



IP Routing: ISIS Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

IS-IS Overview and Basic Configuration 1

- Finding Feature Information 1
- Prerequisites for IS-IS Overview and Basic Configuration 2
- Information About IS-IS Overview and Basic Configuration 2
 - IS-IS Functional Overview 2
 - IS Address Assignment 2
 - IS-IS PDU Types 3
 - IIHs 3
 - LSPs 3
 - SNPs 4
 - IS-IS Supported Circuit Types 4
 - Operation of IS-IS on Point-to-Point Circuits 4
 - Operation of IS-IS on Multiaccess Circuits 5
 - IS-IS Election of the Designated Intermediate System 5
 - IS-IS Overview of LSPDB Synchronization 6
 - Handling of Newer LSPs 6
 - Handling of Older LSPs 7
 - Handling LSPs That Are the Same 7
 - IS-IS Overview of the Shortest Path Calculation 9
- How to Create Monitor and Make Changes to a Basic IS-IS Network 10
 - Enabling IS-IS as an IP Routing Protocol on the Device 10
 - Enabling IS-IS as an IP Routing Protocol on the Interface 11
- Monitoring IS-IS 13
 - Troubleshooting Tips 16
- Configuration Examples for a Basic IS-IS Network 16
 - Example: Configuring a Basic IS-IS Network 16
- Where to Go Next 18
- Additional References for IS-IS Overview and Basic Configuration 19

Feature Information for IS-IS Overview and Basic Configuration 20

Glossary 21

CHAPTER 2**Reducing Failure Detection Times in IS-IS Networks 23**

Finding Feature Information 23

Prerequisites for Reducing Failure Detection Times in IS-IS Networks 24

Information About Reducing Failure Detection Times in IS-IS Networks 24

 Importance of Fast Network Failure Detection 24

How to Reduce Failure Detection Times in IS-IS Networks 25

 Using IP Event Dampening to Decrease Failure Detection Times 25

 Tuning IS-IS Hello Parameters to Decrease Link Failure Detection Times 26

 Configuring an IS-IS Point-to-Point Adjacency over Broadcast Media 28

 Monitoring IS-IS Network Convergence Time 29

Configuration Examples for Reducing Failure Detection Times in IS-IS Networks 31

 Example Configuring IS-IS to Achieve Fast Convergence by Reducing Failure Detection
 Times 31

Where to Go Next 31

Additional References 31

Feature Information for Reducing Failure Detection Times in IS-IS Networks 32

CHAPTER 3**Enhancing Security in an IS-IS Network 35**

Finding Feature Information 35

Prerequisites for Enhancing Security in an IS-IS Network 35

Information About Enhancing Security in an IS-IS Network 36

 Importance of Preventing Unauthorized Information from Entering an IS-IS Network 36

 IS-IS Authentication Functionality 36

 Benefits of IS-IS Clear Text Authentication 37

 Benefits of IS-IS HMAC-MD5 Authentication 37

 Migration from Old Clear Text Authentication to HMAC-MD5 Authentication 37

 Migration from Old Clear Text Authentication to the New Clear Text
 Authentication 38

How to Enhance Security in an IS-IS Network 38

 Setting an Authentication Password for each Interface 38

 Setting a Password at Level 1 39

 Setting a Password at Level 2 40

Configuring IS-IS Authentication	42
Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time	42
Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance	42
Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface	45
Migrating to a New Authentication Type	47
Configuring Authentication on a New Router Being Added to a Network That Already Has Authentication Configured	48
Configuration Examples for Enhancing Security in an IS-IS Network	49
Example Configuring IS-IS HMAC-MD5 Authentication	49
Example Configuring IS-IS Clear Text Authentication	50
Additional References	50
Feature Information for Enhancing Security in an IS-IS Network	51

CHAPTER 4
Configuring Integrated IS-IS Protocol Shutdown Support Maintaining Configuration

Parameters	53
Finding Feature Information	53
Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	54
Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	54
IS-IS Process and Adjacencies	54
PDU Packet Types in IS-IS Routing	55
How to Create, Monitor and Make Changes to Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	56
Enabling IS-IS as an IP Routing Protocol on the Device	56
Enabling IS-IS as an IP Routing Protocol on the Interface	57
Monitoring IS-IS	59
Troubleshooting Tips	62
Shutting Down IS-IS to Make Changes to Your IS-IS Network	62
Shutting Down IS-IS in Interface Mode	63
Shutting Down IS-IS in Router Mode	64
Configuration Examples for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	65
Example: Configuring a Basic IS-IS Network	65

Example: Shutting Down IS-IS in Interface Mode	67
Example: Shutting Down IS-IS in Router Mode	67
“Where to Go Next	68
Additional References for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	69
Feature Information for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	70

CHAPTER 5**IS-IS Support for Route Tags 71**

Finding Feature Information	71
Prerequisites for IS-IS Support for Route Tags	71
Information About IS-IS Support for Route Tags	72
Route Redistribution	72
IS-IS Caching of Redistributed Routes	72
Prioritize the Update of IP Prefixes in the RIB to Reduce Alternate-Path Calculation Time	72
IS-IS Priority-Driven IP Prefix RIB Installation	72
IS-IS Routes Tagged to Control Their Redistribution	73
How Route Summarization Can Enhance Scalability in IS-IS Networks	73
Benefits of IS-IS Route Tags	74
IS-IS Route Tag Characteristics	74
IS-IS Route Leaking Based on a Route Tag	74
Limit the Number of Routes That Are Redistributed into IS-IS	74
Streamline the Routing Table Update Process by Excluding Connected IP Prefixes from LSP Advertisements	75
Small-Scale Method to Reduce IS-IS Convergence Time	75
Large-Scale Method to Reduce IS-IS Convergence Time	75
Benefit of Excluding IP Prefixes of Connected Networks in LSP Advertisements	75
How to Configure IS-IS Support for Route Tags	76
Configuring IS-IS Incremental SPF	76
Assigning a High Priority Tag to an IS-IS IP Prefix	77
Troubleshooting Tips	79
Tagging Routes for Networks Directly Connected to an Interface	79
What to Do Next	81
Tagging Routes Using a Route Map	81

What to Do Next	83
Tagging a Summary Address	83
What to Do Next	85
Using the Tag to Set Values and or Redistribute Routes	85
Limiting the Number of IS-IS Redistributed Routes	87
Requesting a Warning About the Number of Prefixes Redistributed into IS-IS	88
Excluding Connected IP Prefixes on a Small Scale	90
Excluding Connected IP Prefixes on a Large Scale	92
Monitoring IS-IS Network Convergence Time	95
Configuration Examples for IS-IS Support for Route Tags	97
Example Assigning a High Priority Tag Value to an IS-IS IP Prefix	97
Example Tagging Routes for Networks Directly Connected to an Interface and Redistributing Them	97
Example: Redistributing IS-IS Routes Using a Route Map	97
Example: Tagging a Summary Address and Applying a Route Map	98
Example Filtering and Redistributing IS-IS Routes Using an Access List and a Route Map	99
Example: IS-IS Limit on the Number of Redistributed Routes	100
Example: Requesting a Warning About the Number of Redistributed Routes	100
Example Excluding Connected IP Prefixes on a Small Scale	100
Example Excluding Connected IP Prefixes on a Large Scale	101
Where to Go Next	101
Additional References	101
Feature Information for Reducing Alternate-Path Calculation Times in IS-IS Networks	102

CHAPTER 6
IS-IS Multiarea Support 105

Finding Feature Information	105
Restrictions for IS-IS Multiarea Support	105
Information About IS-IS Multiarea Support	106
Overview of IS-IS Multiarea Support	106
Merging External Areas	108
Benefits of IS-IS Multiarea Support	109
How to Configure IS-IS Multiarea Support	109
Assigning IS-IS Areas	109
Enabling CLNS Routing for an Area on an Interface	110
Enabling Partitioning Avoidance	111

Configuration Examples for IS-IS Multiarea Support **112**

- Example Assigning IS-IS Areas **112**
- Example Enabling CLNS Routing for an Area on an Interface **113**
- Example Enabling Partitioning Avoidance **113**

Additional References for IS-IS Multiarea Support **113**

Feature Information for IS-IS Multiarea Support **114**

Glossary **115**



IS-IS Overview and Basic Configuration

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 device. 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, page 1](#)
- [Prerequisites for IS-IS Overview and Basic Configuration, page 2](#)
- [Information About IS-IS Overview and Basic Configuration, page 2](#)
- [How to Create Monitor and Make Changes to a Basic IS-IS Network, page 10](#)
- [Configuration Examples for a Basic IS-IS Network, page 16](#)
- [Where to Go Next, page 18](#)
- [Additional References for IS-IS Overview and Basic Configuration, page 19](#)
- [Feature Information for IS-IS Overview and Basic Configuration, page 20](#)
- [Glossary, page 21](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for IS-IS Overview and Basic Configuration

- This document assumes knowledge of CLNS, IPv4, and IPv6.
- The amount of knowledge required for each technology is dependent on your deployment. 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 devices (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 devices, showing what neighbors should be expected in the adjacencies table.

Information About IS-IS Overview and Basic Configuration

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 device in Open Systems Interconnection (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 devices regardless of whether they are in the same Level-1 area. The set of Level-2 devices 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 devices in the same area. When the IS operates at Level 2, the system ID must be unique among all devices in the domain.

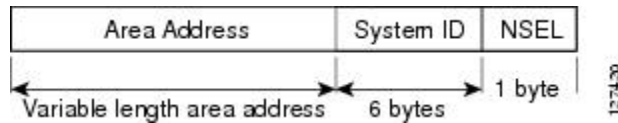
**Note**

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: NET Format



IS-IS PDU Types

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

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 device on that circuit.
- Level-2 LAN IIHs—These are sent on multiaccess circuits when the sending IS operates as a Level-2 device 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 value is always 0 except when the LSP is a pseudonode LSP (see “Operation of IS-IS on Multiaccess Circuits” section).

- 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 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” section.

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 and 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.

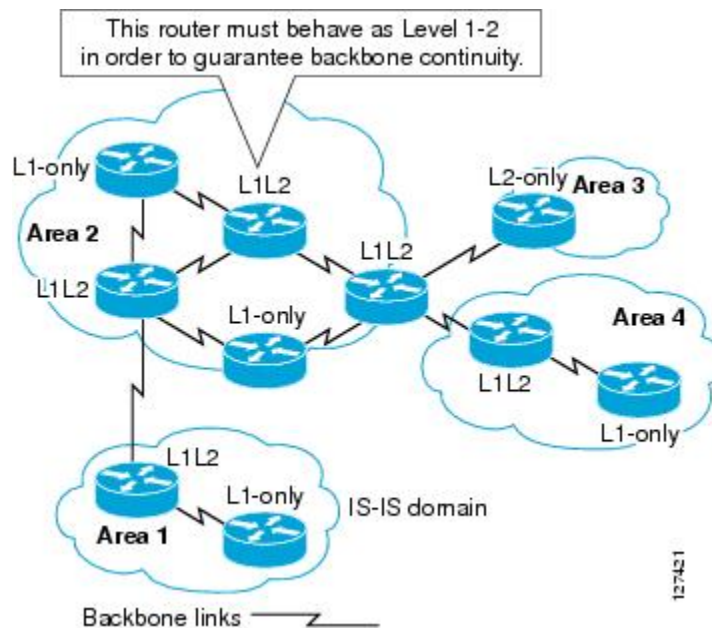
ISs form separate adjacencies for each level with neighbor ISs on the circuit.

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 devices 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: Level 1, Level 2, and Level 1-2 Devices in an IS-IS Network Topology



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

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 “Handling of Newer LSPs” section 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.

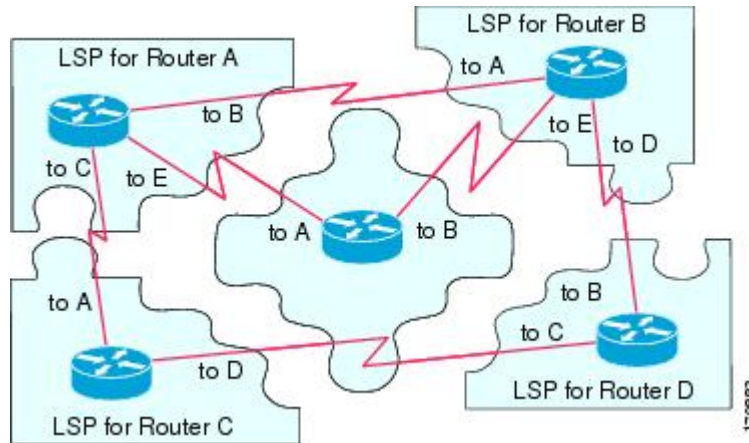
In a multiaccess circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

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 devices in an area or to all Level-2 devices in a Level-2 subdomain.

Figure 3: IS-IS Network Map

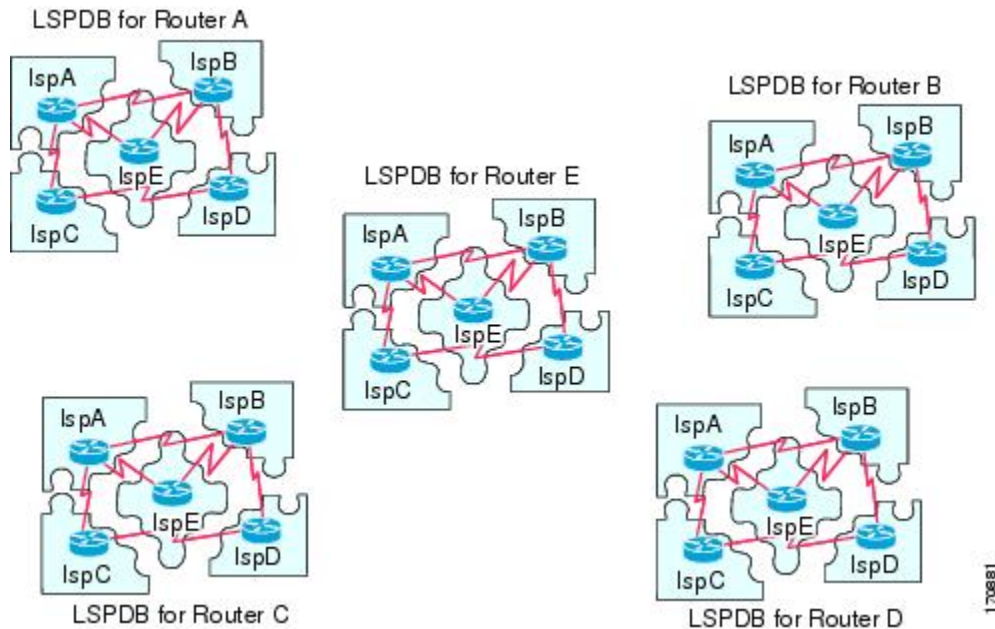


The figure below shows each device in the IS-IS network with its fully updated link-state database, after the adjacencies have been formed among the neighbor devices.

**Note**

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

Figure 4: IS-IS Devices with Synchronized LSPDBs



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 SPF calculations 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 devices 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. LSP 0 has special properties, including the significance of the setting of the ATT bit to indicate attachment to other areas. When LSPs that are numbered 1 through 255 have the ATT bit set, it is not significant.

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

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

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis <i>[area-tag]</i> Example: Device(config)# router isis	Assigns a tag to an IS-IS process. Enters router configuration mode. <ul style="list-style-type: none"> • 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 device.
Step 4	net <i>network-entity-title</i>	Configures the NET on the device.

	Command or Action	Purpose
	Example: <pre>Device(config-router)# net 49.0001.0000.0000.000b.00</pre>	<ul style="list-style-type: none"> The NET identifies the device for IS-IS.
Step 5	end Example: <pre>Device(config-router)# end</pre>	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: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: <pre>Device(config)# interface GigabitEthernet 1/0/2</pre>	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	<p>ip address <i>ip-address</i> <i>mask</i> [<i>secondary</i>]</p> <p>Example:</p> <pre>Device(config-if)# ip address 172.16.1.27 255.255.255.0</pre>	Sets the primary IP address on the interface.
Step 5	<p>ip router isis [<i>area-tag</i>]</p> <p>Example:</p> <pre>Device(config-if)# ip router isis company1</pre>	<p>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).</p> <ul style="list-style-type: none"> • Use the <i>area-tag</i> argument to specify to which IS-IS process the device belongs. • If there is more than one IS-IS process on the device, 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	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	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 area-tag is-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**] [**11**] [**12**] [**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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	isis display delimiter [return <i>count</i> character <i>count</i>] Example: Device(config)# isis display delimiter return 3	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: Device(config)# exit	Returns to privileged EXEC mode.
Step 5	show ip protocols Example: Device# show ip protocols	Displays the parameters and current state of the active routing protocol process. <ul style="list-style-type: none"> 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 area-tag is-neighbors [<i>type number</i>] [detail] Example: Device# show clns is-neighbors detail	Displays IS-IS information for IS-IS device adjacencies.
Step 7	show clns interface [<i>type number</i>] Example: Device# show clns interface	List the CLNS-specific information about each interface.
Step 8	show clns area-tag neighbors [<i>type number</i>] [area] [detail] Example: Device# show clns area3 neighbors	Displays both ES and IS neighbors. <ul style="list-style-type: none"> The show clns neighbor command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your devices, showing what neighbors should be expected in the adjacencies table, to facilitate verification.
Step 9	show clns area-tag traffic Example: Device# 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: <ul style="list-style-type: none"> 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> To check for partial route calculations (PRCs), enter the show cns 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 [<i>ip-address</i> [<i>mask</i>]] [[longer-prefixes] <i>protocol</i> [<i>process-id</i>] list [<i>access-list-number</i> <i>access-list-name</i>] static download]] Example: Device# show ip route 172.16.0.21	Displays the current state of the routing table.
Step 11	show isis [<i>process-tag</i>] database [level-1] [level-2] [l1] [l2] [detail] [lspid] Example: Device# show isis database detail	Displays additional information about the IS-IS database. <ul style="list-style-type: none"> Displays the link-state database for Level-1 and Level-2, the contents for each LSP, and the link-state protocol PDU identifier.
Step 12	show isis database verbose Example: Device# 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: Device# 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 [<i>area-tag</i>] [ipv6 *] spf-log Example: Device# show isis spf-log	Displays how often and why the device has run a full shortest path first (SPF) calculation. <ul style="list-style-type: none"> If the device 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.

	Command or Action	Purpose
Step 15	show isis [<i>process-tag</i>] [<i>ipv6</i> *] topology Example: Device# show isis topology	Displays a list of all connected devices in all areas.
Step 16	show isis [<i>area-tag</i>] neighbors [<i>detail</i>] Example: Device# show isis neighbors detail	Displays IS-IS adjacency information. <ul style="list-style-type: none"> 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 devices, 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 about the IS-IS adjacencies that have formed.

```
Device1# show isis neighbors detail

System Id      Type Interface IP Address      State Holdtime Circuit Id
Device2        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

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.

Configuration Examples for a Basic IS-IS Network

Example: Configuring a Basic IS-IS Network

The following example shows how to configure three devices to run IS-IS as an IP routing protocol.

Device 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

```

Device 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

```

Device 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 devices are connected within the IS-IS network:

```
DeviceB# show isis topology
```

```

IS-IS paths to level-1 routers
System Id      Metric  Next-Hop      Interface  SNPA
DeviceA        10     DeviceA       Se2/0      *HDLC*
DeviceB        --
DeviceC        10     DeviceC       Se5/0      *HDLC*
IS-IS paths to level-2 routers
System Id      Metric  Next-Hop      Interface  SNPA
DeviceA        10     DeviceA       Se2/0      *HDLC*
DeviceB        --
DeviceC        10     DeviceC       Se5/0      *HDLC*

```

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

```
DeviceB# show isis database
```

```

IS-IS Level-1 Link State Database:
LSPID      LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
DeviceA.00-00  0x00000005  0x1A1D        1063          0/0/0
DeviceB.00-00  * 0x00000006  0xD15B        1118          0/0/0
DeviceC.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
DeviceA.00-00  0x00000008  0x0BF4        1136          0/0/0
DeviceB.00-00  * 0x00000008  0x1701        1137          0/0/0
DeviceC.00-00  0x00000004  0x3624        1133          0/0/0

```

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

```
DeviceB# 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
```

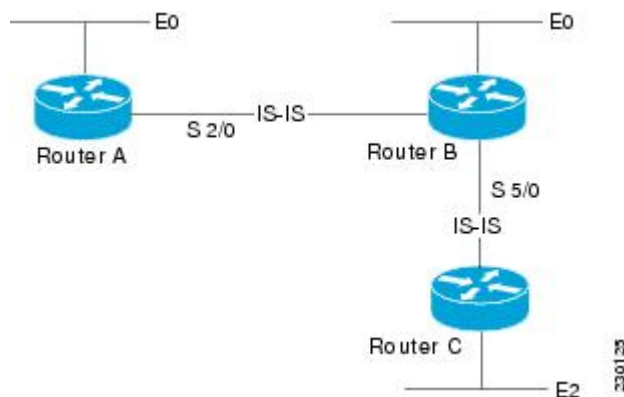
The **show isis spf-log** command displays logs of Level 1 and Level 2 LSPs including time of occurrence, duration, count, and the event that triggered the LSP.

```
DeviceC## show isis spf-log

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

The figure below illustrates the sample configuration.

Figure 5: IS-IS Routing



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 for IS-IS Overview and Basic Configuration

Related Documents

Related Topic	Document Title
IPv6 Routing: IS-IS Support for IPv6	"IPv6 Routing: IS-IS Support for IPv6 " module
IPv6 Routing: Route Redistribution	"IPv6 Routing: Route Redistribution" module
IPv6 Routing: IS-IS Support for IPv6	"IPv6 Routing: IS-IS Support for IPv6 " module

Standards

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

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	<i>Use of OSI IS-IS for Routing in TCP/IP and Dual Environments</i> (http://www.ietf.org/rfc/rfc1195.txt)

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 Overview and Basic Configuration

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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 1: Feature Information for IS-IS Overview and Basic Configuration

Feature Name	Releases	Feature Information
IS-IS Overview and Basic Configuration	Cisco IOS XE 3.2SE	<p>Integrated Intermediate System-to-Intermediate System (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 device. That map is then used to calculate the shortest path to destinations.</p> <p>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.</p>

Glossary

area —A physically connected portion of a routing domain in which all devices 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 device.

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 devices 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.



CHAPTER 2

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 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, page 23](#)
- [Prerequisites for Reducing Failure Detection Times in IS-IS Networks, page 24](#)
- [Information About Reducing Failure Detection Times in IS-IS Networks, page 24](#)
- [How to Reduce Failure Detection Times in IS-IS Networks, page 25](#)
- [Configuration Examples for Reducing Failure Detection Times in IS-IS Networks, page 31](#)
- [Where to Go Next, page 31](#)
- [Additional References, page 31](#)
- [Feature Information for Reducing Failure Detection Times in IS-IS Networks, page 32](#)

Finding Feature Information

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

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

Prerequisites for 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

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 resigaled 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

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 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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 1/0/2	Enters interface configuration mode.
Step 4	dampening [<i>half-life-period reuse-threshold</i>] [<i>suppress-threshold max-suppress-time</i> [<i>restart-penalty</i>]] Example: Device(config-if)# dampening	Enables interface dampening. <ul style="list-style-type: none"> • Entering the dampening command without any keywords or arguments enables interface dampening with the default configuration parameters. <p>Note The default values for the <i>half-life-period</i>, <i>reuse-threshold</i>, <i>suppress-threshold</i>, <i>max-suppress-time</i>, and <i>restart-penalty</i> arguments are 5, 1000, 2000, 20, and 2000, respectively.</p>

	Command or Action	Purpose
		<ul style="list-style-type: none"> When the timer for the <i>restart-penalty</i> argument is manually configured, the values must be manually entered for all arguments.
Step 5	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	show dampening interface Example: Device# show dampening interface	Displays a summary of dampened interfaces.
Step 7	show interface dampening Example: Device# 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: Device> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface interface-type interface-number Example: Device(config)# interface GigabitEthernet 1/0/2	Configures an interface type and enters interface configuration mode.
Step 4	isis hello-interval {seconds minimal} [level-1 level-2] Example: Device(config-if)# isis hello-interval 5 level-1	Specifies the length of time between the sending of IS-IS hello PDUs. <ul style="list-style-type: none"> The default value is 10. The hello interval multiplied by the hello multiplier equals the hold time. If the minimal keyword is specified, the hold time is 1 second and the system computes the hello interval based on the hello multiplier. The hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because only a single type of hello PDU is sent on serial links, it is independent of Level 1 or Level 2.) The level-1 and level-2 keywords are used on X.25, SMDS, and Frame Relay multiaccess networks or LAN interfaces. <p>Note A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network, due to false failure detection events. A slower hello interval saves bandwidth and CPU. Especially when used in combination with a higher hello multiplier, this configuration may increase overall network stability, but has typical slower network convergence as a consequence.</p>
Step 5	isis hello-multiplier multiplier [level-1 level-2] Example: Device(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. <ul style="list-style-type: none"> The default value is 3. A multiplier value of 1 is very aggressive--we recommend a value of at least 3.
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Configuring an IS-IS Point-to-Point Adjacency over Broadcast Media

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.



Note

Having a multipoint interface instead of a point-to-point interface 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: Device> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-type interface-number</i> Example: Device(config)# interface GigabitEthernet 1/0/2	Configures an interface type and enters interface configuration mode.
Step 4	isis network point-to-point Example: Device(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.

	Command or Action	Purpose
Step 5	end Example: Device(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] [I1] [I2] [detail] [lspid]**
6. **show isis [process-tag] route**
7. **show isis spf-log**
8. **show isis [process-tag] topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	isis display delimiter [return count character count] Example: Device(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.

	Command or Action	Purpose
Step 4	exit Example: Device(config)# exit	Returns to privileged EXEC mode.
Step 5	show isis database [level-1] [level-2] [11] [12] [detail] [lspid] Example: Device# show isis database detail	Displays the IS-IS link-state database.
Step 6	show isis [process-tag] route Example: Device# show isis financetag route	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	show isis spf-log Example: Device# 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: Device# show isis financetag topology	Displays a list of all connected routers in all areas. <ul style="list-style-type: none"> • If a process tag is specified, output is limited to the specified routing process. When "null" is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.

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

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	<i>Cisco IOS IP Routing: ISIS Command Reference</i>
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 [http://www.cisco.com/cisco/featurenavigator](#). An account on Cisco.com is not required.

Table 2: Feature Information for Reducing Failure Detection Times in IS-IS Networks

Feature Name	Software Releases	Feature Information
IS-IS Support for BFD over IPv4	Cisco IOS XE 3.2SE	<p>Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and convergence time will be consistent and predictable.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.</p>
Integrated IS-IS Point-to-Point Adjacency over Broadcast Media	Cisco IOS XE 3.2SE	<p>When a network consists of only two networking devices connected to broadcast media and uses the integrated IS-IS protocol, it is better for the system to handle the link as a point-to-point link instead of as a broadcast link. This feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.</p>



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, page 35](#)
- [Prerequisites for Enhancing Security in an IS-IS Network, page 35](#)
- [Information About Enhancing Security in an IS-IS Network, page 36](#)
- [How to Enhance Security in an IS-IS Network, page 38](#)
- [Configuration Examples for Enhancing Security in an IS-IS Network, page 49](#)
- [Additional References, page 50](#)
- [Feature Information for Enhancing Security in an IS-IS Network, page 51](#)

Finding Feature Information

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

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

Prerequisites for 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 devices 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.

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

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--but not both. However, different modes may be configured for different modes may 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.

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, on page 42](#). 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.



Note

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.

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Enters interface configuration mode.
Step 4	isis password <i>password</i> [level-1 level-2] Example: Device(config-if)# isis password sjpass level-1	Configures the authentication password for an interface. <ul style="list-style-type: none"> • 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: Device(config-if)# end	Returns to privileged EXEC mode.
Step 7	show ip interface [<i>type number</i>] [brief] Example: Device# show ip interface gigabitethernet 0/0/0	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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis [area- tag] Example: Device(config)# router isis salesarea	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	area-password password Example: Device(config-router)# area-password companyz	Configures the IS-IS area authentication password. <ul style="list-style-type: none"> • Using the area-password command on all devices in an area will prevent unauthorized devices 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: Device(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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis <i>[area-tag]</i> Example: Device (config)# router isis salesarea	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	domain-password <i>password</i> [authenticate snp {validate send-only}] Example: Device (config-router) # domain-password company2	Configures the IS-IS routing domain authentication password. <p>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.</p> <p>Note Using the domain-password command on all devices in an area will prevent unauthorized devices from injecting false routing information into the link-state database.</p> <p>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).</p>
Step 5	end Example: Device (config-router) # end	Returns to privileged EXEC mode.

Configuring IS-IS Authentication

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

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

Before You Begin

In order to use HMAC-MD5 or clear text authentication with encrypted keys, the Integrated IS-IS routing protocol must be 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. **router isis** [*area-tag*]
9. **authentication send-only** [*level-1* | *level-2*]
10. Repeat Steps 1 through 9 on each device 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 device that will communicate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	key chain <i>name-of-chain</i> Example: Device(config)# key chain remote3754	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Device(config-keychain)# key 100	Identifies an authentication key on a key chain. <ul style="list-style-type: none"> • The <i>key-id</i> argument must be a number.
Step 5	key-string <i>text</i> Example: Device(config-keychain-key)# key-string mno172	Specifies the authentication string for a key. <ul style="list-style-type: none"> • The <i>text</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	exit Example: Device(config-keychain-key)# exit	Returns to keychain configuration mode.
Step 7	exit Example: Device(config-keychain)# exit	Returns to global configuration mode.
Step 8	router isis [area- tag] Example: Device(config)# router isis 1	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 9	authentication send-only [level-1 level-2] Example: Device(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 device that will communicate.	Use the same key string on each device.

	Command or Action	Purpose
Step 11	<p>authentication mode {md5 text} [level-1 level-2]</p> <p>Example:</p> <pre>Device(config-router)# authentication mode md5</pre>	<p>Specifies the type of authentication used in IS-IS PDUs for the IS-IS instance.</p> <ul style="list-style-type: none"> • Specify md5 for MD5 authentication. • Specify text for clear text authentication.
Step 12	<p>authentication key-chain <i>name-of-chain</i> [level-1 level-2]</p> <p>Example:</p> <pre>Device(config-router)# authentication key-chain remote3754</pre>	<p>Enables MD5 authentication for the IS-IS instance.</p>
Step 13	<p>Repeat Steps 11 and 12 on each router that will communicate.</p>	--
Step 14	<p>no authentication send-only</p> <p>Example:</p> <pre>Device(config-router)# no authentication send-only</pre>	<p>Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS PDUs being sent and received.</p> <ul style="list-style-type: none"> • 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	<p>Repeat Step 14 on each device that will communicate.</p>	--

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

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 device 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 device that will communicate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	key chain <i>name-of-chain</i> Example: Device(config)# key chain multistate87723	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Device(config-keychain)# key 201	Identifies an authentication key on a key chain. <ul style="list-style-type: none"> • The <i>key-id</i> argument must be a number.

	Command or Action	Purpose
Step 5	key-string <i>text</i> Example: Device(config-keychain-key)# key-string idaho	Specifies the authentication string for a key. <ul style="list-style-type: none"> • The <i>text</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	exit Example: Device(config-keychain-key)# exit	Returns to keychain configuration mode.
Step 7	exit Example: Device(config-keychain)# exit	Returns to global configuration mode.
Step 8	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Configures an interface.
Step 9	isis authentication send-only [level-1 level-2] Example: Device(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 device that will communicate.	Use the same key string on each device.
Step 11	isis authentication mode { md5 text } [level-1 level-2] Example: Device(config-if)# isis authentication mode md5	Specifies the type of authentication used for an IS-IS interface. <ul style="list-style-type: none"> • Specify md5 for MD5 authentication. • Specify text for clear text authentication.
Step 12	isis authentication key-chain <i>name-of-chain</i> [level-1 level-2] Example: Device(config-if)# isis authentication key-chain multistate87723	Enables MD5 authentication for an IS-IS interface.
Step 13	Repeat Steps 11 and 12 on each router that will communicate.	--

	Command or Action	Purpose
Step 14	no isis authentication send-only Example: <pre>Device(config-if)# no isis authentication send-only</pre>	Specifies that authentication is performed on PDUs being sent and received on a specified IS-IS interface.
Step 15	Repeat Step 14 on each device that will communicate.	--

Migrating to a New Authentication Type

SUMMARY STEPS

1. Load all devices 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](#), on page 42.

DETAILED STEPS

-
- Step 1** Load all devices 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](#), on page 42.
-

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	key chain <i>name-of-chain</i> Example: Device(config)# key chain multistate87723	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	key <i>key-id</i> Example: Device(config-keychain)# key 201	Identifies an authentication key on a key chain. <ul style="list-style-type: none"> • The <i>key-id</i> argument must be a number.
Step 5	key-string <i>text</i> Example: Device(config-keychain-key)# key-string idaho	Specifies the authentication string for a key. <ul style="list-style-type: none"> • The <i>text</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.

	Command or Action	Purpose
Step 6	exit Example: Device(config-keychain-key)# exit	Returns to keychain configuration mode.
Step 7	exit Example: Device(config-keychain)# exit	Returns to global configuration mode.
Step 8	interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Configures an interface.
Step 9	isis authentication mode {md5 text} [level-1 level-2] Example: Device(config-if)# isis authentication mode md5	Specifies the type of authentication used for an IS-IS interface. <ul style="list-style-type: none"> • Specify md5 for MD5 authentication. • Specify text for clear text authentication.
Step 10	isis authentication key-chain <i>name-of-chain</i> [level-1 level-2] Example: Device(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

The following example configures a key chain and key for IS-IS HMAC-MD5 authentication for GigabitEthernet interface 3/0/0 (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 GigabitEthernet3/0/0
 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 GigabitEthernet interface 3/0/0 (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 GigabitEthernet3/0/0
 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
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
IPv6 Routing: IS-IS Multitopology Support for IPv6	“ <i>Reducing Link Failure and Topology Change Notification Times in IS-IS Networks</i> ” module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	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

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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 3: 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	Cisco IOS XE 3.2SE	<p>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.</p> <p>This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.</p>



Configuring Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

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.

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 are 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, page 53](#)
- [Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, page 54](#)
- [Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , page 54](#)
- [How to Create, Monitor and Make Changes to Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , page 56](#)
- [Configuration Examples for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , page 65](#)
- [“Where to Go Next, page 68](#)
- [Additional References for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, page 69](#)
- [Feature Information for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , page 70](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

- 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 devices (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 devices, showing what neighbors should be expected in the adjacencies table. For more information about verifying IS-IS configuration and formed adjacencies, see “Monitoring IS-IS”.

Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

IS-IS Process and Adjacencies

IS-IS requires some configuration on both the device and the interface. An IS-IS process is created when you enable IS-IS on a device and define a specific tag to identify that routing process. Interfaces configured with a specific tag will be part of the corresponding device process. More than one IS-IS process can run on a device 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 devices 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 devices from all areas. The areas are connected to local areas. Within a local area, devices know how to reach all system IDs. Between areas, devices know how to reach the backbone, and the backbone devices know how to reach other areas.

Devices establish Level 1 adjacencies to perform routing within a local area (intra-area routing). Devices 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 device instance, use the **is-type** command in device configuration mode to remove the Level-2 capability. You can also use the **is-type** command to configure a different device instance as a Level-2 device.

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 devices 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 device. 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 device.

IS-IS LSPs include specific information about the device’s attachments. The following information is included in multiple Type Length Value (TLV) fields in the main body of the LSP:

- The links to neighbor device 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 Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

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

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis [<i>area-tag</i>] Example: Device(config)# router isis	Assigns a tag to an IS-IS process. Enters router configuration mode. <ul style="list-style-type: none"> • 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 device.
Step 4	net <i>network-entity-title</i> Example: Device(config-router)# net 49.0001.0000.0000.000b.00	Configures the NET on the device. <ul style="list-style-type: none"> • The NET identifies the device for IS-IS.

	Command or Action	Purpose
Step 5	end Example: Device(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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 1/0/2	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	<p>ip address <i>ip-address</i> <i>mask</i> [<i>secondary</i>]</p> <p>Example:</p> <pre>Device(config-if)# ip address 172.16.1.27 255.255.255.0</pre>	Sets the primary IP address on the interface.
Step 5	<p>ip router isis [<i>area-tag</i>]</p> <p>Example:</p> <pre>Device(config-if)# ip router isis company1</pre>	<p>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).</p> <ul style="list-style-type: none"> • Use the <i>area-tag</i> argument to specify to which IS-IS process the device belongs. • If there is more than one IS-IS process on the device, 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	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	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 area-tag is-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**] [**11**] [**12**] [**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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	isis display delimiter [return <i>count</i> character <i>count</i>] Example: Device(config)# isis display delimiter return 3	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: Device(config)# exit	Returns to privileged EXEC mode.
Step 5	show ip protocols Example: Device# show ip protocols	Displays the parameters and current state of the active routing protocol process. <ul style="list-style-type: none"> 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 area-tag is-neighbors [<i>type number</i>] [detail] Example: Device# show clns is-neighbors detail	Displays IS-IS information for IS-IS device adjacencies.
Step 7	show clns interface [<i>type number</i>] Example: Device# show clns interface	List the CLNS-specific information about each interface.
Step 8	show clns area-tag neighbors [<i>type number</i>] [area] [detail] Example: Device# show clns area3 neighbors	Displays both ES and IS neighbors. <ul style="list-style-type: none"> The show clns neighbor command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your devices, showing what neighbors should be expected in the adjacencies table, to facilitate verification.
Step 9	show clns area-tag traffic Example: Device# show clns area3 traffic	Displays traffic statistics. <p>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:</p> <ul style="list-style-type: none"> 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> To check for partial route calculations (PRCs), enter the show cns 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 [<i>ip-address</i> [<i>mask</i>]] [[longer-prefixes] <i>protocol</i> [<i>process-id</i>] list [<i>access-list-number</i> <i>access-list-name</i>] static download]] Example: Device# show ip route 172.16.0.21	Displays the current state of the routing table.
Step 11	show isis [<i>process-tag</i>] database [level-1] [level-2] [l1] [l2] [detail] [lspid] Example: Device# show isis database detail	Displays additional information about the IS-IS database. <ul style="list-style-type: none"> Displays the link-state database for Level-1 and Level-2, the contents for each LSP, and the link-state protocol PDU identifier.
Step 12	show isis database verbose Example: Device# 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: Device# 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 [<i>area-tag</i>] [ipv6 *] spf-log Example: Device# show isis spf-log	Displays how often and why the device has run a full shortest path first (SPF) calculation. <ul style="list-style-type: none"> If the device 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.

	Command or Action	Purpose
Step 15	show isis [<i>process-tag</i>] [<i>ipv6</i> *] topology Example: Device# show isis topology	Displays a list of all connected devices in all areas.
Step 16	show isis [<i>area-tag</i>] neighbors [detail] Example: Device# show isis neighbors detail	Displays IS-IS adjacency information. <ul style="list-style-type: none"> 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 devices, 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 about the IS-IS adjacencies that have formed.

```
Device1# show isis neighbors detail

System Id      Type Interface IP Address      State Holdtime Circuit Id
Device2        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

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 device 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 reenabling 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 device 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

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0	Configures an interface and enters interface configuration mode.
Step 4	isis protocol shutdown Example: Device(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 device.

	Command or Action	Purpose
Step 5	end Example: Device(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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis <i>area-tag</i> Example: Device(config)# router isis 1	Enables the IS-IS routing protocol and specifies an IS-IS process. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	protocol shutdown Example: Device(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.

	Command or Action	Purpose
Step 5	end Example: Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

Example: Configuring a Basic IS-IS Network

The following example shows how to configure three devices to run IS-IS as an IP routing protocol.

Device 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
```

Device 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
```

Device 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 devices are connected within the IS-IS network:

```
DeviceB# show isis topology
```

```
IS-IS paths to level-1 routers
System Id      Metric      Next-Hop      Interface      SNPA
DeviceA        10          DeviceA       Se2/0          *HDLC*
DeviceB        --
DeviceC        10          DeviceC       Se5/0          *HDLC*
IS-IS paths to level-2 routers
System Id      Metric      Next-Hop      Interface      SNPA
DeviceA        10          DeviceA       Se2/0          *HDLC*
DeviceB        --
DeviceC        10          DeviceC       Se5/0          *HDLC*
```

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

```
DeviceB# show isis database
```

```
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
DeviceA.00-00  0x00000005  0x1A1D        1063          0/0/0
DeviceB.00-00  * 0x00000006  0xD15B        1118          0/0/0
DeviceC.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
DeviceA.00-00  0x00000008  0x0BF4        1136          0/0/0
DeviceB.00-00  * 0x00000008  0x1701        1137          0/0/0
DeviceC.00-00  0x00000004  0x3624        1133          0/0/0
```

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

```
DeviceB# 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
```

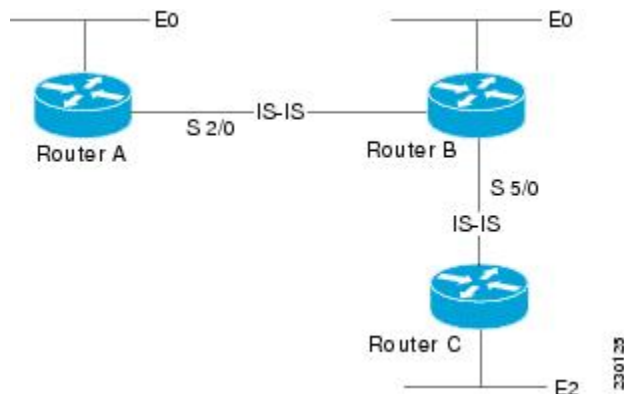
The **show isis spf-log** command displays logs of Level 1 and Level 2 LSPs including time of occurrence, duration, count, and the event that triggered the LSP.

```
DeviceC## show isis spf-log
```

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

The figure below illustrates the sample configuration.

Figure 6: IS-IS Routing



Example: Shutting Down IS-IS in Interface Mode

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

```
Device# 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:

```
Device# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Device(config)# Interface GigabitEthernet 0/0
```

```
Device(config-if)# isis protocol shutdown
```

```
Device(config-if)# end
```

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

```
Device# 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 device output shows that the device has two IS-IS adjacencies:

```
Device# 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:

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

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

```
Device# 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:

```
Device(config)# router isis areal
Device(config-router)# no protocol shutdown
Device(config-router)# end
Device# 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 for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	<i>Cisco IOS IP Routing: ISIS Command Reference</i>
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
<ul style="list-style-type: none"> • 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	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments <i>Use of OSI IS-IS for Routing in TCP/IP and Dual Environments</i> (http://www.ietf.org/rfc/rfc1195.txt)

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 Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 4: Feature Information for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

Feature Name	Releases	Feature Information
Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	Cisco IOS XE Release 3.2SE	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.



IS-IS Support for Route Tags

The IS-IS Support for Route Tags feature enables you to tag Intermediate System-to-Intermediate System (IS-IS) route prefixes and use those tags in a route map to control IS-IS route redistribution or route leaking. The results are network scalability and faster convergence for device updates.

- [Finding Feature Information, page 71](#)
- [Prerequisites for IS-IS Support for Route Tags, page 71](#)
- [Information About IS-IS Support for Route Tags, page 72](#)
- [How to Configure IS-IS Support for Route Tags, page 76](#)
- [Configuration Examples for IS-IS Support for Route Tags, page 97](#)
- [Where to Go Next, page 101](#)
- [Additional References, page 101](#)
- [Feature Information for Reducing Alternate-Path Calculation Times in IS-IS Networks, page 102](#)

Finding Feature Information

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

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

Prerequisites for IS-IS Support for Route Tags

Because the Intermediate System-to-Intermediate System (IS-IS) route tag will be used in a route map, you must understand how to configure a route map.

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 type, length, values (TLV) Type 135.

You must understand the task for which you are using the route tag, such as route redistribution, route summarization, or route leaking.

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

Before you tag any IS-IS routes, you need to make the following decisions:

- Your goal to set values for routes or redistribute routes (or both).
- Where in your network you want to tag routes.
- Where in your network you want to reference the tags.
- Which tagging method you will use. This method determines which task to perform.

Information About IS-IS Support for Route Tags

Route Redistribution

Devices 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 device or a Level 2 device. Level 2 routes injected as Level 1 routes is called route leaking.

IS-IS Caching of Redistributed Routes

Intermediate System-to-Intermediate System (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 link-state packet (LSP) protocol data unit (PDU) generation, significantly improving network scalability.

Prioritize 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 Intermediate System-to-Intermediate System (IS-IS) prefixes or routes that must be updated. You can tag important IS-IS IP prefixes and configure the device 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 devices in a Multiprotocol Label Switching (MPLS) VPN environment are considered high-priority prefixes.

IS-IS Priority-Driven IP Prefix RIB Installation

In a network where devices run the Intermediate System-to-Intermediate System (IS-IS) protocol, convergence is achieved when a consistent view of the topology is distributed to all devices in the network. When a network event causes a topology change, a number of steps must occur in order for convergence to occur. The device

that initially detects the topology change (for example, an interface state change) must inform other devices of the topology change by flooding updated routing information (in the form of link-state protocol data units [PDUs]) to other devices. All devices, including the device that detected the topology change, must utilize the updated topology information to recompute shortest paths (run a shortest path first [SPF]), providing the updated output of the SPF calculation to the device's routing information base (RIB), which eventually causes the updated routing information to be used to forward packets. Until all devices have performed these basic steps, some destinations might 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 are installed before updates to prefixes that do not have this designation. Priority-driven IP prefixes reduce the convergence time for the important IS-IS IP prefixes and results in faster updating for routes that are dependent on these prefixes. Faster updates 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 are tagged with a tag designated for fast convergence.
- 2 Medium-priority prefixes—any /32 prefixes that are not 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 are 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.

IS-IS Routes Tagged to Control Their Redistribution

You can control the redistribution of Intermediate System-to-Intermediate System (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 enhances the scalability of a routing protocol. Summarization reduces the number of routing updates that are flooded across areas or routing domains. For example, in multiarea Intermediate System-to-Intermediate System (IS-IS) networks, a good addressing scheme can optimize summarization by not allowing an overly large Level 2 database to be unnecessarily populated with updates that have come from Level 1 areas.

A device can summarize prefixes on redistribution whether the prefixes have come from internal prefixes, local redistribution, or Level 1 device 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 Intermediate System-to-Intermediate System (IS-IS) routes to control their redistribution. You can configure a route map to set a tag for an IS-IS IP prefix (route) or match on the tag (perhaps on a different device) to redistribute IS-IS routes. Although the **match tag** and **set tag** commands existed for other protocols before the IS-IS Support for Route Tags feature, they were not implemented for IS-IS, so they did nothing when specified in an IS-IS network.

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 Intermediate System-to-Intermediate System (IS-IS) route tag number can be up to 4 bytes long. The tag value is set into a sub-TLV 1 for type, length, values (TLV) Type 135.

Only one tag can be set to an IS-IS IP route (prefix). The tag is sent in link-state packet (LSP) protocol data units (PDUs) 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 device because the tag is new information for the PDUs.

IS-IS Route Leaking Based on a Route Tag

You can tag Intermediate System-to-Intermediate System (IS-IS) routes to configure route leaking (redistribution). Because only the appropriate routes are redistributed—or leaked—the results is network scalability and faster convergence for the device update. If you configure route leaking and you want to match on a tag, use a route map (not a distribute list).

There are two general steps to using IS-IS route tags: tagging routes and referencing the tag to set values for the routes 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. 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 metric, next hop, and so on) or redistribute routes. You might tag routes on one device, but reference the tag on other devices, depending on what you want to achieve. For example, you could tag the interface on Device A with a tag, match the tag on Device B to set values, and redistribute routes on Device C based on values using a route map.

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

If you mistakenly inject a large number of IP routes into an Intermediate System-to-Intermediate System (IS-IS), perhaps by redistributing Border Gateway Protocol (BGP) into IS-IS, the network can be severely flooded. You can limit 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 is reached

or configure the software to generate a system warning once the number of redistributed prefixes reaches the maximum value.

In some cases when a limit is not placed on the number of redistributed routes, the link-state packet (LSP) might become full and routes might be dropped. You 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 no space is left in any of the fragments, an LSPFULL error message is generated.

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

**Note**

You cannot both limit redistributed prefixes and also choose to be warned only.

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

To speed up Intermediate System-to-Intermediate System (IS-IS) convergence time, limit the number of IP prefixes carried in link-state packets (LSPs). Configuring interfaces as unnumbered will 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. Two alternative methods avoid the overpopulation of routing tables and thereby reduce IS-IS convergence time. To choose the method that works best for your network type, you should become familiar with the concepts described in the following sections:

Small-Scale Method to Reduce IS-IS Convergence Time

You can explicitly configure an Intermediate System-to-Intermediate System (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 devices in your network, with possibly ten times as many physical interfaces involved, adding this command to each device's configuration is not practical.

Large-Scale Method to Reduce IS-IS Convergence Time

A way to reduce Intermediate System-to-Intermediate System (IS-IS) convergence is to configure the IS-IS instance on a device to advertise only passive interfaces (by using the **advertise-passive-only** command). This command relies on the fact that a user enabling IS-IS on a loopback interface usually configures the loopback as passive (to prevent sending unnecessary hello PDUs 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 Intermediate System-to-Intermediate System (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 Configure IS-IS Support for Route Tags

Configuring IS-IS 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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis [<i>area-tag</i>] Example: Device(config)# router isis	Enables Intermediate System-to-Intermediate System (IS-IS) as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	ispf [<i>level-1</i> <i>level-2</i> <i>level-1-2</i>] [<i>seconds</i>] Example: Device(config-router)# ispf level-1-2 60	Enables IS-IS incremental SPF. <ul style="list-style-type: none"> • The <i>seconds</i> argument represents the number of seconds after configuring this command that incremental SPF is activated. The range is 1 to 600. The default value is 120 seconds. The <i>seconds</i> argument applies only when you have enabled IS-IS.

	Command or Action	Purpose
Step 5	end Example: Device(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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface Ethernet 0	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	ip router isis [<i>area-tag</i>] Example: <pre>Router(config-if)# ip router isis tag13</pre>	Enables IS-IS as an IP routing protocol, and assigns a tag to a process, if required. Note If the <i>area-tag</i> 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 <i>tag-value</i> Example: <pre>Router(config-if)# isis tag 17</pre>	Sets a tag on the IP address configured for an interface when this IP prefix is put into an IS-IS LSP. <ul style="list-style-type: none"> The <i>tag-value</i> argument requires an integer in a range from 1 to 4294967295 and serves as a tag on an IS-IS route.
Step 6	exit Example: <pre>Router(config-if)# exit</pre>	Returns to global configuration mode.
Step 7	router isis [<i>area-tag</i>] Example: <pre>Router(config)# router isis marketing</pre>	Enables the IS-IS routing protocol and specifies an IS-IS process. Enters router configuration mode. Note If the <i>area-tag</i> 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 <i>tag-value</i> Example: <pre>Router(config-router)# ip route priority high tag 17</pre>	Assigns a high priority to prefixes associated with the specified tag value. <ul style="list-style-type: none"> 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 <i>tag-value</i> argument.
Step 9	end Example: <pre>Router(config-router)# end</pre>	(Optional) Saves configuration commands to the running configuration file and returns to privileged EXEC mode.
Step 10	show isis rib [<i>ip-address</i> <i>ip-address-mask</i>] Example: <pre>Router# show isis rib 255.255.255.0</pre>	Displays paths for a specific route in the IP Version 4 IS-IS local RIB. <ul style="list-style-type: none"> 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

You can enter the **debug isis rib local** command to verify whether the IP prefixes that are advertised by Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) protocol data units (PDUs) are being updated correctly in the IS-IS local Routing Information Base (RIB).

Tagging Routes for Networks Directly Connected to an Interface

Before You Begin

- 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	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>interface <i>type number</i></p> <p>Example:</p> <pre>Router(config)# interface ethernet 0</pre>	Configures an interface.
Step 4	<p>ip address <i>ip-address mask</i></p> <p>Example:</p> <pre>Router(config-if)# ip address 10.1.1.1 255.255.255.0</pre>	<p>Sets a primary IP address for an interface.</p> <ul style="list-style-type: none"> In this example, the network 10.1.1.0 will be tagged.
Step 5	<p>ip address <i>ip-address mask secondary</i></p> <p>Example:</p> <pre>Router(config-if)# ip address 10.2.2.1 255.255.255.0 secondary</pre>	<p>(Optional) Sets a secondary IP address for an interface.</p> <ul style="list-style-type: none"> In this example, the network 10.2.2.0 will be tagged.
Step 6	<p>isis tag <i>tag-value</i></p> <p>Example:</p> <pre>Router(config-if)# isis tag 120</pre>	<p>Sets a tag on the IP addresses configured under this interface when those IP prefixes are put into an IS-IS LSP.</p> <ul style="list-style-type: none"> The tag must be an integer.
Step 7	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 8	<p>show isis database verbose</p> <p>Example:</p> <pre>Router# show isis database verbose</pre>	<p>(Optional) Displays details about the IS-IS link-state database, including the route tag.</p> <ul style="list-style-type: none"> Perform this step if you want to verify the tag.
Step 9	<p>show ip route [<i>ip-address</i> [<i>mask</i>] [longer-prefixes] <i>protocol</i> [<i>process-id</i>] list [<i>access-list-number</i> <i>access-list-name</i>]]</p>	<p>(Optional) Displays the current state of the routing table.</p> <ul style="list-style-type: none"> Perform this step if you want to verify the tag.

	Command or Action	Purpose
	Example: <pre>Router# show ip route 10.1.1.1 255.255.255.0</pre>	

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 or Redistribute Routes.”

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: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>route-map map-tag [permit deny] [sequence-number]</p> <p>Example:</p> <pre>Router(config)# route-map static-color permit 15</pre>	<p>Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another.</p> <ul style="list-style-type: none"> • This command causes the router to enter route-map configuration mode.
Step 4	<p>match tag tag-value [...tag-value]</p> <p>Example:</p> <pre>Router(config-route-map)# match tag 15</pre>	<p>(Optional) Matches routes tagged with the specified tag numbers.</p> <ul style="list-style-type: none"> • 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.
Step 5	Use an additional match command for each match criterion that you want.	<p>(Optional) See the appropriate match commands in the <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i></p> <ul style="list-style-type: none"> • Repeat this step for each match criterion you that want.
Step 6	<p>set tag tag-value</p> <p>Example:</p> <pre>Router(config-route-map)# set tag 10</pre>	Specifies the tag number to set.
Step 7	Set another value, depending on what else you want to do with the tagged routes.	<p>(Optional) See the following set commands in the <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i></p> <ul style="list-style-type: none"> • 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	<p>end</p> <p>Example:</p> <pre>Router(config-route-map)# end</pre>	(Optional) Exits configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
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. <ul style="list-style-type: none"> • Perform this step if you want to verify the tag.
Step 12	show ip route [<i>ip-address</i> [<i>mask</i>] [longer-prefixes] <i>protocol</i> [<i>process-id</i>] [list <i>access-list-number</i> <i>access-list-name</i>]] Example: Router# show ip route 10.1.1.1 255.255.255.0	(Optional) Displays the current state of the routing table. <ul style="list-style-type: none"> • Perform this step if you want to verify the tag.

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.”

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	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>router isis [area-tag]</p> <p>Example:</p> <pre>Router(config)# router isis</pre>	<p>Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required.</p> <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	<p>metric-style wide</p> <p>Example:</p> <pre>Router(config-router)# metric-style wide</pre>	Configures a router running IS-IS so that it generates and accepts type, length, and value object (TLV) 135 for IP addresses.
Step 5	<p>summary-address address mask {level-1 level-1-2 level-2} [tag tag-value] [metric metric-value]</p> <p>Example:</p> <pre>Router(config-router)# summary-address 192.168.0.0 255.255.0.0 tag 12345 metric 321</pre>	<p>Creates aggregate addresses for IS-IS.</p> <p>Note If a tagged route is summarized and the tag is not explicitly configured in the summary-address command, then the tag is lost.</p>
Step 6	<p>end</p> <p>Example:</p> <pre>Router(config-router)# end</pre>	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 7	<p>show isis database verbose</p> <p>Example:</p> <pre>Router# show isis database verbose</pre>	<p>(Optional) Displays details about the IS-IS link-state database, including the route tag.</p> <ul style="list-style-type: none"> • Perform this step if you want to verify the tag.
Step 8	<p>show ip route [ip-address [mask] [longer-prefixes] protocol [process-id] [list access-list-number access-list-name]]</p> <p>Example:</p> <pre>Router# show ip route 10.1.1.1 255.255.255.0</pre>	<p>(Optional) Displays the current state of the routing table.</p> <ul style="list-style-type: none"> • Perform this step if you want to verify the tag.

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 or Redistribute Routes” section.

Using the Tag to Set Values and or Redistribute Routes

Before You Begin

You must have already applied a tag on the interface, in a route map, or on a summary route. See the [IS-IS Routes Tagged to Control Their Redistribution](#), on page 73.

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>route-map <i>map-tag</i> [permit deny] [<i>sequence-number</i>]</p> <p>Example:</p> <pre>Router(config)# route-map static-color permit 15</pre>	<p>Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another.</p> <ul style="list-style-type: none"> • This command causes you to enter route-map configuration mode.
Step 4	<p>match tag <i>tag-value</i></p> <p>Example:</p> <pre>Router(config-route-map)# match tag 120</pre>	(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 <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i> .
Step 6	Set a value, depending on what you want to do with the tagged routes.	(Optional) See the following set commands in the <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i> . <ul style="list-style-type: none"> • 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	<p>exit</p> <p>Example:</p> <pre>Router(config-route-map)# exit</pre>	(Optional) Returns to global configuration mode.
Step 10	<p>router isis</p> <p>Example:</p> <pre>Router(config)# router isis</pre>	(Optional) Enables the IS-IS routing protocol and specifies an IS-IS process.
Step 11	<p>metric-style wide</p> <p>Example:</p> <pre>Router(config-router)# metric-style wide</pre>	Configures a router running IS-IS so that it generates and accepts type, length, and value object (TLV) 135 for IP addresses.
Step 12	<p>redistribute <i>protocol</i> [<i>process-id</i>] [level-1 level-1-2 level-2] [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [route-map <i>map-tag</i>]</p>	(Optional) Redistributes routes from one routing domain into another routing domain.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-router)# redistribute static ip metric 2 route-map static-color</pre>	

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	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>router isis [<i>area-tag</i>]</p> <p>Example:</p> <pre>Device(config)# router isis</pre>	<p>Enables Intermediate System-to-Intermediate System (IS-IS) as an IP routing protocol and assigns a tag to a process, if required.</p> <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	<p>redistribute <i>protocol</i> [<i>process-id</i>] {level-1 level-1-2 level-2} [<i>as-number</i>] [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [match</p>	<p>Redistributes routes from one routing domain into another routing domain.</p>

	Command or Action	Purpose
	<pre>{internal external 1 external 2} [tag tag-value] [route-map map-tag] Example: Device(config-router)# redistribute eigrp 10 level-1</pre>	
Step 5	<pre>redistribute maximum-prefix maximum [percentage] [warning-only withdraw] Example: Device(config-router)# redistribute maximum-prefix 1000 80</pre>	<p>Sets a maximum number of IP prefixes that are allowed to be redistributed into IS-IS.</p> <ul style="list-style-type: none"> • There is no default value for the <i>maximum</i> argument. • The <i>percentage</i> 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. <p>Note If the warning-only keyword had been configured in this command, no limit would be enforced; a warning message would be logged.</p>
Step 6	<pre>end Example: Device(config-router)# end</pre>	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	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>router isis [<i>area-tag</i>]</p> <p>Example:</p> <pre>Device(config)# router isis</pre>	<p>Enables Intermediate System-to-Intermediate System (IS-IS) as an IP routing protocol and assigns a tag to a process, if required.</p> <ul style="list-style-type: none"> • Enters router configuration mode.
Step 4	<p>redistribute <i>protocol</i> [<i>process-id</i>] {level-1 level-1-2 level-2} [<i>as-number</i>] [metric <i>metric-value</i>] [metric-type <i>type-value</i>] match {internal external 1 external 2} [tag <i>tag-value</i>] [route-map <i>map-tag</i>]</p> <p>Example:</p> <pre>Device(config-router)# redistribute eigrp 10 level-1</pre>	<p>Redistributes routes from one routing domain into another routing domain.</p>
Step 5	<p>redistribute maximum-prefix <i>maximum</i> [<i>percentage</i>] [warning-only withdraw]</p> <p>Example:</p> <pre>Device(config-router)# redistribute maximum-prefix 1000 80 warning-only</pre>	<p>Causes a warning message to be logged when the maximum number of IP prefixes are redistributed into IS-IS.</p> <ul style="list-style-type: none"> • 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 <i>maximum</i> argument. • The <i>percentage</i> 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	<p>lsp-full suppress {[external] [interlevel] none}</p> <p>Example:</p> <pre>Device(config-router)# lsp-full suppress external interlevel</pre>	<p>(Optional) Controls which routes are suppressed when the link-state packet (LSP) protocol data unit (PDU) becomes full.</p> <ul style="list-style-type: none"> • The default is external (redistributed routes are suppressed). • The interlevel keyword causes routes from another level to be suppressed.

	Command or Action	Purpose
		<ul style="list-style-type: none"> The external and interval keywords can be specified together or separately.
Step 7	end Example: Device(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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Router(config)# interface Ethernet 0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address netmask</i> Example: Router(config-if)# ip address 192.168.20.1 255.255.255.0	Sets a primary IP address for an interface. <ul style="list-style-type: none"> • 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 [<i>area- tag</i>] 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 [<i>area- tag</i>] Example: Router(config)# router isis	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. <ul style="list-style-type: none"> • Enters router configuration mode.
Step 11	net <i>network-entity-title</i> 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.

	Command or Action	Purpose
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. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface loopback <i>number</i> Example: Router(config)# interface loopback 0	Configures a loopback interface and enters interface configuration mode.
Step 4	ip address <i>ip-address netmask</i> Example: Router(config-if)# ip address 192.168.10.1 255.255.255.255	Sets a primary IP address for an interface. <ul style="list-style-type: none"> 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 <i>type number</i> Example: Router(config)# interface Ethernet 0	Configures an interface type and enters interface configuration mode.
Step 8	ip address <i>ip-address netmask</i> Example: Router(config-if)# ip address 192.168.20.1 255.255.255.0	Sets a primary IP address for an interface. <ul style="list-style-type: none"> 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.

	Command or Action	Purpose
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. <ul style="list-style-type: none"> • 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.
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*] **route**
7. **show isis** [*area-tag*] [*ipv6* | *] **spf-log**
8. **show isis** [*process-tag*] **topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	isis display delimiter [<i>return count</i> <i>character count</i>] Example: Device(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: Device(config)# exit	Returns to privileged EXEC mode.
Step 5	show isis database [<i>level-1</i>] [<i>level-2</i>] [<i>l1</i>] [<i>l2</i>] [<i>detail</i>] [<i>lspid</i>] Example: Device# show isis database detail	Displays the Intermediate System-to-Intermediate System (IS-IS) link-state database.

	Command or Action	Purpose
Step 6	show isis [area-tag] route Example: Device# show isis financetag route	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	show isis [area-tag] [ipv6 *] spf-log Example: Device# show isis spf-log	Displays how often and why the device has run a full shortest path first (SPF) calculation.
Step 8	show isis [process-tag] topology Example: Device# show isis financetag topology	Displays a list of all connected devices in all areas. <ul style="list-style-type: none"> • If a process tag is specified, output is limited to the specified routing process. When “null” is specified for the process tag, the output is displayed only for the device process that has no tag specified. If a process tag is not specified, the output is displayed for all processes.

Examples

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

- When the SPF's were executed
- Total elapsed time for the SPF computation
- Number of nodes that make up the topology in the SPF calculation
- Number of triggers that caused the SPF calculation
- Information regarding what triggered the SPF calculation

Device# **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 IS-IS Support for Route Tags

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
```

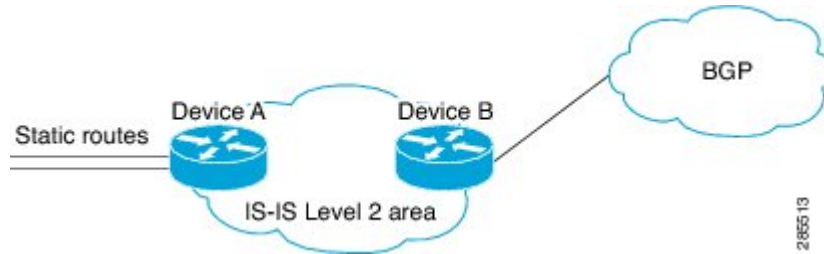
Example: Redistributing IS-IS Routes Using a Route Map

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

The figure below illustrates a flat Level 2 Intermediate System-to-Intermediate System (IS-IS) area. On the left edge are static routes from Device A to reach some IP prefixes. Device A redistributes the static routes

into IS-IS. Device B runs the Border Gateway Protocol (BGP) and redistributes IS-IS routes into BGP and then uses the tag to apply different administrative policy based on different tag values.

Figure 7: Example of Redistributing IS-IS Routes Using a Route Map



Device 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
```

Device B

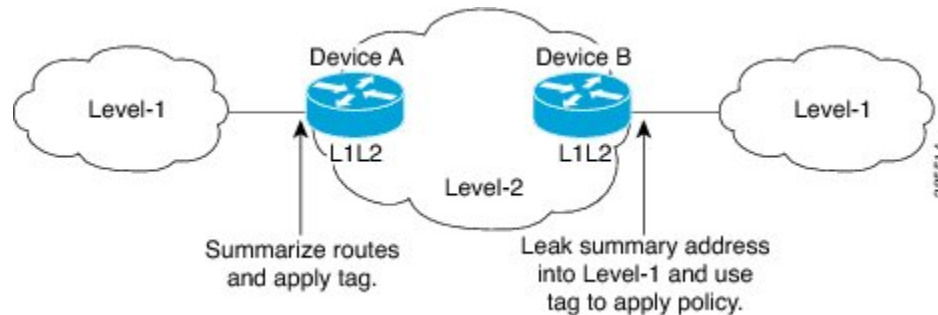
```
router bgp 100
 redistribute isis level-2 route-map tag-policy
 route-map tag-policy permit 20
  match tag 10
  set metric 1000
```

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. Device A and Device B are Level 1/Level 2 edge devices in the Level 2 area. On edge Device A, a summary address is configured to reduce the number of IP addresses put into the Level 2 Intermediate System-to-Intermediate System (IS-IS) database. Also, a tag value of 100 is set to the summary address.

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

Figure 8: Tag on a Summary Address



Device A

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

Device 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 the Number of Redistributed Routes

This example shows how to set a maximum of 1200 prefixes that can be redistributed into an Intermediate System-to-Intermediate System (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 link-state packet (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 are 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 Intermediate System-to-Intermediate System (IS-IS) network convergence times, complete the optional tasks in one or more of the following modules in the *IP Routing: IS-IS Configuration Guide*:

- “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

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	<i>Cisco IOS IP Routing: ISIS Command Reference</i>
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 [http://www.cisco.com/cisco/featurenavigator](#). An account on Cisco.com is not required.

Table 5: 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 Cisco IOS XE Release 3.2SE	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. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.
IS-IS Incremental SPF	12.0(24)S 12.2(18)S 12.3(2)T Cisco IOS XE 3.1.0 SG Cisco IOS XE Release 3.2SE	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. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.
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 Cisco IOS XE Release 3.2SE	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. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.

Feature Name	Releases	Feature Information
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 Cisco IOS XE Release 3.2SE	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. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.
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 Cisco IOS XE Release 3.2SE	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. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.
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 Cisco IOS XE Release 3.2SE	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. In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.



IS-IS Multiarea Support

Cisco software supports the configuration of multiple Intermediate System-to-Intermediate System (IS-IS) areas within a single device ISO Connectionless Network Service (CLNS). The IS-IS Multiarea Support feature lets you merge areas by configuring multiple Network Entity Titles (NETs) on a device.

This module describes the IS-IS Multiarea Support feature and explains how to configure it.

- [Finding Feature Information, page 105](#)
- [Restrictions for IS-IS Multiarea Support, page 105](#)
- [Information About IS-IS Multiarea Support, page 106](#)
- [How to Configure IS-IS Multiarea Support, page 109](#)
- [Configuration Examples for IS-IS Multiarea Support, page 112](#)
- [Additional References for IS-IS Multiarea Support, page 113](#)
- [Feature Information for IS-IS Multiarea Support, page 114](#)
- [Glossary, page 115](#)

Finding Feature Information

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

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

Restrictions for IS-IS Multiarea Support

- Routing is supported for only one Level 2 area per device.
- An interface cannot be part of more than one Level 1 or one Level 2 area per device.

- Only one process can be configured to perform Level 2 (interarea) routing. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1.
- Redistribution between IS-IS areas cannot be configured.

Information About IS-IS Multiarea Support

Overview of IS-IS Multiarea Support

Small Intermediate System-to-Intermediate System (IS-IS) networks are built as a single area that includes all the devices in the network. As the network increases in size, all Level 2 devices from all areas are connected through a backbone. This network backbone is, in turn, connected to local areas. Within a local area, devices reach all system IDs. Between areas, devices reach the backbone, and the backbone devices reach other areas.

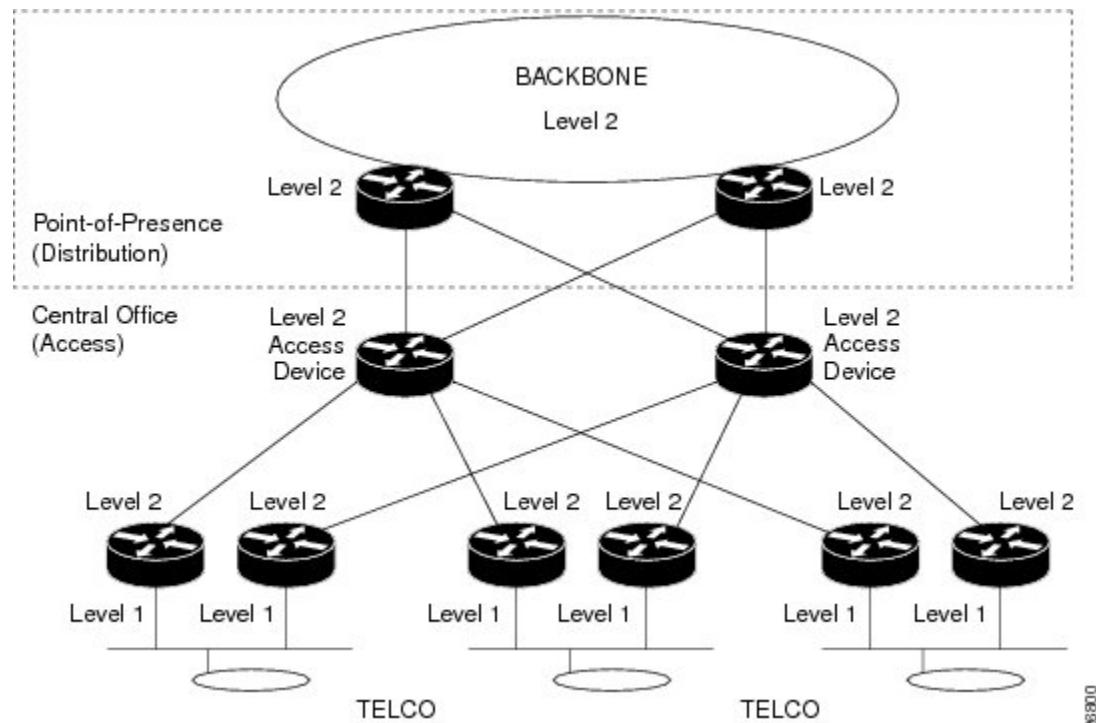
Devices establish Level 1 adjacencies to perform routing within a local area (intra-area routing). Devices establish Level 2 adjacencies to perform routing between Level 1 areas (interarea routing).

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 devices are used to interconnect each area to the Level 2 backbone.

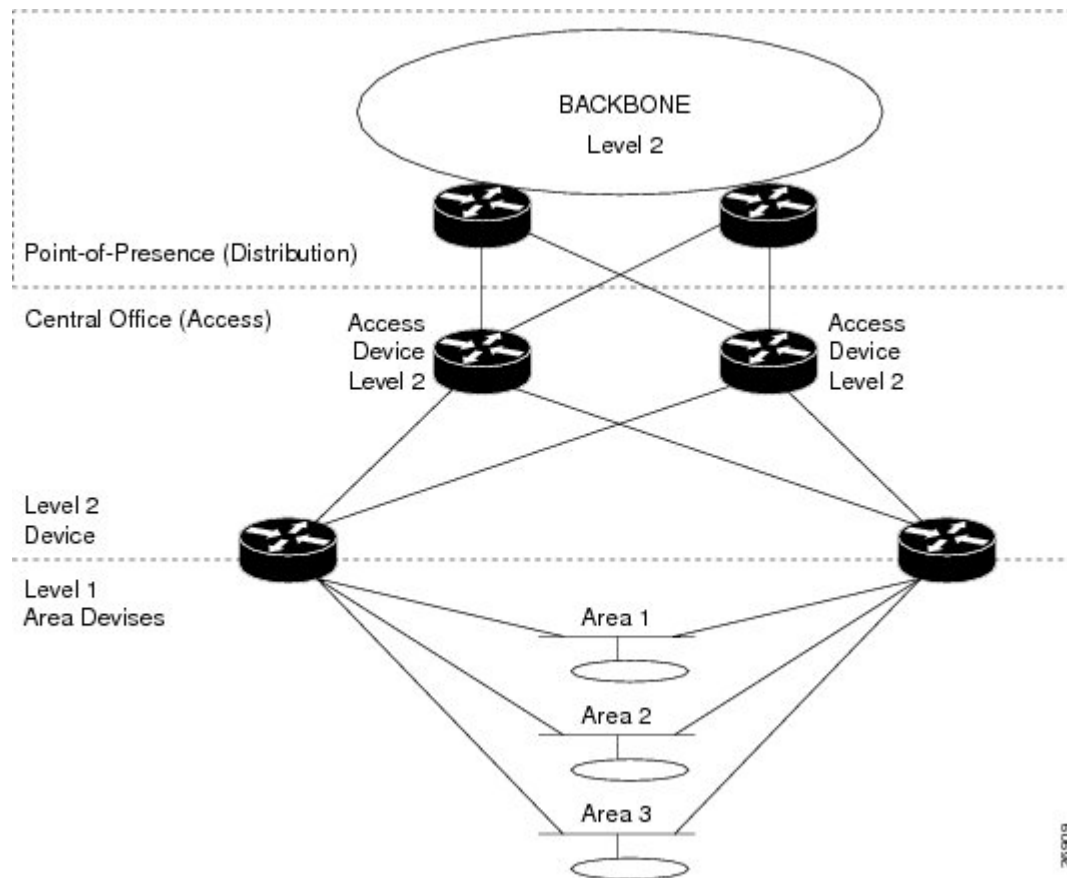
IP routes from the Level 1 device are advertised by default on the Level 2 device. Even when multiple Level 1 routing processes are configured on the same unit, they are advertised on the Level 2 device. No additional configuration is required to redistribute all Level 1 IP routes into the Level 2 process.

The figure below represents a Telco network used to monitor the status of the switching equipment in multiple remote central offices (where the telco equipment resides) from a central monitoring point. In this example, the CLNS network of the Telco is used to monitor the status of the switching equipment.

Figure 9: Telco IS-IS Network for Monitoring Remote Equipment Status



The figure below shows the same network reconfigured using multiarea IS-IS. The number of local access devices has been reduced. Each device continues to provide access to the backbone, but also participates in multiple Level 1 areas. In this example a 3:1 reduction in the number of devices required is shown.



Merging External Areas

Distinct areas defined in a multiarea device cannot share a common area address. This means that all devices in a single area must have unique system IDs. However, it is possible for two areas to be “merged” external to the router, such as when a common area number is introduced by other devices in the two areas. When this happens, the areas that now have a common area number are said to be “merged” into a single area.

The Intermediate System-to-Intermediate System (IS-IS) Multiarea Support feature lets you merge areas by configuring multiple network entity titles (NETs) on a device. If these NETs define a device to be in both area A and area B, for example, the device can potentially merge areas A and B. The result of the merge will be one Level 1 area with two area addresses: A and B.



Note

All devices in this merged area must have Network Service Access Point (NSAP) addresses with unique system IDs.

Benefits of IS-IS Multiarea Support

- The IS-IS Multiarea Support feature makes it possible for one Cisco device to support multiple Level 1 areas.
- A single Cisco device can now connect up to 29 areas, as well as perform Level 2 (interarea) routing in the backbone.
- This feature also provides connectivity between Level 1 areas that are local to the device. Previously, Level 1 areas could only to be connected using the Level 2 backbone.

How to Configure IS-IS Multiarea Support

Assigning IS-IS Areas

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	isis [<i>area-tag</i>] Example: <pre>Device(config-if) # isis test-area</pre>	Specifies the area tagged to the IS-IS interface of the Connectionless Network Service (CLNS).
Step 5	net <i>network-entity-title</i> Example: <pre>Device(config-if)# net 47.0004.004d.0001.0000.0c11.1111.00</pre>	Configures Network Entity Titles (NETs) for the routing process. <ul style="list-style-type: none"> Specify an NET for each routing process if you are configuring multiarea IS-IS.
Step 6	end Example: <pre>Device(config-if)# end</pre>	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling CLNS Routing for an Area on an Interface

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config) # interface gigabitethernet 0/0	Enters interface configuration mode.
Step 4	clns router isis [<i>area-tag</i>] Example: Device(config-if) # clns router isis areal	Specifies the area tagged to the IS-IS interface of the Connectionless Network Service (CLNS).
Step 5	ip address <i>ip-address-mask</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Defines the IP address for the interface. Note An IP address is required on all interfaces in an area enabled for IS-IS if any one interface is configured for IS-IS routing.
Step 6	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling Partitioning Avoidance

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis <i>area-tag</i> Example: Device(config)# router isis	Enables the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specifies an IS-IS process.
Step 4	partition avoidance Example: Device(config-router)# partition avoidance	Stops an IS-IS Level 1-2 border device from using a Level 1 area prefix on a Level 2 backbone. Withdraws area prefix if partition is detected
Step 5	end Example: Device(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for IS-IS Multiarea Support

Example Assigning IS-IS Areas

```

Device> enable

Device# configure terminal

Device(config)# interface gigabitethernet 0/0

Device(config-if)# router isis test-area

Device(config-if)# net 47.0004.004d.0001.0000.0c11.1111.00

Device(config-if)# end

```


Example Enabling CLNS Routing for an Area on an Interface

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/0
Device(config-if)# clns router isis test-area
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# end
```

Example Enabling Partitioning Avoidance

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# partition avoidance
Device(config)# end
```

Additional References for IS-IS Multiarea Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IS-IS commands	Cisco IOS IP Routing: IS-IS Command Reference
IS-IS conceptual information	“Integrated IS-IS Routing Protocol Overview” module in the IP Routing: IS-IS Configuration Guide

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 Multiarea Support

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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 6: Feature Information for IS-IS Multiarea Support

Feature Name	Releases	Feature Information
IS-IS Multiarea Support	Cisco IOS XE 3.2SE	<p>Cisco software supports the configuration of multiple Level 1 Intermediate System-to-Intermediate System (IS-IS) areas within a single device ISO Connectionless Network Service (CLNS). The IS-IS Multiarea Support feature lets you merge areas by configuring multiple Network Entity Titles (NETs) on a device.</p> <p>In Cisco IOS XE Release 3.2SE, support was added for the Cisco Catalyst 3850 Series Switches.</p> <p>No commands were introduced or modified.</p>

Glossary

Area —Group of connected routers and end systems in a routing domain (or autonomous system). All routers in the domain share topology and adjacency data. If Level 1 (intra-area) routing is enabled in the domain, all routers know how to reach all system IDs. If Level 2 routing is enabled in the domain, all routers know how to reach all other areas.

Conventional IS-IS —In this feature module, a router configured to perform intra-area (Level 1) IS-IS routing in a single area is considered to be conventionally configured. That router can also be configured to perform Level 2 (interarea) routing.

IS-IS —Intermediate System-to-Intermediate System Protocol as defined by ISO 10589 and RFC 1195.

Level 1 —Routers that establish Level 1 adjacencies in order to form a Level 1 area and perform intra-area routing.

Level 2 —Routers that establish Level 2 adjacencies in order to form a Level 2 area and perform interarea routing.

LSDB —link-state packet database. Database of all link-state packets from all routers in an area.

LSP —link-state packet. Packet containing information about the link state on a router instance.

OSI —Open Systems Interconnect (model). Protocol stack with ISO CLNS at Layer 3.

