          deurze.00-00  TLVCODE

00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER

00:14:49    3384     41      1          milles.00-01  TLVCODE

00:14:23    2932     41      3          milles.00-00  TLVCODE

00:05:18    3140     41      1                        PERIODIC

00:03:54    3144     41      1          milles.01-00  TLVCODE

00:03:49    2908     41      1          milles.01-00  TLVCODE

00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT

00:03:15    3054     41      1          milles.00-00  TLVCODE

00:02:53    2958     41      1          mortel.00-00  TLVCODE
```

Configuration Examples for Reducing Alternate-Path Calculation Times in IS-IS Networks

Example Assigning a High Priority Tag Value to an IS-IS IP Prefix

The following example uses the **ip route priority high** command to assign a tag value of 200 to the IS-IS IP prefix:

```
interface Ethernet 0
 ip router isis
 isis tag 200
!
router isis
 ip route priority high tag 200
```

Example Tagging Routes for Networks Directly Connected to an Interface and Redistributing Them

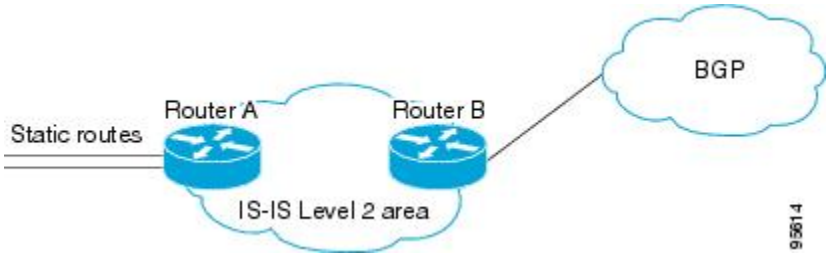
In this example, two interfaces are tagged with different tag values. By default, these two IP addresses would have been put into the IS-IS Level 1 and Level 2 database. However, by using the **redistribute** command with a route map to match tag 110, only IP address 172.16.10.5 255.255.255.0 is put into the Level 2 database.

```
interface ethernet 1/0
 ip address 192.168.129.1 255.255.255.0
 ip router isis
 isis tag 120
interface ethernet 1/1
 ip address 172.16.10.5 255.255.255.0
 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
```

Example Redistributing IS-IS Routes Using a Route Map

In a scenario using route tags, you might configure some commands on one router and other commands on another router. For example, you might have a route map that matches on a tag and sets a different tag on a router at the edge of a network, and on different routers you might configure the redistribution of routes based on a tag in a different route map.

Figure 6



The figure above illustrates a flat Level 2 IS-IS area. On the left edge are static routes from Router A to reach some IP prefixes. Router A redistributes the static routes into IS-IS. Router B runs BGP and

redistributes IS-IS routes into BGP and then uses the tag to apply different administrative policy based on different tag values.

Router A

```
router isis
 net 49.0000.0000.0001.00
 metric-style wide
 redistribute static ip route-map set-tag
!
route-map set-tag permit 5
 set tag 10
```

Router B

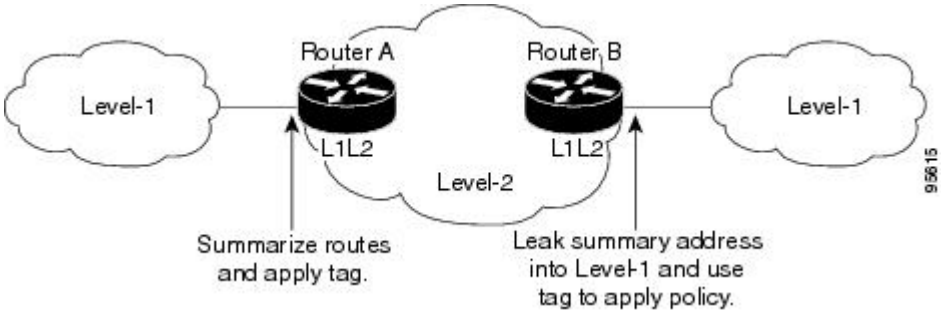
```
router bgp 100
 redistribute isis level-2 route-map tag-policy
route-map tag-policy permit 20
 match tag 10
 set metric 1000
```

Example Tagging a Summary Address and Applying a Route Map

The figure below illustrates two Level 1 areas and one Level 2 area between them. Router A and Router B are Level 1/Level 2 edge routers in the Level 2 area. On edge Router A, a summary address is configured to reduce the number of IP addresses put into the Level 2 IS-IS database. Also, a tag value of 100 is set to the summary address.

On Router B, the summary address is leaked into the Level 1 area, and administrative policy is applied based on the tag value.

Figure 7



Router A

```
router isis
 net 49.0001.0001.0001.00
 metric-style wide
 summary-address 10.0.0.0 255.0.0.0 tag 100
```

Router B

```
router isis
 net 49.0002.0002.0002.0002.0
 metric-style wide
 redistribute isis ip level-2 into level-1 route-map match-tag
```

```
route-map match-tag permit 10
 match tag 100
```

Example Filtering and Redistributing IS-IS Routes Using an Access List and a Route Map

In this example, the first **redistribute isis ip** command controls the redistribution of Level 1 routes into Level 2. Only the routes with the tag of 90 and whose IP prefix is not 192.168.130.5/24 will be redistributed from Level 1 into Level 2.

The second **redistribute isis ip** command controls the route leaking from Level 2 into the Level 1 domain. Only the routes tagged with 60 or 50 will be redistributed from Level 2 into Level 1.

```
interface ethernet 1
 ip address 192.168.130.5 255.255.255.0
 ip router isis
 isis tag 60
!
interface ethernet 2
 ip address 192.168.130.15 255.255.255.0
 ip router isis
 isis tag 90
!
interface ethernet 3
 ip address 192.168.130.25 5 255.255.255.0
 ip router isis
 isis tag 50
!
router isis
 net 49.0001.0001.0001.0001.00
 metric-style wide
 redistribute isis ip level-1 into level-2 route-map redist1-2
 redistribute isis ip level-2 into level-1 route-map leak2-1
!
access-list 102 deny ip host 192.168.130.5 host 255.255.255.255
access-list 102 permit ip any any
!
route-map leak2-1 permit 10
 match tag 60
!
route-map leak2-1 permit 20
 match tag 50
!
route-map redist1-2 permit 10
 match ip address 102
 match tag 90
```

Example IS-IS Limit on Number of Redistributed Routes

This example shows how to set a maximum of 1200 prefixes that can be redistributed into IS-IS. When the number of prefixes redistributed reaches 80 percent of 1200 (960 prefixes), a warning message is logged. When 1200 prefixes are redistributed, IS-IS rebuilds the LSP fragments without external prefixes and no redistribution occurs.

```
router isis 1
 redistribute maximum-prefix 1200 80 withdraw
```

Example Requesting a Warning About the Number of Redistributed Routes

This example shows how to allow two warning messages to be logged. The first message is generated if the number of prefixes redistributed reaches 85 percent of 600 (510 prefixes), and the second message is

generated if the number of redistributed prefixes reaches 600. However, the number of redistributed prefixes is not limited. If the LSPFULL state occurs, external prefixes will be suppressed.

```
router isis 1
 redistribute maximum-prefix 600 85 warning-only
 lsp-full suppress external
```

Example Excluding Connected IP Prefixes on a Small Scale

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
!
```

Example Excluding Connected IP Prefixes on a Large Scale

The following example uses the **advertise-passive-only** command, which applies to the entire IS-IS instance, thereby preventing IS-IS from 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
!
```

Where to Go Next

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

- "Overview of IS-IS Fast Convergence"

- "Reducing Failure Detection Times in IS-IS Networks"
- "Reducing Link Failure and Topology Change Notification Times in IS-IS Networks"

Additional References

Related Documents

Related Topic	Document Title
Description of IS-IS type length value (TLV) and its use.	Intermediate System-to-Intermediate Systems (IS-IS) TLVs
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
IS-IS route leaking	IS-IS Route Leaking
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Reducing Alternate-Path Calculation Times in IS-IS Networks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 8 Feature Information for Reducing Alternate-Path Calculation Times in IS-IS Networks

Feature Name	Releases	Feature Information
IS-IS Caching of Redistributed Routes	12.0(27)S 12.2(25)S 12.3(7)T Cisco IOS XE 3.1.0 SG	The IS-IS Caching of Redistributed Routes feature improves Intermediate System-to-Intermediate System (IS-IS) convergence time when routes are being redistributed into IS-IS. This document introduces new commands for monitoring and maintaining IS-IS redistributed routes.
IS-IS Incremental SPF	12.0(24)S 12.2(18)S 12.3(2)T Cisco IOS XE 3.1.0 SG	Integrated IS-IS can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing IS-IS to converge faster on a new routing topology in reaction to a network event.
IS-IS Limit on Number of Redistributed Routes	12.0(25)S 12.2(18)S 12.3(4)T Cisco IOS XE 3.1.0 SG	The IS-IS Limit on Number of Redistributed Routes feature provides for a user-defined maximum number of prefixes that are allowed to be redistributed into IS-IS from other protocols or other IS-IS processes. Such a limit can help prevent the router from being flooded by too many redistributed routes.
IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements	12.0(22)S 12.2(18)S 12.3(2)T Cisco IOS XE 3.1.0 SG	This document describes two Integrated Intermediate System-to-Intermediate System (IS-IS) mechanisms to exclude IP prefixes of connected networks from link-state PDU (LSP) advertisements, thereby reducing IS-IS convergence time.

Feature Name	Releases	Feature Information
IS-IS Support for Priority-Driven IP Prefix RIB Installation	12.0(26)S 12.2(18)SXE 12.2(25)S 12.3(4)T Cisco IOS XE 3.1.0 SG	The IS-IS Support for Priority-Driven Prefix RIB Installation feature allows customers to designate a subset of IP prefixes advertised by IS-IS for faster processing and installation in the global routing table as one way to achieve faster convergence. For example, Voice over IP (VoIP) gateway addresses may need to be processed first to help VoIP traffic get updated faster than other types of packets.
IS-IS Support for Route Tags	12.2(18)S 12.2(27)SBC 12.3(2)T Cisco IOS XE 3.1.0 SG	The IS-IS Support for Route Tags feature provides the capability to tag IS-IS route prefixes and use those tags in a route map to control IS-IS route redistribution or route leaking.

Enhancing Security in an IS-IS Network

This module describes processes that you can follow to enhance network security when you use Intermediate System-to-Intermediate System (IS-IS) in your network. You can set passwords, prevent unauthorized routers from forming adjacencies with routers in your IS-IS network, and use the IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication feature.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Enhancing Security in an IS-IS Network

- Before performing the tasks in this module, you should be familiar with the concepts described in the "Integrated IS-IS Routing Protocol Overview" and "Configuring a Basic IS-IS Network" modules.
- It is assumed you already have IS-IS running on your network.

Information About Enhancing Security in an IS-IS Network

Importance of Preventing Unauthorized Information from Entering an IS-IS Network

It is recommended that you configure the security features described in this module in order to prevent unauthorized routing messages from being placed into the network routing domain. You can set an authentication password for each interface, as well as set an area password for each IS-IS area to prevent unauthorized routers from injecting false routing information into the link-state database, or you can configure a type of IS-IS authentication--either IS-IS HMAC-MD5 or enhanced clear text authentication.

Configuring IS-IS Authentication

The following sections describe configuration tasks for IS-IS authentication. Two types of authentication are supported: IS-IS HMAC-MD5 and clear text. The task you perform depends on whether you are introducing authentication or migrating from an existing authentication scheme.

Before you can configure authentication, you must make the following decisions:

- Whether to configure authentication for the IS-IS instance and/or for individual IS-IS interfaces (both tasks are included in this section).
- At what level(s) authentication is to be used.
- What type of authentication (IS-IS HMAC-MD5 or clear text) is to be used.

- IS-IS Authentication Functionality, page 160
- Benefits of IS-IS Clear Text Authentication, page 161
- Benefits of IS-IS HMAC-MD5 Authentication, page 161

IS-IS Authentication Functionality

New style IS-IS authentication (IS-IS HMAC-MD5 and clear text) provides a number of advantages over the old style password configuration commands that were described in the previous sections, "Setting an Authentication Password for each Interface" and "Setting a Password at Level 1".

- Passwords are encrypted when the software configuration is displayed.
- Passwords are easier to manage and change.
- Passwords can be rolled over to new passwords without disrupting network operations.
- Non-disruptive authentication transitions are supported by allowing configuration which allowed the router to accept PDUs without authentication or with stale authentication information, yet send PDUs with current authentication. Such transitions are useful when you are migrating from no authentication to some type of authentication, when you are changing authentication type, and when you are changing keys.

IS-IS has five PDU types: link state PDU (LSP), LAN Hello, Point-to-Point Hello, complete sequence number PDU (CSNP), and partial sequence number PDU (PSNP). IS-IS HMAC-MD5 authentication or clear text password authentication can be applied to all five PDU types. The authentication can be enabled on different IS-IS levels independently. The interface-related PDUs (LAN Hello, Point-to-Point Hello, CSNP, and PSNP) can be enabled with authentication on different interfaces, with different levels and different passwords.

Either authentication mode or old password mode may be configured on a given scope (IS-IS instance or interface) and level--bit not both. However, different modes may be configured for different modes mat be configured for different scopes or levels. If mixed modes are intended, different keys should be used for different modes in order not to compromise the encrypted password in the PDUs.

Benefits of IS-IS Clear Text Authentication

IS-IS clear text (plain text) authentication provides the same functionality as is provided by using the **area-password** or **domain-password** command. However, use of clear text authentication takes advantage of the more flexible key management capabilities described above.

Benefits of IS-IS HMAC-MD5 Authentication

- IS-IS now supports MD5 authentication, which is more secure than clear text authentication. IS-IS HMAC-MD5 authentication adds an HMAC-MD5 digest to each IS-IS protocol data unit (PDU). HMAC is a mechanism for message authentication codes (MACs) using cryptographic hash functions. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain.
- MD5 authentication or clear text authentication can be enabled on Level 1 or Level 2 independently.
- Passwords can be rolled over to new passwords without disrupting routing messages.

For the purpose of network transition, you can configure the networking device to accept PDUs without authentication or with wrong authentication information, yet *send* PDUs with authentication. Such transition might be because you are migrating from no authentication to some type of authentication, you are changing authentication type, or you are changing keys.

Migrating to a New Authentication Type

Before you migrate from using one type of security authentication to another, all routers must be loaded with the new image that supports the new authentication type. The routers will continue to use the original authentication method until all routers have been loaded with the new image that supports the new authentication method, and all routers have been configured to use the new authentication method. Once all routers are loaded with the required image, you must follow the configuration steps for the desired new authentication method as described in the previous Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance, page 166. You also must decide whether to configure authentication for the IS-IS area or for individual IS-IS interfaces. Both tasks are included in the referenced section.

- Migration from Old Clear Text Authentication to HMAC-MD5 Authentication, page 161
- Migration from Old Clear Text Authentication to the New Clear Text Authentication, page 161

Migration from Old Clear Text Authentication to HMAC-MD5 Authentication

When you configure MD5 authentication, the **area-password** and **domain-password** command settings will be overridden automatically with the new authentication commands. When you configure MD5 authentication, the **isis password** command setting will be overridden automatically with the new authentication commands.

Migration from Old Clear Text Authentication to the New Clear Text Authentication

The benefits of migrating from the old method of clear text authentication to the new method of clear text authentication are as follows:

- Passwords are easier to change and maintain.
- Passwords can be encrypted when the system configuration is being displayed (if you use key management).

How to Enhance Security in an IS-IS Network

Setting an Authentication Password for each Interface

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isis password** *password* [**level-1**| **level-2**]
5. Repeat Step 4 for each interface password that you want to set.
6. **end**
7. **show ip interface** [*type number*] [**brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Enters interface configuration mode.
Step 4	**isis password** *password* [**level-1**| **level-2**] **Example:** `Router(config-if)# isis password sjpass level-1`	Configures the authentication password for an interface. • 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.
Step 5	Repeat Step 4 for each interface password that you want to set.	--
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show ip interface** [*type number*] [**brief**] **Example:** `Router# show ip interface serial 1`	Displays the usability status of interfaces configured for IP.

Setting a Password at Level 1

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [area-** *tag* **]**
4. **area-password** *password*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis salesarea`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**area-password** *password* **Example:** `Router(config-router)# area-password companyz`	Configures the IS-IS area authentication password, preventing unauthorized routers from injecting false routing information into the link-state database. • This password is inserted in Level 1 protocol data unit (PDU) link-state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

Setting a Password at Level 2

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **domain-password** *password* [**authenticate snp** {**validate** | **send-only**}]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis salesarea`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**domain-password** *password* [**authenticate snp** {**validate**	**send-only**}] **Example:** `Router(config-router)# domain-password company2`	Configures the IS-IS routing domain authentication password, preventing unauthorized routers from injecting false routing information into the link-state database. **Note** This password is inserted in Level 2 PDU link-state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs). If you specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, the IS-IS routing protocol will insert the password into sequence number PDUs (SNPs). **Note** If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, the IS-IS routing protocol does not insert the password into SNPs.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time

Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance

To achieve a smooth transition from one authentication method to another, allowing for continuous authentication of IS-IS PDUs, perform the task steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**
8. **router isis [area-** *tag* **]**
9. **authentication send-only** [**level-1** | **level-2**]
10. Repeat Steps 1 through 9 on each router that will communicate.
11. **authentication mode** {**md5** | **text**}[**level-1** | **level-2**]
12. **authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
13. Repeat Steps 11 and 12 on each router that will communicate.
14. **no authentication send-only**
15. Repeat Step 14 on each router that will communicate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain remote3754`	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 100`	Identifies an authentication key on a key chain. • The *key-id* argument must be a number.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string mno172`	Specifies the authentication string for a key. • The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to keychain configuration mode.
Step 7	**exit** **Example:** `Router(config-keychain)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 8	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis 1`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 9	**authentication send-only** [**level-1** | **level-2**] **Example:** `Router(config-router)# authentication send-only`	Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS PDUs being sent (not received).
Step 10	Repeat Steps 1 through 9 on each router that will communicate.	Use the same key string on each router.
Step 11	**authentication mode** {**md5** | **text**}[**level-1** | **level-2**] **Example:** `Router(config-router)# authentication mode md5`	Specifies the type of authentication used in IS-IS PDUs for the IS-IS instance. • Specify **md5** for MD5 authentication. • Specify **text** for clear text authentication.
Step 12	**authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Router(config-router)# authentication key-chain remote3754`	Enables MD5 authentication for the IS-IS instance.
Step 13	Repeat Steps 11 and 12 on each router that will communicate.	--
Step 14	**no authentication send-only** **Example:** `Router(config-router)# no authentication send-only`	Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS PDUs being sent and received. • In Step 9 you enable authentication to be performed only for IS-IS PDUs that are being sent. In Step 14 you enter the **no authentication send-only** command so that the authentication is now performed on PDUs sent and received.
Step 15	Repeat Step 14 on each router that will communicate.	--

Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface

To achieve a smooth transition from one authentication method to another, allowing for continuous authentication of IS-IS PDUs, perform the task steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **isis authentication send-only** [**level-1** | **level-2**]
10. Repeat Steps 1 through 9 on each router that will communicate.
11. **isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**]
12. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
13. Repeat Steps 11 and 12 on each router that will communicate.
14. **no isis authentication send-only**
15. Repeat Step 14 on each router that will communicate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain multistate87723`	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 201`	Identifies an authentication key on a key chain. • The *key-id* argument must be a number.

	Command or Action	Purpose
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string idaho`	Specifies the authentication string for a key. • The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to keychain configuration mode.
Step 7	**exit** **Example:** `Router(config-keychain)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface.
Step 9	**isis authentication send-only** [**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication send-only`	Specifies that authentication is performed only on PDUs being sent (not received) on a specified IS-IS interface.
Step 10	Repeat Steps 1 through 9 on each router that will communicate.	Use the same key string on each router.
Step 11	**isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication mode md5`	Specifies the type of authentication used for an IS-IS interface. • Specify **md5** for MD5 authentication. • Specify **text** for clear text authentication.
Step 12	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication key-chain multistate87723`	Enables MD5 authentication for an IS-IS interface.

	Command or Action	Purpose
Step 13	Repeat Steps 11 and 12 on each router that will communicate.	--
Step 14	**no isis authentication send-only** **Example:** `Router(config-if)# no isis authentication send-only`	Specifies that authentication is performed on PDUs being sent and received on a specified IS-IS interface.
Step 15	Repeat Step 14 on each router that will communicate.	--

Migrating to a New Authentication Method

SUMMARY STEPS

1. Load all routers with the image required to support the new, desired authentication method.
2. Configure the new authentication mode on both the interface and the IS-IS area by following the appropriate tasks in the Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time, page 166.

DETAILED STEPS

Step 1 Load all routers with the image required to support the new, desired authentication method.

Step 2 Configure the new authentication mode on both the interface and the IS-IS area by following the appropriate tasks in the Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time, page 166.

Configuring Authentication on a New Router Being Added to a Network That Already Has Authentication Configured

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**]
10. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain multistate87723`	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 201`	Identifies an authentication key on a key chain. • The *key-id* argument must be a number.

	Command or Action	Purpose
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string idaho`	Specifies the authentication string for a key. • The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to keychain configuration mode.
Step 7	**exit** **Example:** `Router(config-keychain)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface.
Step 9	**isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication mode md5`	Specifies the type of authentication used for an IS-IS interface. • Specify **md5** for MD5 authentication. • Specify **text** for clear text authentication.
Step 10	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication key-chain multistate87723`	Enables MD5 authentication for an IS-IS interface.

Configuration Examples for Enhancing Security in an IS-IS Network

- Example Configuring IS-IS HMAC-MD5 Authentication, page 174
- Example Configuring IS-IS Clear Text Authentication, page 174

Example Configuring IS-IS HMAC-MD5 Authentication

The following example configures a key chain and key for IS-IS HMAC-MD5 authentication for Ethernet interface 3 (on Hello PDUs) and for the IS-IS instance (on LSP, CSNP, and PSNP PDUs).

```
!
key chain cisco
 key 100
 key-string tasman-drive
!
interface Ethernet3
 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 cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain cisco level-1
!
```

Example Configuring IS-IS Clear Text Authentication

The following example configures a key chain and key for IS-IS clear text authentication for Ethernet interface 3 (on Hello PDUs) and for the IS-IS instance (on LSP, CSNP, and PSNP PDUs).

```
!
key chain cisco
 key 100
 key-string tasman-drive
!
interface Ethernet3
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication mode text level-1
 isis authentication key-chain cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode text level-1
 authentication key-chain cisco level-1
!
```

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*

Related Topic	Document Title
Key chains and key management	• *Cisco IOS IP Routing: Protocol-Independent Command Reference* • "Configuring IP Routing Protocol-Independent Features" module
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module

Standards

Standard	Title
None	--

RFCs

RFC	Title
RFC 1321	*The MD5 Message-Digest Algorithm*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*
RFC 3567	IS-IS Cryptographic Authentication

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Enhancing Security in an IS-IS Network

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

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

Table 9 Feature Information for Enhancing Security in an IS-IS Network

Feature Name	Releases	Feature Information
IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication	12.0(21)ST 12.0(22)S 12.2(11)S 12.2(13)T 12.2(14)S Cisco IOS XE 3.1.0 SG	The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5 digest to each Intermediate System-to-Intermediate System (IS-IS) protocol data unit (PDU). The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain. IS-IS clear text (plain text) authentication is enhanced so that passwords are encrypted when the software configuration is displayed and passwords are easier to manage and change.