IP Routing: ISIS Configuration Guide, Cisco IOS Release 15M&T

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 NONINFRINGEMENT 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: https://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. (1721R)

© 2018 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 8
- How to Create Monitor and Make Changes to a Basic IS-IS Network 9
  - Enabling IS-IS as an IP Routing Protocol on the Device 9
  - Enabling IS-IS as an IP Routing Protocol on the Interface 10
  - Monitoring IS-IS 11
    - Troubleshooting Tips 14
- Configuration Examples for a Basic IS-IS Network 14
  - Example: Configuring a Basic IS-IS Network 14

Where to Go Next 17
Additional References for IS-IS Overview and Basic Configuration 17
Feature Information for IS-IS Overview and Basic Configuration 18
Glossary 19

CHAPTER 2 **IPv6 Routing: IS-IS Support for IPv6 21**
Finding Feature Information 21
Information About IPv6 Routing: IS-IS Support for IPv6 21
IS-IS Enhancements for IPv6 21
IS-IS Single-Topology Support for IPv6 22
IPv6 IS-IS Local RIB 22
How to Configure IPv6 Routing: IS-IS Support for IPv6 22
Configuring Single-Topology IS-IS for IPv6 22
Customizing IPv6 IS-IS 24
Disabling IPv6 Protocol-Support Consistency Checks 26
Disabling IPv4 Subnet Consistency Checks 28
Verifying IPv6 IS-IS Configuration and Operation 28
Configuration Examples for IPv6 Routing: IS-IS Support for IPv6 30
Example: Customizing IPv6 IS-IS 30
Example: Disabling IPv6 Protocol-Support Consistency Checks 30
Example: Configuring IS-IS for IPv6 30
Additional References 32
Feature Information for IPv6 Routing: IS-IS Support for IPv6 33

CHAPTER 3 **IPv6 Routing: Route Redistribution 35**
Finding Feature Information 35
Information About IPv6 Routing: Route Redistribution 35
IS-IS Enhancements for IPv6 35
IPv6 IS-IS Route Redistribution 36
How to Configure IPv6 Routing: Route Redistribution 36
Redistributing Routes into an IPv6 IS-IS Routing Process 36
Redistributing IPv6 IS-IS Routes Between IS-IS Levels 37
Verifying IPv6 IS-IS Configuration and Operation 38
Configuration Examples for IPv6 Routing: Route Redistribution 39

Example: Redistributing Routes into an IPv6 IS-IS Routing Process 39
Example: Redistributing IPv6 IS-IS Routes Between IS-IS Levels 39
Example: Configuring IS-IS for IPv6 40
Additional References 42
Feature Information for IPv6 Routing: Route Redistribution 43

CHAPTER 4 **Customizing IS-IS for Your Network Design** 45
Finding Feature Information 45
Prerequisites for Customizing IS-IS for Your Network Design 45
Restrictions for Customizing IS-IS for Your Network Design 46
Information About Customizing IS-IS for Your Network Design 46
Enhancing Your IS-IS Network Design at the Interface Level 47
Setting the IS-IS Link-State Metrics 47
Prioritizing Designated Intermediate Systems for IS-IS 48
Enhancing Your IS-IS Network Design at the Router Level 49
Limiting Level 1 and Level 2 Operations on the IS-IS Router 49
Summarizing Address Ranges in the IS-IS Routing Table 50
Generating an IS-IS Default Route 51
Configuring an IS-IS Default Metric 52
Configuration Examples for Customizing IS-IS for Your Network Design 53
Example Configuring a Global Default Metric for IPv4 53
Where to Go Next 55
Additional References 56
Feature Information for Customizing IS-IS for Your Network Design 56

CHAPTER 5 **IS-IS MIB** 59
Finding Feature Information 59
Prerequisites for IS-IS MIB 59
Restrictions for IS-IS MIB 60
Information About IS-IS MIB 60
Cisco IS-IS MIB Table Object Definitions 60
Cisco IS-IS MIB Trap Notifications 68
IS-IS MIB for Generic System-Wide Errors 68
IS-IS MIB for LSP-Specific Errors 69

MIB Support for IS-IS Hello PDU-Specific Errors 70
MIB Support for IS-IS Transition State Changes 71
How to Enable IS-IS MIB 71
Configuring the Router to Send SNMP Notifications for IS-IS to a Host 71
What to Do Next 72
Enabling All IS-IS Traps 73
What to Do Next 74
Enabling IS-IS Error Traps 74
Enabling IS-IS State-Change Traps 75
Verifying IS-IS MIB Traps on the Router 76
Configuration Examples for IS-IS MIB 77
Example Enabling and Verifying IS-IS Error Traps 77
Example Enabling and Verifying IS-IS State Change Traps 77
Where to Go Next 77
Additional References 77
Feature Information for IS-IS MIB 78

CHAPTER 6 **IS-IS Support for an IS-IS Instance per VRF for IP 81**
Finding Feature Information 81
Prerequisites for IS-IS Support for an IS-IS Instance per VRF for IP 81
Restrictions for IS-IS Support for an IS-IS Instance per VRF for IP 82
Information About IS-IS Support for an IS-IS Instance per VRF for IP 82
VRF-Aware IS-IS 82
IS-IS Support for an IS-IS Instance per VRF for IP Feature Operation 82
How to Configure IS-IS Support for an IS-IS Instance per VRF for IP 83
Creating a VRF 83
Attaching an Interface to the VRF 84
Creating VRF Aware IS-IS Instances 85
Before You Begin 85
Creating a VRF-Aware IS-IS Instance in Interface Configuration Mode 85
Creating a VRF-Aware IS-IS Instance in Router Configuration Mode 86
Configuration Examples for IS-IS Support for an IS-IS Instance per VRF for IP 87
Example: Configuring Multiple VRF-Aware IS-IS Instances 87
Example: Creating an IS-IS Instance Without a Process Tag 89

Example: Redistributing Routes from an IS-IS Instance 90
Example: Changing the Interface Ownership 90
Additional References 91
Feature Information for IS-IS Support for an IS-IS Instance per VRF for IP 92

CHAPTER 7 **Configuring Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 93**
Finding Feature Information 93
Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 94
Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 94
IS-IS Process and Adjacencies 94
PDU Packet Types in IS-IS Routing 95
How to Create, Monitor and Make Changes to Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 95
Enabling IS-IS as an IP Routing Protocol on the Device 95
Enabling IS-IS as an IP Routing Protocol on the Interface 96
Monitoring IS-IS 97
Troubleshooting Tips 101
Shutting Down IS-IS to Make Changes to Your IS-IS Network 101
Shutting Down IS-IS in Interface Mode 101
Shutting Down IS-IS in Router Mode 102
Configuration Examples for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 103
Example: Configuring a Basic IS-IS Network 103
Example: Shutting Down IS-IS in Interface Mode 105
Example: Shutting Down IS-IS in Router Mode 106
““Where to Go Next 106
Additional References for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 107
Feature Information for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters 108

CHAPTER 8 **Overview of IS-IS Fast Convergence 109**
Finding Feature Information 109

Prerequisites for IS-IS Fast Convergence 109
Information About IS-IS Fast Convergence 109
Network Convergence 109
Design Recommendations for Achieving Faster Network Convergence 110
Where to Go Next 110
Additional References 111

CHAPTER 9 **Setting Best Practice Parameters for IS-IS Fast Convergence 113**
Finding Feature Information 113
Prerequisites for Setting Best Practice Parameters for IS-IS Fast Convergence 113
Information About Setting Best Practice Parameters for IS-IS Fast Convergence 114
General Steps for Improving Convergence Time in the IS-IS Network 114
How to Set Best Practice Parameters for IS-IS Fast Convergence 114
Setting Best Practice Parameters for IS-IS Fast Convergence 114
Configuration Examples for Setting Best Practice Parameters for IS-IS Fast Convergence 116
Example Enabling IS-IS on a Router and Setting Best Practice Parameters for IS-IS Fast Convergence 116
Where to Go Next 117
Additional References 117
Feature Information for Setting Best Practice Parameters for IS-IS Fast Convergence 118

CHAPTER 10 **Reducing Failure Detection Times in IS-IS Networks 119**
Finding Feature Information 119
Prerequisites for Reducing Failure Detection Times in IS-IS Networks 119
Information About Reducing Failure Detection Times in IS-IS Networks 120
Importance of Fast Network Failure Detection 120
How to Reduce Failure Detection Times in IS-IS Networks 120
Using IP Event Dampening to Decrease Failure Detection Times 120
Tuning IS-IS Hello Parameters to Decrease Link Failure Detection Times 122
Configuring an IS-IS Point-to-Point Adjacency over Broadcast Media 123
Monitoring IS-IS Network Convergence Time 124
Configuration Examples for Reducing Failure Detection Times in IS-IS Networks 126
Example Configuring IS-IS to Achieve Fast Convergence by Reducing Failure Detection Times 126

Where to Go Next 126
Additional References 126
Feature Information for Reducing Failure Detection Times in IS-IS Networks 127

CHAPTER 11 **IPv6 Routing: IS-IS Multitopology Support for IPv6 129**
Finding Feature Information 129
IPv6 Routing: IS-IS Multitopology Support for IPv6 129
IS-IS Enhancements for IPv6 129
IS-IS Multitopology Support for IPv6 130
Transition from Single-Topology to Multitopology Support for IPv6 130
How to Configure IPv6 Routing: IS-IS Multitopology Support for IPv6 130
Configuring Multitopology IS-IS for IPv6 130
Customizing IPv6 IS-IS 132
Verifying IPv6 IS-IS Configuration and Operation 134
Configuration Examples for IPv6 Routing: IS-IS Multitopology Support for IPv6 135
Example: Configuring the IS-IS IPv6 Metric for Multitopology IS-IS 135
Example: Configuring IS-IS for IPv6 135
Additional References 138
Feature Information for IPv6 Routing: IS-IS Multitopology Support for IPv6 139

CHAPTER 12 **Reducing Link Failure and Topology Change Notification Times in IS-IS Networks 141**
Finding Feature Information 141
Prerequisites for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks 141
Information About Reducing Link Failure and Topology Change Notification Times in IS-IS Networks 142
IS-IS LSP Generation Interval and Lifetime 142
IS-IS Throttling Timers That Affect Fast Convergence 142
How to Reduce Link Failure and Topology Change Notification Times in IS-IS Networks 144
Tuning SPF PRC and LSP Generation Exponential Backoff Timers 144
Enabling IS-IS Fast-Flooding of LSPs 146
Monitoring IS-IS Network Convergence Time 147
Configuration Examples for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks 148

Example Tuning IS-IS LSP Generation 148
Example Tuning IS-IS Fast Flooding of LSPs 148
Where to Go Next 149
Additional References 149
Feature Information for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks 150

CHAPTER 13 **IS-IS Support for Route Tags 151**
Finding Feature Information 151
Prerequisites for IS-IS Support for Route Tags 151
Information About IS-IS Support for Route Tags 152
Route Redistribution 152
IS-IS Routes Tagged to Control Their Redistribution 152
How Route Summarization Can Enhance Scalability in IS-IS Networks 152
Benefits of IS-IS Route Tags 152
IS-IS Route Tag Characteristics 152
IS-IS Route Leaking Based on a Route Tag 153
How to Configure IS-IS Support for Route Tags 153
Tagging Routes for Networks Directly Connected to an Interface 153
What to Do Next 155
Tagging Routes Using a Route Map 155
What to Do Next 157
Tagging a Summary Address 157
What to Do Next 158
Using the Tag to Set Values or Redistribute Routes 158
Monitoring IS-IS Network Convergence Time 160
Configuration Examples for IS-IS Support for Route Tags 162
Example: Tagging Routes for Networks Directly Connected to an Interface and Redistributing Them 162
Example: Redistributing IS-IS Routes Using a Route Map 162
Example: Tagging a Summary Address and Applying a Route Map 163
Example: Redistributing IS-IS Routes Using an Access List and a Route Map 164
Where to Go Next 165
Additional References 165

Feature Information for IS-IS Support for Route Tags 166

CHAPTER 14 **Enhancing Security in an IS-IS Network 167**

Finding Feature Information 167

Prerequisites for Enhancing Security in an IS-IS Network 167

Information About Enhancing Security in an IS-IS Network 168

Importance of Preventing Unauthorized Information from Entering an IS-IS Network 168

Configuring IS-IS Authentication 168

IS-IS Authentication Functionality 168

Benefits of IS-IS Clear Text Authentication 169

Benefits of IS-IS HMAC-MD5 Authentication 169

Migrating to a New Authentication Type 169

Migration from Old Clear Text Authentication to HMAC-MD5 Authentication 169

Migration from Old Clear Text Authentication to the New Clear Text Authentication 169

How to Enhance Security in an IS-IS Network 170

Setting an Authentication Password for each Interface 170

Setting a Password at Level 1 171

Setting a Password at Level 2 172

Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time 173

Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance 173

Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface 175

Migrating to a New Authentication Method 177

Configuring Authentication on a New Router Being Added to a Network That Already Has Authentication Configured 178

Configuration Examples for Enhancing Security in an IS-IS Network 180

Example Configuring IS-IS HMAC-MD5 Authentication 180

Example Configuring IS-IS Clear Text Authentication 180

Additional References 181

Feature Information for Enhancing Security in an IS-IS Network 182

CHAPTER 15 **IS-IS IPv6 Multi-Process Support 183**

Finding Feature Information 183

Prerequisites for IS-IS IPv6 Multi-Process Support 183

Information About IS-IS IPv6 Multi-Process Support 184

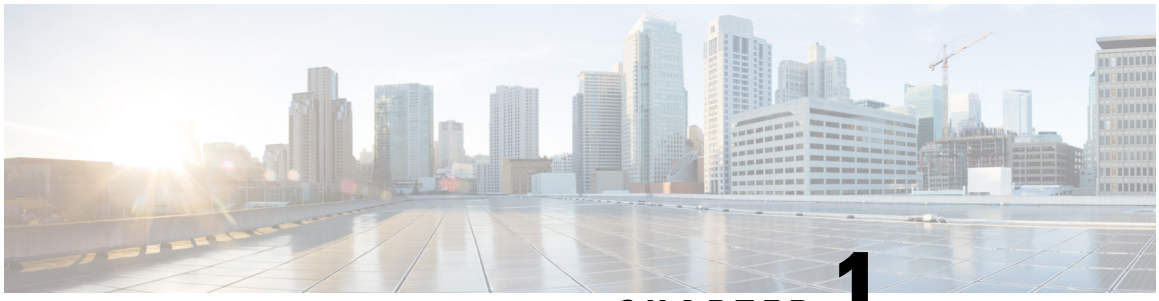
IS-IS IPv6 Multi-Process Support Overview 184
How to Configure IS-IS IPv6 Multi-Process Support 184
Configuring IS-IS IPv6 Multi-Process Support 184
Configuration Examples for IS-IS IPv6 Multi-Process Support 188
Example: IS-IS IPv6 Multi-Process Support Configuration 188
Additional References for IS-IS IPv6 Multi-Process Support 189
Feature Information for IS-IS IPv6 Multi-Process Support 189

CHAPTER 16 **IS-IS IPv6 Administrative Tag 191**
Finding Feature Information 191
Information About IS-IS IPv6 Administrative Tag 191
IS-IS Administrative Tags in IPv6 Prefixes 191
How to Configure an IS-IS IPv6 Administrative Tag 192
Assigning a Tag to an IS-IS IPv6 Prefix 192
Assigning a High Priority Administrative Tag to an IS-IS IPv6 Prefix 193
Using an IS-IS IPv6 Administrative Tag to Redistribute Routes 194
Using an IS-IS IPv6 Administrative Tag to Configure Routes 196
Applying an IS-IS IPv6 Tag to a Summary Prefix 198
Configuration Examples for IS-IS IPv6 Administrative Tag 200
Example: Assigning a Tag to an IS-IS IPv6 Prefix 200
Example: Assigning a High Priority Administrative Tag to an IS-IS IPv6 Prefix 201
Example: Using an IS-IS IPv6 Administrative Tag to Redistribute Routes 201
Example: Using an IS-IS IPv6 Administrative Tag to Configure Routes 201
Example: Applying an IS-IS IPv6 Administrative Tag to a Summary Prefix 202
Additional References 202
Feature Information for IS-IS IPv6 Administrative Tag 203

CHAPTER 17 **IS-IS IPv6 Advertise Passive Only 205**
Finding Feature Information 205
Prerequisites for IS-IS IPv6 Advertise Passive Only 205
Information About IS-IS IPv6 Advertise Passive Only 206
IPv6 Prefixes Only Allowed on Passive Interfaces 206
How to Configure IS-IS IPv6 Advertise Passive Only 206
Configuring IS-IS Instances on a Device to Advertise Passive Interface IPv6 Prefixes Only 206

Configuration Examples for IS-IS IPv6 Advertise Passive Only 208
Example: Configuring IS-IS Instances on a Device to Advertise Only Passive Interfaces 208
Additional References 209
Feature Information for IS-IS IPv6 Advertise Passive Only 210

CHAPTER 18 **IS-IS Inbound Filtering 211**
Finding Feature Information 211
Prerequisites for IS-IS Inbound Filtering 211
Information About IS-IS Inbound Filtering 211
How to Configure IS-IS Inbound Filtering 212
Configuring Route Filtering by Route Destination Using an Access List 212
Configuring Route Filtering by Next Hop (or Route Source) 213
Configuring Route Filtering by Route Destination Using a Prefix List 215
Configuring Route Filtering Using Tags 216
Configuring Route Filtering by IPv6 Route Destination Using a Prefix List 217
Configuration Examples for IS-IS Inbound Filtering 218
Example: Configuring Route Filtering by Route Destination Using an Access List 218
Example: Configuring Route Filtering by Next Hop (or Route Source) 219
Example: Configuring Route Filtering by Route Destination Using a Prefix List 219
Example: Configuring Route Filtering Using Tags 219
Example: Configuring Route Filtering by IPv6 Route Destination Using a Prefix List 219
Verifying IS-IS Inbound Filtering 220
Additional References 221
Feature Information for IS-IS Inbound Filtering 221



CHAPTER 1

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, on page 1
- Prerequisites for IS-IS Overview and Basic Configuration, on page 2
- Information About IS-IS Overview and Basic Configuration, on page 2
- How to Create Monitor and Make Changes to a Basic IS-IS Network, on page 9
- Configuration Examples for a Basic IS-IS Network, on page 14
- Where to Go Next, on page 17
- Additional References for IS-IS Overview and Basic Configuration, on page 17
- Feature Information for IS-IS Overview and Basic Configuration, on page 18
- Glossary, on page 19

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.

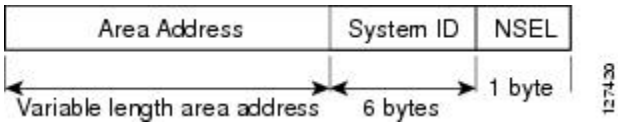
- System ID—This field is 6 octets long and immediately follows the area address. When the IS operates at Level 1, the system ID must be unique among all the Level-1 devices in the same area. When the IS operates at Level 2, the system ID must be unique among all devices in the domain.

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.

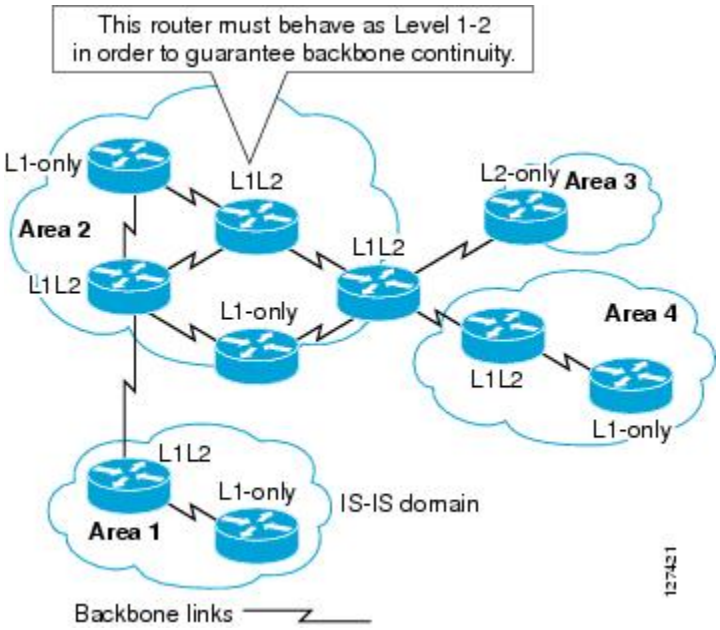
ISs form separate adjacencies for each level with neighbor ISs on the circuit.

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.

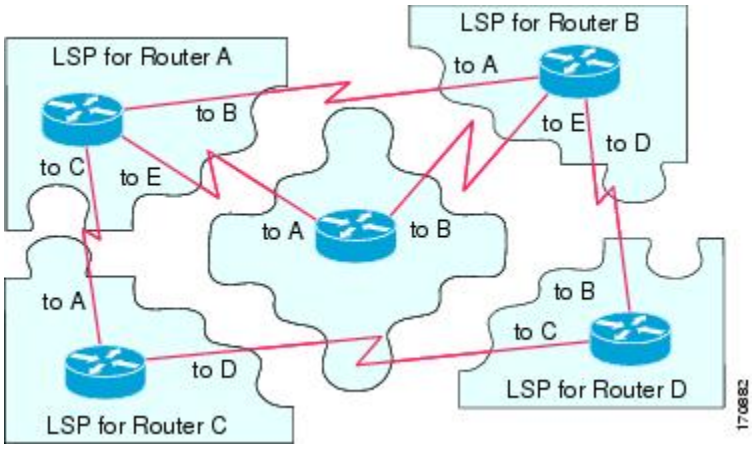
On a point-to-point circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

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.

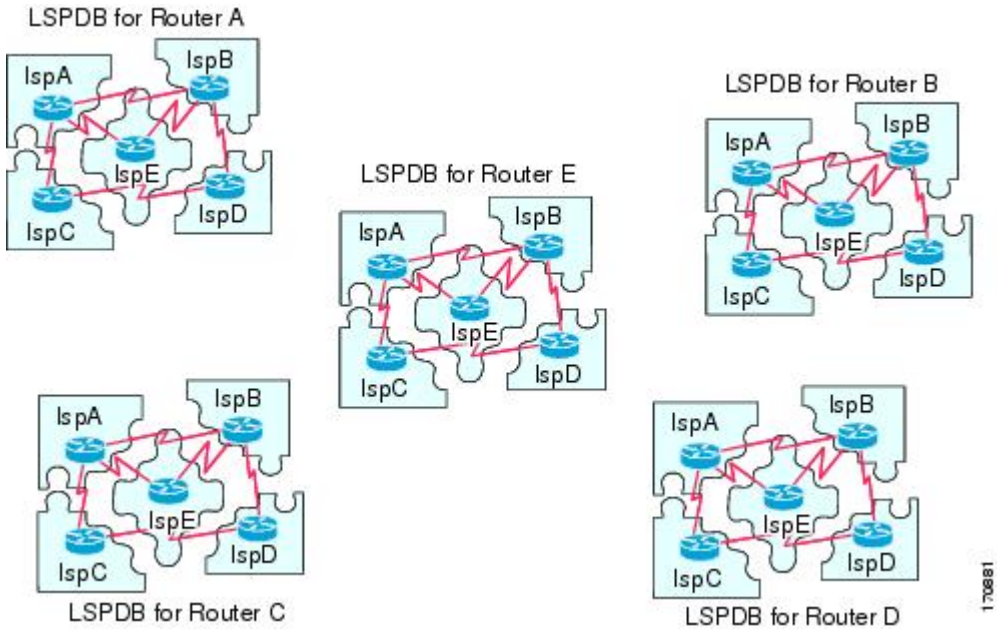
Figure 3: IS-IS Network Map



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

A Level-2 IS that indicates that it has one or more Level-2 neighbors in other areas may be used by Level-1 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. • 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`	Assigns a tag to an IS-IS process. Enters router configuration mode. • Configure tags to identify multiple IS-IS processes by giving a meaningful name for each routing process. If the tag is not specified, a null tag (0) is assumed and the process is referenced with a null tag. The tag name must be unique among all IP router processes for the device.
Step 4	**net** *network-entity-title* **Example:** `Device(config-router)# net 49.0001.0000.0000.000b.00`	Configures the NET on the device. • The NET identifies the device for IS-IS.
Step 5	**end** **Example:**	Exits router configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-router)# end`	

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [*secondary*] **Example:** `Device(config-if)# ip address 172.16.1.27 255.255.255.0`	Sets the primary IP address on the interface.
Step 5	**ip router isis** [*area-tag*] **Example:** `Device(config-if)# ip router isis company1`	Enables IS-IS on the interfaces that are to use IS-IS to distribute their IP information (and additionally that might be used to establish IS-IS adjacencies). • Use the *area-tag* argument to specify to which IS-IS process the 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.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring IS-IS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isis display delimiter** [**return** *count* | **character** *count*]
4. **exit**
5. **show ip protocols**
6. **show clns** *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**] [**l1**] [**l2**] [**detail**] [**lspid**]
12. **show isis database verbose**
13. **show isis lsp-log**
14. **show isis** [*area-tag*] [**ipv6** | *] **spf-log**
15. **show isis** [*process-tag*] [**ipv6** | *] **topology**
16. **show isis** [*area-tag*] **neighbors** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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	**isis display delimiter** [**return** *count*	**character** *count*] **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. • 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** [*type number*] [**detail**] **Example:** `Device# show clans is-neighbors detail`	Displays IS-IS information for IS-IS device adjacencies.
Step 7	**show clns interface** [*type number*] **Example:** `Device# show clns interface`	List the CLNS-specific information about each interface.
Step 8	**show clns** *area-tag* **neighbors** [*type number*] [**area**] [**detail**] **Example:** `Device# show clns area3 neighbors`	Displays both ES and IS neighbors. • The **show clns neighbor** command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your 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: • 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

	Command or Action	Purpose
		compared to an earlier execution of the command, can indicate instability or traffic problems. • To check for partial route calculations (PRCs), enter the **show clns traffic** command. PRCs are flooded when a change that does not affect topology is reported through an LSP; typical examples include the addition or removal of a prefix or metric changes for external or passive interfaces. A PRC update queue that remains full or increases to the maximum value for long periods of time indicates network instability. • LSP checksum errors indicate a problem. • The update queue should not stay full and should not drop much.
Step 10	**show ip route** [*ip-address* [*mask*]] [[**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]] **Example:** `Device# show ip route 172.16.0.21`	Displays the current state of the routing table.
Step 11	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Device# show isis database detail`	Displays additional information about the IS-IS database. • Displays the link-state database for Level-1 and Level-2, the contents for each LSP, and the link-state protocol PDU identifier.
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** [*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. • 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

	Command or Action	Purpose
		when a network change occurs, but then it should cease.
Step 15	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **Example:** `Device# show isis topology`	Displays a list of all connected devices in all areas.
Step 16	**show isis** [*area-tag*] **neighbors** [**detail**] **Example:** `Device# show isis neighbors detail`	Displays IS-IS adjacency information. • The **show isis neighbor detail** command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your 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
```

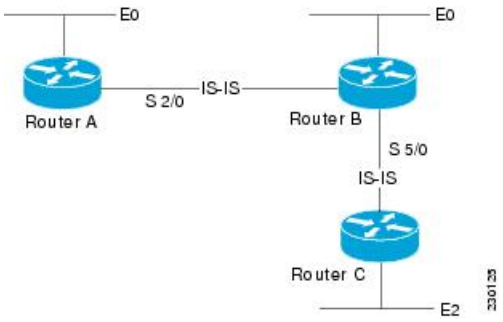
The **show isis spf-log** command displays logs of Level 1 and Level 2 LSPs including time of occurrence, duration, count, and the event that triggered the LSP.

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

MIBs

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

RFCs

RFC	Title
RFC 1195	*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* (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 www.cisco.com/go/cfn. 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		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. This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

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.

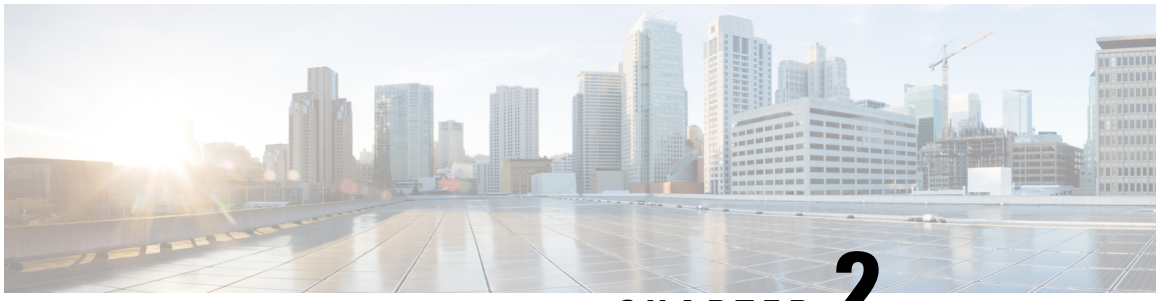
Level-2 router —An IS that supports Level-2 routing.

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

IPv6 Routing: IS-IS Support for IPv6

This module describes how to configure Integrated Intermediate System-to-Intermediate System (IS-IS) for IPv6. IS-IS is an Interior Gateway Protocol (IGP) that advertises link-state information throughout the network to create a picture of the network topology. IS-IS is an Open Systems Interconnection (OSI) hierarchical routing protocol that designates an intermediate system as a Level 1 or Level 2 device. Level 2 devices route between Level 1 areas to create an intradomain routing backbone. Integrated IS-IS uses a single routing algorithm to support several network address families, such as IPv6, IPv4, and OSI.

- Finding Feature Information, on page 21
- Information About IPv6 Routing: IS-IS Support for IPv6, on page 21
- How to Configure IPv6 Routing: IS-IS Support for IPv6, on page 22
- Configuration Examples for IPv6 Routing: IS-IS Support for IPv6, on page 30
- Additional References, on page 32
- Feature Information for IPv6 Routing: IS-IS Support for IPv6, on page 33

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.

Information About IPv6 Routing: IS-IS Support for IPv6

IS-IS Enhancements for IPv6

IS-IS in IPv6 functions the same and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. Extensions to the IS-IS command-line interface (CLI) allow configuration of IPv6-specific parameters. IPv6 IS-IS extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

IS-IS in IPv6 supports either single-topology mode or multiple topology mode.

IS-IS Single-Topology Support for IPv6

Single-topology support for IPv6 allows IS-IS for IPv6 to be configured on interfaces along with other network protocols (for example, IPv4 and Connectionless Network Service [CLNS]). All interfaces must be configured with the identical set of network address families. In addition, all routers in the IS-IS area (for Level 1 routing) or the domain (for Level 2 routing) must support the identical set of network layer address families on all interfaces.

When single-topology support for IPv6 is being used, either old- or new-style TLVs may be used. However, the TLVs used to advertise reachability to IPv6 prefixes use extended metrics. Cisco routers do not allow an interface metric to be set to a value greater than 63 if the configuration is not set to support only new-style TLVs for IPv4. In single-topology IPv6 mode, the configured metric is always the same for both IPv4 and IPv6.

IPv6 IS-IS Local RIB

A router that is running IS-IS IPv6 maintains a local RIB in which it stores all routes to destinations it has learned from its neighbors. At the end of each SPF, IS-IS attempts to install the best (that is, the least-cost) routes to a destination present in the local RIB in the global IPv6 routing table.

How to Configure IPv6 Routing: IS-IS Support for IPv6

Configuring Single-Topology IS-IS for IPv6

Perform this task to create an IPv6 IS-IS process and enable IPv6 IS-IS support on an interface.

Configuring IS-IS comprises two activities. The first activity creates an IS-IS routing process and is performed using protocol-independent IS-IS commands. The second activity in configuring IPv6 IS-IS configures the operation of the IS-IS protocol on an interface.

Before you begin

Before configuring the router to run IPv6 IS-IS, globally enable IPv6 using the **ipv6 unicast-routing** global configuration command.

Note If you are using IS-IS single-topology support for IPv6, IPv4, or both IPv6 and IPv4, you may configure both IPv6 and IPv4 on an IS-IS interface for Level 1, Level 2, or both Level 1 and Level 2. However, if both IPv6 and IPv4 are configured on the same interface, they must be running the same IS-IS level. That is, IPv4 cannot be configured to run on IS-IS Level 1 only on a specified Ethernet interface while IPv6 is configured to run IS-IS Level 2 only on the same Ethernet interface.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router isis** *area-tag*
4. **net** *network-entity-title*
5. **exit**
6. **interface** *type number*
7. **ipv6 address** {*ipv6-address* / *prefix-length* | *prefix-name sub-bits* / *prefix-length*
8. **ipv6 router isis** *area-name*

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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**net** *network-entity-title* **Example:** `Device(config-router)# net 49.0001.0000.0000.000c.00`	Configures an IS-IS network entity title (NET) for the routing process. • The *network-entity-title* argument defines the area addresses for the IS-IS area and the system ID of the router. **Note** For more details about the format of the *network-entity-title* argument, refer to the " Configuring ISO CLNS " chapter in the *Cisco IOS ISO CLNS Configuration Guide* .
Step 5	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:**	Specifies the interface type and number, and enters interface configuration mode.
Step 7	**ipv6 address** {*ipv6-address* / *prefix-length*	*prefix-name sub-bits* / *prefix-length* **Example:**	Specifies the IPv6 network assigned to the interface and enables IPv6 processing on the interface.

	Command or Action	Purpose
	`Device(config-if)# ipv6 address 2001:DB8::3/64`	**Note** Refer to Implementing IPv6 Addressing and Basic Connectivity for more information on configuring IPv6 addresses.
Step 8	**ipv6 router isis** *area-name* **Example:** `Device(config-if)# ipv6 router isis area2`	Enables the specified IPv6 IS-IS routing process on an interface.

Customizing IPv6 IS-IS

Perform this task to configure a new administrative distance for IPv6 IS-IS, configure the maximum number of equal-cost paths that IPv6 IS-IS will support, configure summary prefixes for IPv6 IS-IS, and configure an IS-IS instance to advertise the default IPv6 route (::/0). It also explains how to configure the hold-down period between partial route calculations (PRCs) and how often Cisco IOS software performs the SPF calculation when using multitopology IS-IS.

You can customize IS-IS multitopology for IPv6 for your network, but you likely will not need to do so. The defaults for this feature are set to meet the requirements of most customers and features. If you change the defaults, refer to the IPv4 configuration guide and the IPv6 command reference to find the appropriate syntax.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **default-information originate** [**route-map** *map-name*]
6. **distance** *value*
7. **maximum-paths** *number-paths*
8. **summary-prefix** *ipv6-prefix prefix-length* [**level-1** | **level-1-2**| **level-2**]
9. **prc-interval** *seconds* [*initial-wait*] [*secondary-wait*]
10. **spf-interval** [**level-1** | **level-2**] *seconds initial-wait*] [*secondary-wait*]
11. **exit**
12. **interface** *type number*
13. **isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables 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	**router isis** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**address-family ipv6** [**unicast** | **multicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**default-information originate** [**route-map** *map-name*] **Example:** `Device(config-router-af)# default-information originate`	(Optional) Injects a default IPv6 route into an IS-IS routing domain. • The **route-map** keyword and *map-name* argument specify the conditions under which the IPv6 default route is advertised. • If the **route map** keyword is omitted, then the IPv6 default route will be unconditionally advertised at Level 2.
Step 6	**distance** *value* **Example:** `Device(config-router-af)# distance 90`	(Optional) Defines an administrative distance for IPv6 IS-IS routes in the IPv6 routing table. • The *value*argument is an integer from 10 to 254. (The values 0 to 9 are reserved for internal use).
Step 7	**maximum-paths** *number-paths* **Example:** `Device(config-router-af)# maximum-paths 3`	(Optional) Defines the maximum number of equal-cost routes that IPv6 IS-IS can support. • This command also supports IPv6 Border Gateway Protocol (BGP) and Routing Information Protocol (RIP). • The *number-paths* argument is an integer from 1 to 64. The default for BGP is one path; the default for IS-IS and RIP is 16 paths.
Step 8	**summary-prefix** *ipv6-prefix prefix-length* [**level-1** | **level-1-2**| **level-2**] **Example:**	(Optional) Allows a Level 1-2 router to summarize Level 1 prefixes at Level 2, instead of advertising the Level 1 prefixes directly when the router advertises the summary.

	Command or Action	Purpose
	`Device(config-router-af)# summary-prefix 2001:DB8::/24`	• The *ipv6-prefix* argument in the **summary-prefix** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. • The *prefix-length* argument is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Step 9	**prc-interval** *seconds* [*initial-wait*] [*secondary-wait*] **Example:** `Device(config-router-af)# prc-interval 20`	(Optional) Configures the hold-down period between PRCs for multitopology IS-IS for IPv6.
Step 10	**spf-interval** [**level-1** | **level-2**] *seconds initial-wait*] [*secondary-wait*] **Example:** `Device(config-router-af)# spf-interval 30`	(Optional) Configures how often Cisco IOS software performs the SPF calculation for multitopology IS-IS for IPv6.
Step 11	**exit** **Example:** `Device(config-router-af)# exit`	Exits address family configuration mode, and returns the router to router configuration mode. • Repeat this step to exit router configuration mode and return the router to global configuration mode.
Step 12	**interface** *type number* **Example:**	Specifies the interface type and number, and enters interface configuration mode.
Step 13	**isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**] **Example:** `Device(config-if)# isis ipv6 metric 20`	(Optional) Configures the value of an multitopology IS-IS for IPv6 metric.

Disabling IPv6 Protocol-Support Consistency Checks

Perform this task to disable protocol-support consistency checks in IPv6 single-topology mode.

For single-topology IS-IS IPv6, routers must be configured to run the same set of address families. IS-IS performs consistency checks on hello packets and will reject hello packets that do not have the same set of configured address families. For example, a router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 or IPv6 only. In order to allow adjacency to be formed in mismatched address-families network, the **adjacency-check** command in IPv6 address family configuration mode must be disabled.

Note Entering the **no adjacency-check** command can adversely affect your network configuration. Enter the **no adjacency-check** command only when you are running IPv4 IS-IS on all your routers and you want to add IPv6 IS-IS to your network but you need to maintain all your adjacencies during the transition. When the IPv6 IS-IS configuration is complete, remove the **no adjacency-check**command from the configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **no adjacency-check**

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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**address-family ipv6** [**unicast**	**multicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**no adjacency-check** **Example:** `Device(config-router-af)# no adjacency-check`	Disables the IPv6 protocol-support consistency checks performed on hello packets, allowing IPv6 to be introduced into an IPv4-only network without disrupting existing adjacencies. • The **adjacency-check**command is enabled by default.

Disabling IPv4 Subnet Consistency Checks

Perform this task to disable IPv4 subnet consistency checking when forming adjacencies. software historically makes checks on hello packets to ensure that the IPv4 address is present and has a consistent subnet with the neighbor from which the hello packets are received. To disable this check, use the **no adjacency-check** command in the router configuration mode. However, if multitopology IS-IS is configured, this check is automatically suppressed, because multitopology IS-IS requires routers to form an adjacency regardless of whether or not all routers on a LAN support a common protocol.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **no adjacency-check**

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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**no adjacency-check** **Example:** `Device(config-router-af)# no adjacency-check`	Disables the IPv6 protocol-support consistency checks performed on hello packets, allowing IPv6 to be introduced into an IPv4-only network without disrupting existing adjacencies. • The **adjacency-check**command is enabled by default.

Verifying IPv6 IS-IS Configuration and Operation

SUMMARY STEPS

1. **enable**
2. **show ipv6 protocols** [**summary**]
3. **show isis** [*process-tag*] [**ipv6** | *****] **topology**

4. **show clns** [*process-tag*] **neighbors** *interface-type interface-number*] [**area**] [**detail**]
5. **show clns** *area-tag* **is-neighbors** [*type number*] [**detail**]
6. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
7. **show isis ipv6 rib** [*ipv6-prefix*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 protocols** [**summary**] **Example:** `Device# show ipv6 protocols`	Displays the parameters and current state of the active IPv6 routing processes.
Step 3	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **Example:** `Device# show isis topology`	Displays a list of all connected routers running IS-IS in all areas.
Step 4	**show clns** [*process-tag*] **neighbors** *interface-type interface-number*] [**area**] [**detail**] **Example:** `Device# show clns neighbors detail`	Displays end system (ES), intermediate system (IS), and multitopology IS-IS (M-ISIS) neighbors.
Step 5	**show clns** *area-tag* **is-neighbors** [*type number*] [**detail**] **Example:** `Device# show clns is-neighbors detail`	Displays IS-IS adjacency information for IS-IS neighbors. • Use the **detail** keyword to display the IPv6 link-local addresses of the neighbors.
Step 6	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Device# show isis database detail`	Displays the IS-IS link-state database. • In this example, the contents of each LSP are displayed using the **detail** keyword.
Step 7	**show isis ipv6 rib** [*ipv6-prefix*] **Example:** `Device# show isis ipv6 rib`	Displays the IPv6 local RIB.

Configuration Examples for IPv6 Routing: IS-IS Support for IPv6

Example: Customizing IPv6 IS-IS

The following example advertises the IPv6 default route (::/0)--with an origin of Ethernet interface 0/0/1--with all other routes in router updates sent on Ethernet interface 0/0/1. This example also sets an administrative distance for IPv6 IS-IS to 90, defines the maximum number of equal-cost paths that IPv6 IS-IS will support as 3, and configures a summary prefix of 2001:DB8::/24 for IPv6 IS-IS.

```
router isis
 address-family ipv6
 default-information originate
 distance 90
 maximum-paths 3
 summary-prefix 2001:DB8::/24
 exit
```

Example: Disabling IPv6 Protocol-Support Consistency Checks

The following example disables the **adjacency-check** command to allow a network administrator to configure IPv6 IS-IS on the router without disrupting the existing adjacencies:

```
router isis
 address-family ipv6
 no adjacency-check
```

Example: Configuring IS-IS for IPv6

In the following example, output information about the parameters and current state of that active IPv6 routing processes is displayed using the **show ipv6 protocols**command:

```
Device# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0
    Ethernet1
    Serial1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Address Summarization:
    L2: 2001:DB8:33::/16  advertised with metric 0
    L2: 2001:DB8:44::/16  advertised with metric 20
    L2: 2001:DB8:66::/16  advertised with metric 10
    L2: 2001:DB8:77::/16  advertised with metric 10
```

In the following example, output information about all connected routers running IS-IS in all areas is displayed using the **show isis topology**command:

```
Device# show isis topology
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000C
0000.0000.000D  20      0000.0000.00AA  Se1/0/1         *HDLC*
0000.0000.000F  10      0000.0000.000F  GE0/0/1         0050.e2e5.d01d
0000.0000.00AA  10      0000.0000.00AA  Se1/0/1         *HDLC*
IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000A  10      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000B  20      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000C  --
0000.0000.000D  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000E  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
```

In the following example, output information to confirm that the local router has formed all the necessary IS-IS adjacencies with other IS-IS neighbors is displayed using the **show clns is-neighbors**command. To display the IPv6 link-local addresses of the neighbors, specify the **detail** keyword.

```
Device# show clns is-neighbors detail
System Id      Interface   State  Type Priority  Circuit Id         Format
0000.0000.00AA Se1    Up     L1   0         00                 Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::YYYY:D37C:C854:5
  Uptime: 17:21:38
0000.0000.000F Et0     Up     L1   64        0000.0000.000C.02  Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::XXXX:E2FF:FEE5:D01D
  Uptime: 17:21:41
0000.0000.000A Et0     Up     L2   64        0000.0000.000C.01  Phase V
  Area Address(es): 49.000b
  IPv6 Address(es): FE80::ZZZZ:F6FF:FE8D:F063
  Uptime: 17:22:06
```

In the following example, detailed output information about LSPs received from other routers and the IPv6 prefixes they are advertising is displayed using the **show isis database**command with the **detail** keyword specified:

```
Device# show isis database detail
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
 --More--
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:DB8::/64
```

```
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.000A.00-00  0x00000059   0x378A        949               0/0/0
  Area Address: 49.000b
  NLPID:        0x8E
  IPv6 Address: 2001:DB8:1:1:1:1:1:1
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IPv6 2001:DB8:3:YYYY::/64
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IS-Extended 0000.0000.000A.01
  Metric: 10         IS-Extended 0000.0000.000B.00
  Metric: 10         IS-Extended 0000.0000.000C.01
  Metric: 0          IPv6 11:1:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:2:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:3:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:4:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:5:YYYY:1:1:1:1:1/128
0000.0000.000A.01-00  0x00000050   0xB0AF        491               0/0/0
  Metric: 0          IS-Extended 0000.0000.000A.00
  Metric: 0          IS-Extended 0000.0000.000B.00
```

The following example shows output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Device# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  2001:DB8:88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
* 2001:DB8:1357:1::/64
    via FE80::202:7DFF:FE1A:9471/GigabitEthernet2/1/0, type L2  metric 10 LSP [4/9]
* 2001:DB8:45A::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IPv6 commands	*Cisco IOS IPv6 Command Reference*

Related Topic	Document Title
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*
IPv6 Routing: IS-IS Support for IPv6	"*Integrated IS-IS Routing Protocol Overview* " module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

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

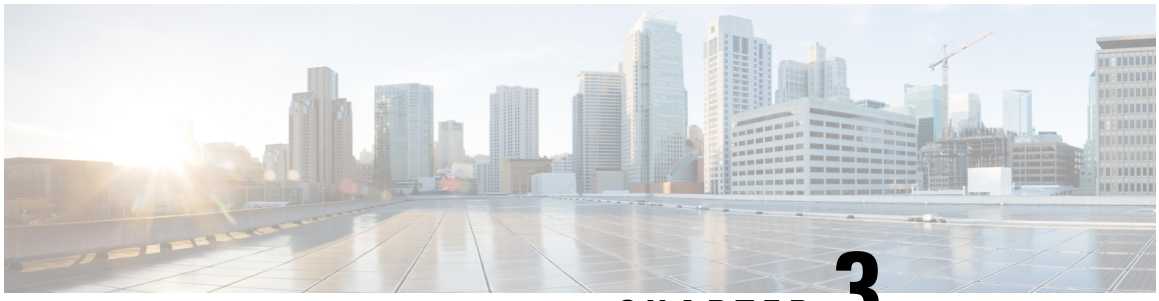
Feature Information for IPv6 Routing: IS-IS Support for IPv6

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

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

Table 2: Feature Information for IPv6 Routing: IS-IS Support for IPv6

Feature Name	Releases	Feature Information
IPv6 Routing: IS-IS Support for IPv6		IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. The following commands were introduced or modified: **address-family ipv6 (IS-IS)**, **adjacency-check**, **default-information originate (IPv6 IS-IS)**, **distance (IPv6)**, **ipv6 router isis** , **isis ipv6 metric**, **maximum-paths (IPv6)**, **prc-interval (IPv6)**, **router isis** , **show clns neighbors**, **show ipv6 protocols**, **show isis database**, **show isis topology**, **spf-interval**, **summary-prefix (IPv6 IS-IS)**.
IPv6 ISIS Local RIB		A router that is running IS-IS IPv6 maintains a local RIB in which it stores all routes to destinations it has learned from its neighbors. The following command was introduced: **show isis ipv6 rib**.



CHAPTER 3

IPv6 Routing: Route Redistribution

IPv6 route redistribution supports redistributing routes into an IPv6 IS-IS routing process and redistributing IPv6 IS-IS routes between IS-IS levels.

- Finding Feature Information, on page 35
- Information About IPv6 Routing: Route Redistribution, on page 35
- How to Configure IPv6 Routing: Route Redistribution, on page 36
- Configuration Examples for IPv6 Routing: Route Redistribution, on page 39
- Additional References, on page 42
- Feature Information for IPv6 Routing: Route Redistribution, on page 43

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.

Information About IPv6 Routing: Route Redistribution

IS-IS Enhancements for IPv6

IS-IS in IPv6 functions the same and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. Extensions to the IS-IS command-line interface (CLI) allow configuration of IPv6-specific parameters. IPv6 IS-IS extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

IS-IS in IPv6 supports either single-topology mode or multiple topology mode.

IPv6 IS-IS Route Redistribution

IS-IS for IPv6 supports redistributing routes into an IPv6 IS-IS routing process and redistributing IPv6 IS-IS routes between IS-IS levels.

How to Configure IPv6 Routing: Route Redistribution

Redistributing Routes into an IPv6 IS-IS Routing Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast**]
5. **redistribute** *source-protocol* [*process-id*] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*]
6. **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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**address-family ipv6** [**unicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • **unicast**—(Optional) Specifies the unicast IPv6 unicast address family. This is the default option.
Step 5	**redistribute** *source-protocol* [*process-id*] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*] **Example:**	Redistributes routes from the specified protocol into the IS-IS process. • *source-protocol*—Can be one of the following: **bgp**, **connected**, **isis**, **rip** or **static**. • *process-id*—(Optional) Routing process name.

	Command or Action	Purpose
	`Device(config-router-af)# redistribute bgp 64500 metric 100 route-map isismap`	• **metric** *metric-value*—Redistributes routes based on the metric value. • **metric-type** *type-value*—Specifies the link type, which can be the following: **external** to set an external ISIS metric type, **internal** to set an internal ISIS metric type, **rib-metric-as-external** to set metric type to external and use the RIB metric, and **rib-metric-as-internal** to set metric type to internal and use the RIB metric.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Redistributing IPv6 IS-IS Routes Between IS-IS Levels

Perform this task to redistribute IPv6 routes learned at one IS-IS level into a different level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast**]
5. **redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*
6. **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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.

	Command or Action	Purpose
Step 4	**address-family ipv6** [**unicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • **unicast**—(Optional) Specifies the unicast IPv6 unicast address family. This is the default option.
Step 5	**redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name* **Example:** `Device(config-router-af)# redistribute isis level-1 into level-2`	Redistributes IPv6 routes from one IS-IS level into another IS-IS level. • By default, the routes learned by Level 1 instances are redistributed by the Level 2 instance. **Note** The *protocol* argument must be **isis** in this configuration of the **redistribute** command. Only the arguments and keywords relevant to this task are specified here.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Verifying IPv6 IS-IS Configuration and Operation

SUMMARY STEPS

1. **enable**
2. **show ipv6 protocols** [**summary**]
3. **show isis** [*process-tag*] [**ipv6** | *****] **topology**
4. **show clns** [*process-tag*] **neighbors** *interface-type interface-number*] [**area**] [**detail**]
5. **show clns** *area-tag* **is-neighbors** [*type number*] [**detail**]
6. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
7. **show isis ipv6 rib** [*ipv6-prefix*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 protocols** [**summary**] **Example:** `Device# show ipv6 protocols`	Displays the parameters and current state of the active IPv6 routing processes.

	Command or Action	Purpose
Step 3	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **Example:** `Device# show isis topology`	Displays a list of all connected routers running IS-IS in all areas.
Step 4	**show clns** [*process-tag*] **neighbors** *interface-type interface-number*] [**area**] [**detail**] **Example:** `Device# show clns neighbors detail`	Displays end system (ES), intermediate system (IS), and multitopology IS-IS (M-ISIS) neighbors.
Step 5	**show clns** *area-tag* **is-neighbors** [*type number*] [**detail**] **Example:** `Device# show clns is-neighbors detail`	Displays IS-IS adjacency information for IS-IS neighbors. • Use the **detail** keyword to display the IPv6 link-local addresses of the neighbors.
Step 6	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Device# show isis database detail`	Displays the IS-IS link-state database. • In this example, the contents of each LSP are displayed using the **detail** keyword.
Step 7	**show isis ipv6 rib** [*ipv6-prefix*] **Example:** `Device# show isis ipv6 rib`	Displays the IPv6 local RIB.

Configuration Examples for IPv6 Routing: Route Redistribution

Example: Redistributing Routes into an IPv6 IS-IS Routing Process

The following example redistributes IPv6 BGP routes into the IPv6 IS-IS Level 2 routing process:

```
router isis
 address-family ipv6
 redistribute bgp 64500 metric 100 route-map isismap
 exit
```

Example: Redistributing IPv6 IS-IS Routes Between IS-IS Levels

The following example redistributes IPv6 IS-IS Level 1 routes into the IPv6 IS-IS Level 2 routing process:

```
router isis
 address-family ipv6
 redistribute isis level-1 into level-2
```

Example: Configuring IS-IS for IPv6

In the following example, output information about the parameters and current state of that active IPv6 routing processes is displayed using the **show ipv6 protocols**command:

```
Device# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    GigabitEthernet0/0/3
    GigabitEthernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Address Summarization:
    L2: 2001:DB8:33::/16  advertised with metric 0
    L2: 2001:DB8:44::/16  advertised with metric 20
    L2: 2001:DB8:66::/16  advertised with metric 10
    L2: 2001:DB8:77::/16  advertised with metric 10
```

In the following example, output information about all connected routers running IS-IS in all areas is displayed using the **show isis topology**command:

```
Device# show isis topology
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000C
0000.0000.000D  20      0000.0000.00AA  Se1/0/1         *HDLC*
0000.0000.000F  10      0000.0000.000F  GE0/0/1         0050.e2e5.d01d
0000.0000.00AA  10      0000.0000.00AA  Se1/0/1         *HDLC*
IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000A  10      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000B  20      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000C  --
0000.0000.000D  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000E  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
```

In the following example, output information to confirm that the local router has formed all the necessary IS-IS adjacencies with other IS-IS neighbors is displayed using the **show clns is-neighbors**command. To display the IPv6 link-local addresses of the neighbors, specify the **detail** keyword.

```
Device# show clns is-neighbors detail
System Id      Interface   State  Type Priority  Circuit Id         Format
0000.0000.00AA Se1/0/1     Up     L1   0         00                 Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::YYYY:D37C:C854:5
  Uptime: 17:21:38
0000.0000.000F Et0/0/1     Up     L1   64        0000.0000.000C.02  Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::XXXX:E2FF:FEE5:D01D
  Uptime: 17:21:41
0000.0000.000A Et0/0/3     Up     L2   64        0000.0000.000C.01  Phase V
```

```
  Area Address(es): 49.000b
  IPv6 Address(es): FE80::ZZZZ:F6FF:FE8D:F063
  Uptime: 17:22:06
```

In the following example, detailed output information that displays both end system (ES) and intermediate system (IS) neighbors is displayed using the **show clns neighbors** command with the **detail** keyword.

```
Device# show clns neighbors detail
System Id          Interface    SNPA            State  Holdtime  Type Protocol
0000.0000.0007     GE3/3        aa00.0400.6408  UP     26        L1   IS-IS
Area Address(es): 20
IP Address(es): 172.16.0.42*
Uptime: 00:21:49
0000.0C00.0C35     GE3/2        0000.0c00.0c36  Up     91        L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.42*
Uptime: 00:21:52
0800.2B16.24EA     GE3/3        aa00.0400.2d05  Up     27        L1   M-ISIS
Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
0800.2B14.060E     GE3/2        aa00.0400.9205  Up     8         L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52
```

In the following example, detailed output information about LSPs received from other routers and the IPv6 prefixes they are advertising is displayed using the **show isis database**command with the **detail** keyword specified:

```
Device# show isis database detail
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
 --More--
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:DB8::/64
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.000A.00-00  0x00000059   0x378A        949               0/0/0
  Area Address: 49.000b
  NLPID:        0x8E
  IPv6 Address: 2001:DB8:1:1:1:1:1:1
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IPv6 2001:DB8:3:YYYY::/64
```

```
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IS-Extended 0000.0000.000A.01
  Metric: 10         IS-Extended 0000.0000.000B.00
  Metric: 10         IS-Extended 0000.0000.000C.01
  Metric: 0          IPv6 11:1:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:2:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:3:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:4:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:5:YYYY:1:1:1:1:1/128
0000.0000.000A.01-00  0x00000050   0xB0AF        491               0/0/0
  Metric: 0          IS-Extended 0000.0000.000A.00
  Metric: 0          IS-Extended 0000.0000.000B.00
```

The following example shows output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Device# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  2001:DB8:88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
* 2001:DB8:1357:1::/64
    via FE80::202:7DFF:FE1A:9471/GigabitEthernet2/1/0, type L2  metric 10 LSP [4/9]
* 2001:DB8:45A::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

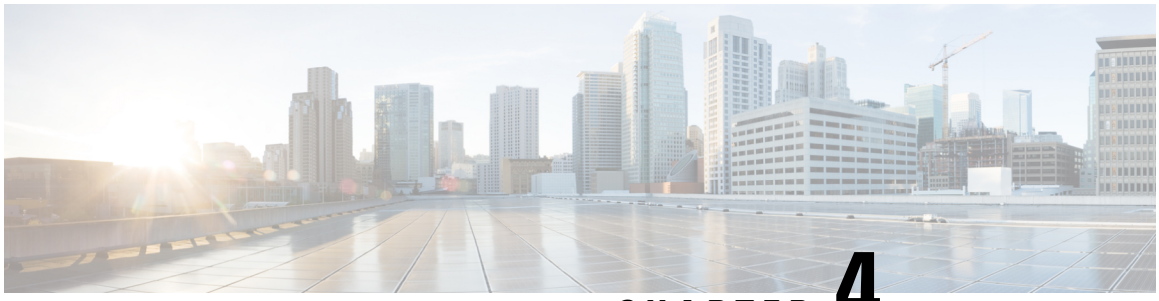
Feature Information for IPv6 Routing: Route Redistribution

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

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

Table 3: Feature Information for IPv6 Routing: Route Redistribution

Feature Name	Releases	Feature Information
IPv6 Routing: Route Redistribution		IS-IS for IPv6 supports redistributing routes into an IPv6 IS-IS routing process and redistributing IPv6 IS-IS routes between IS-IS levels. The following commands were introduced or modified: **address-family ipv6**, **redistribute isis (IPv6)**.



CHAPTER 4

Customizing IS-IS for Your Network Design

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

- Finding Feature Information, on page 45
- Prerequisites for Customizing IS-IS for Your Network Design, on page 45
- Restrictions for Customizing IS-IS for Your Network Design, on page 46
- Information About Customizing IS-IS for Your Network Design, on page 46
- Configuration Examples for Customizing IS-IS for Your Network Design, on page 53
- Where to Go Next, on page 55
- Additional References, on page 56
- Feature Information for Customizing IS-IS for Your Network Design, on page 56

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 Customizing IS-IS for Your Network Design

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

- IS-IS must be enabled.

Restrictions for Customizing IS-IS for Your Network Design

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

Information About Customizing IS-IS for Your Network Design

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

If you want to configure a global default metric, see the Configuring an IS-IS Default Metric, on page 52.

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

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

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

Enhancing Your IS-IS Network Design at the Interface Level

Setting the IS-IS Link-State Metrics

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type name* **Example:** `Router(config)# interface ethernet 0`	Enters interface configuration mode.
Step 4	**isis metric** *default-metric* [**level-1**	**level-2**] **Example:** `Router(config-if)# isis metric 15 level-1`	Configures the metric for an interface. **Note** We highly recommend that you configure the metrics on all interfaces. If you do not do so, all links will have the same cost and the cost to reach any node in the network will be logically equivalent to the number of hops.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:**	(Optional) Displays the IS-IS link-state database. • To display information about each LSP and the link-state database, enter the **detail** keyword.

	Command or Action	Purpose
	`Router# show isis database detail`	

Prioritizing Designated Intermediate Systems for IS-IS

SUMMARY STEPS

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

DETAILED STEPS

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

Enhancing Your IS-IS Network Design at the Router Level

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	`Router# show isis topology level-1`	• To confirm paths to all Level 1 or Level 2 routers in the area or areas in which this router resides, enter the **level-1** or **level-2** keywords, respectively.

Example

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

```
Router# show isis topology
Tag L2BB:
IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0005  --
0000.0000.0009  10      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0017  20      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0053  30      0000.0000.0009  Tu529           *Tunnel*
0000.0000.0068  20      0000.0000.0009  Tu529           *Tunnel*
Tag A3253-01:
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.0003  10      0000.0000.0003  Et1             0000.0c03.6944
0000.0000.0005  --
0000.0000.0053  10      0000.0000.0053  Et1             0060.3e58.ccdb
```

Summarizing Address Ranges in the IS-IS Routing Table

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**router isis** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol. • Enters router configuration mode.
Step 4	**summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**}[**tag** *tag-number*] [**metric** *metric-value*] **Example:** `Router(config-router)# summary-address 10.1.0.0 255.255.0.0 level-2`	Creates aggregate addresses for IS-IS. **Note** Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes. This command helps reduce the size of the routing table.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show isis database verbose** **Example:** `Router# show isis database verbose`	(Optional) Displays detailed information about the IS-IS database.

Generating an IS-IS Default Route

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring an IS-IS Default Metric

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Examples for Customizing IS-IS for Your Network Design

Example Configuring a Global Default Metric for IPv4

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

```
interface Ethernet3/1
 ip address 172.16.10.2 255.255.0.0
 ip router isis area1
 no ip route-cache
 duplex half
!
interface Ethernet3/2
 ip address 192.168.242.2 255.255.255.0
 ip router isis area1
```

```
 no ip route-cache
 duplex half
router isis area1
 net 01.0000.0309.1234.00
 metric-style wide
 metric 111
```

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

```
Router# show clns interface
Ethernet3/1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 39 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 922 milliseconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
Ethernet3/2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 20 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x1, local circuit ID 0x2
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

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

```
interface Ethernet3/1
 ip address 172.30.10.2 255.255.0.0
 ip router isis area1
 no ip route-cache
 duplex half
 isis metric 10
!
interface Ethernet3/2
 ip address 192.168.224.2 255.255.255.0
 ip router isis area1
```

```
 no ip route-cache
 duplex half
router isis area1
 net 01.0000.0309.1234.00
 metric-style wide
 metric 111
```

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

```
Router# show clns interface
Ethernet3/1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 53 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: mekong.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: mekong.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 4 seconds
    Next IS-IS LAN Level-2 Hello in 4 seconds
Ethernet3/2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 30 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x1, local circuit ID 0x2
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 922 milliseconds
```

Where to Go Next

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

Additional References

Related Documents

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

RFCs

RFCs	Title
RFC 1195	*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

Technical Assistance

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

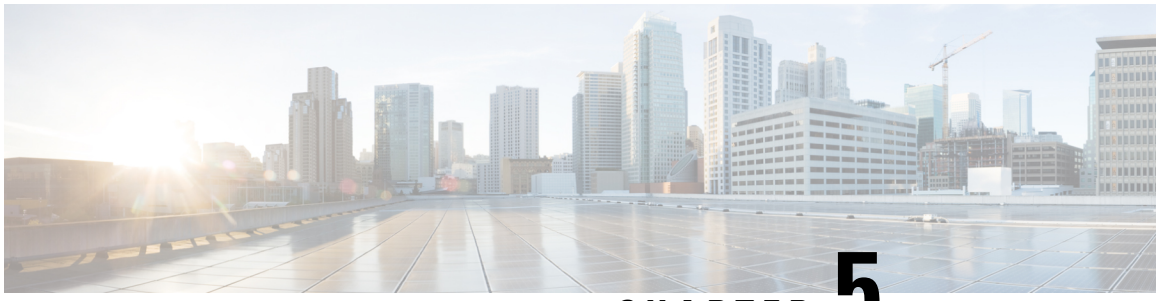
Feature Information for Customizing IS-IS for Your Network Design

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

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

Table 4: Feature Information for Customizing IS-IS for Your Network Design

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



CHAPTER 5

IS-IS MIB

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

- Finding Feature Information, on page 59
- Prerequisites for IS-IS MIB, on page 59
- Restrictions for IS-IS MIB, on page 60
- Information About IS-IS MIB, on page 60
- How to Enable IS-IS MIB, on page 71
- Configuration Examples for IS-IS MIB, on page 77
- Where to Go Next, on page 77
- Additional References, on page 77
- Feature Information for IS-IS MIB, on page 78

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 MIB

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

Restrictions for IS-IS MIB

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

Information About IS-IS MIB

Cisco IS-IS MIB Table Object Definitions

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

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

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

- ciiManAreaAddr
- ciiManAreaAddrExistState

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

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

- ciiAreaAddr

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

- ciiSysProtSuppProtocol
- ciiSysProtSuppExistState

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

- ciiSummAddressType
- ciiSummAddress

- ciiSummAddrPrefixLen
- ciiSummAddrExistState
- ciiSummAddrMetric
- ciiSummAddrFullMetric

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

- ciiRedistributeAddrType
- ciiRedistributeAddrAddress
- ciiRedistributeAddrPrefixLen
- ciiRedistributeAddrExistState

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

- ciiRouterSysID
- ciiRouterLevel
- ciiRouterHostName
- ciiRouterID

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

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

The ciiSysLevelEntry table defines the following MIB objects:

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

- ciiSysLevelSPFConsiders
- ciiSysLevelTEEnabled

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

The ciiCircEntry table contains circuit-specific information about each broadcast or point-to-point interface used in this IS-IS. Each entry is associated with a corresponding interface, based on the circuit type (broadcast or point-to-point interfaces). In other words, only interfaces that are configured as broadcast or point-to-point can be polled. The Cisco implementation of the IS-IS MIB does not support the following circuit types: staticIn, staticOut, dA (dynamically assigned). The ciiCircEntry table defines the following MIB objects:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The ciiISAdjEntry table defines the following MIB objects:

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

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

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

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

- ciiISAdjAreaAddrIndex
- ciiISAdjAreaAddress

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

- ciiISAdjIPAddrIndex
- ciiISAdjIPAddrType
- ciiISAdjIPAddrAddress

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

- ciiISAdjProtSuppProtocol

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

The ciiRAEntry table defines the following MIB objects:

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

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

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

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

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

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

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

The ciiLSPSummaryEntry table defines the following MIB objects:

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

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

- ciiLSPTLVIndex
- ciiLSPTLVSeq
- ciiLSPTLVChecksum

- ciiLSPTLVType
- ciiLSPTLVLen
- ciiLSPTLVValue

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

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

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

Cisco IS-IS MIB Trap Notifications

IS-IS MIB for Generic System-Wide Errors

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

- ciiManualAddressDrops--The ciiManualAddressDrops trap is generated when one of the manually configured area addresses assigned to the system is ignored while computing routes.
- ciiAuthenticationFailure--The ciiAuthenticationFailure trap is generated when the authenticating type information field in the PDU received from a circuit is incorrect. This is an edge-triggered notification.

- ciiIDLenMismatch--When an LSP with a different value of SystemID length is received, the ciiIDLenMismatch notification is generated specific to the circuit where the LSP was detected. This is an edge-triggered notification and hence will be generated only once for PDUs received on the same circuit.
- ciiMaxAreaAddressesMismatch--When the value of Maximum Area Addresses is changed in the LSP that is received from a circuit, the ciiMaxAreaAddressesMismatch trap notification is generated. The header of the packet is used to identify the cause of the mismatch in Maximum Area Address. This trap is an edge-triggered notification and hence will be generated only once for PDUs received on the same circuit.

IS-IS MIB for LSP-Specific Errors

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

- ciiCorruptedLSPDetected--When an LSP stored in memory is corrupted, the ciiCorruptedLSPDetected trap is generated.
- ciiAttemptToExceedMaxSequence--The ciiAttemptToExceedMaxSequence trap is generated each time a sequence number on a generated LSP wraps around the 32-bit sequence counter, forcing it to be purged and hence waiting for its reannouncement.
- ciiOwnLSPPurge--The ciiOwnLSPPurge trap is generated when a LSP is received from a circuit with your systemID and zero age.
- ciiSequenceNumberSkip--When an LSP is received without a SystemID or differing contents, the ciiSequenceNumberSkip trap is generated in order to increment the sequence number by 1.
- ciiAuthenticationTypeFailure--When an LSP is received from a circuit filled with a wrong authentication type field, the ciiAuthenticationTypeFailure notification is generated. This is an edge-triggered notification.
- ciiLSPTooLargeToPropagate--When an attempt is made to send an LSP over the circuit with a size greater than dataLinkBlockSize (link-specific parameter for maximum size of a data packet), the ciiLSPTooLargeToPropagate trap is generated indicating that the LSP could not be propagated. This is an edge-triggered notification and will be generated only once for all PDUs received on the same circuit.

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

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

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

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

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

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

MIB Support for IS-IS Hello PDU-Specific Errors

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

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

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

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

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

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

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

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

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

MIB Support for IS-IS Transition State Changes

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

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

How to Enable IS-IS MIB

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

Before you begin

SNMP must be enabled on your network.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

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

Examples

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

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

What to Do Next

To globally enable all IS-IS traps, refer to the Enabling All IS-IS Traps, on page 73. To enable groups of IS-IS traps, refer to the Enabling IS-IS Error Traps, on page 74 and the Enabling IS-IS State-Change Traps, on page 75.

Enabling All IS-IS Traps

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps isis** **Example:** `Router(config)# snmp-server enable traps isis`	Enables all SNMP notifications defined in the IS-IS MIB. **Note** This step is required only if you wish to enable all IS-IS traps. To enable specific groups of traps, see the Enabling IS-IS Error Traps, on page 74 or the Enabling IS-IS State-Change Traps, on page 75. When you enter the **no snmp-server enable traps isis** command, all IS-IS traps will be disabled.
Step 4	**no snmp-server enable traps isis** [**errors** [*error-type*]] [**state-change** [*state-change-type*]] **Example:** `Router(config)# no snmp-server enable traps isis state-change database-overload`	Disables the sending of SNMP notifications for IS-IS state changes. **Note** This step is required only if you wish to disable a particular trap or set of traps. To enable specific groups of traps, see the Enabling IS-IS Error Traps, on page 74 or the Enabling IS-IS State-Change Traps, on page 75.
Step 5	**exit** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config)# exit`	
Step 6	**show running-config** [*options*] **Example:** `Router# show running-config | include traps`	Displays the running configuration to verify which traps have been enabled.

Examples

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

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

What to Do Next

To enable some but not all IS-IS traps, refer to Enabling IS-IS Error Traps, on page 74. To enable one or more IS-IS state-change traps, refer to Enabling IS-IS State-Change Traps, on page 75.

Enabling IS-IS Error Traps

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps isis** [**errors** [*error-type*]] [**state-change** [*state-change-type*]] **Example:**	Enables SNMP notifications for IS-IS errors. • When you enter the **lsp** keyword for the *error-type*, only the LSP error traps are enabled. (See the

	Command or Action	Purpose
	`Router(config)# snmp-server enable traps isis errors lsp`	**snmp-server enable traps isis** command in the *Cisco IOS IP Routing: ISIS Command Reference* for a list of *error-type* keywords.)
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration sessions and exits global configuration mode.

Examples

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

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

Enabling IS-IS State-Change Traps

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps isis** [**state-change** [*state-change-type*]]	Enables SNMP notifications for IS-IS state changes.

	Command or Action	Purpose
	Example: `Router(config)# snmp-server enable traps isis state-change`	**Note** When the **snmp-server enable traps isis state-change**command is entered without any of the optional keywords, both IS-IS state change traps are enabled. Entering the **no snmp-server enable traps isis state-change**command will disable both IS-IS state-change traps.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration sessions and exits global configuration mode.

Examples

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

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

Verifying IS-IS MIB Traps on the Router

SUMMARY STEPS

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

DETAILED STEPS

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

Configuration Examples for IS-IS MIB

Example Enabling and Verifying IS-IS Error Traps

The following example enables all IS-IS error traps:

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

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

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

Example Enabling and Verifying IS-IS State Change Traps

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

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

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

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

Where to Go Next

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

Additional References

Related Documents

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

Related Topic	Document Title
SNMP configuration	"Configuring SNMP Support" section of the *Cisco IOS Network Management Configuration Guide*
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

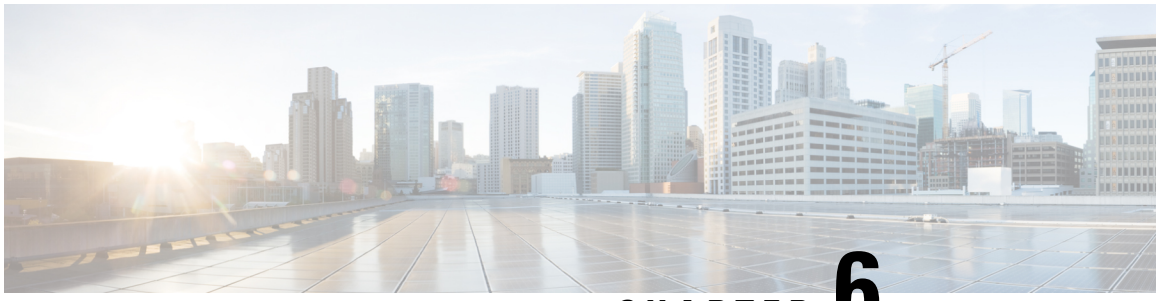
Feature Information for IS-IS MIB

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

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

Table 5: Feature Information for IS-IS MIB

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



CHAPTER 6

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

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

- Finding Feature Information, on page 81
- Prerequisites for IS-IS Support for an IS-IS Instance per VRF for IP, on page 81
- Restrictions for IS-IS Support for an IS-IS Instance per VRF for IP, on page 82
- Information About IS-IS Support for an IS-IS Instance per VRF for IP, on page 82
- How to Configure IS-IS Support for an IS-IS Instance per VRF for IP, on page 83
- Configuration Examples for IS-IS Support for an IS-IS Instance per VRF for IP, on page 87
- Additional References, on page 91
- Feature Information for IS-IS Support for an IS-IS Instance per VRF for IP, on page 92

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 an IS-IS Instance per VRF for IP

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

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

IS-IS VRF support is supported only for IPv4.

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

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

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

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

VRF-Aware IS-IS

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

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

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

For example, an ISP can create three VRFs--VRF First, VRF Second, and VRF Third--to represent three separate customers. A VRF-aware IS-IS instance is created and associated with each VRF: tagFIRST, tagSECOND, and tagTHIRD. Each instance will have its own routing process, IS-IS database, and routing table, and will calculate its own shortest path first (SPF) tree.

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

Creating a VRF

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	`Device(config-vrf)# rd 1:1`	
Step 6	**end** **Example:** `Device(config-vrf)# end`	Exits VRF configuration mode and returns to privileged EXEC mode.

Attaching an Interface to the VRF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
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	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-if)# ip vrf forwarding vrfFirst`	Associates a VPN routing and forwarding instance (VRF) with an interface or subinterface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Creating VRF Aware IS-IS Instances

Before You Begin

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 0/2`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [*secondary*] **Example:** `Router(config-if)# ip address 172.16.11.1 255.255.255.255`	Sets a primary or secondary IP address for an interface.
Step 5	**ip router isis** *process-tag* **Example:**	Configures an IS-IS routing process for IP on an interface and attaches a tag to the routing process.

	Command or Action	Purpose
	`Device(config-if)# ip router isis vrfFirst`	**Note** The configuration of the interface-mode **ip router isis** command will overwrite the prior configuration on that interface, but only if the new configuration is attempting to change the interface ownership to a different instance that is in the same VRF as the currently configured owner instance. The configuration will be rejected if the attempted change is between two instances that are associated with different VRFs.
Step 6	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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** *process-tag* **Example:**	Enables the IS-IS routing protocol, specifies an IS-IS process, and enters router configuration mode.

	Command or Action	Purpose
	`Device(config)# router isis tagFirst`	
Step 4	**vrf** *vrf-name* **Example:** `Device(config-router)# vrf vrfFirst`	Associates an IS-IS instance with a VRF. • It is presumed that the VRF named vrfFirst was previously created.
Step 5	**net** *network-entity-title* **Example:** `Device(config-router)# net 49.000b.0000.0001.0002.00`	Configures an IS-IS NET for a CLNS routing process.
Step 6	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode.

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

Example: Configuring Multiple VRF-Aware IS-IS Instances

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

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

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

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

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

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

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

```
Router# show isis tagThird topology
Tag tagThird:
IS-IS paths to level-2 routers
System Id             Metric  Next-Hop                Interface   SNPA
router-02             10      router-02               Fa4/3       0010.0ddc.e00b
router-03             10      router-03               Et0/2       0006.0e03.0c45
router-04             10      router-04               Fa4/0       000a.f3c3.1c70
.                             router-04               Fa4/1       000a.f3c3.1c71
.
.

Router# show clns tagSecond neighbors
Tag tagSecond:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
router-03      Fa0/2       00d0.2b7f.9502      Up     9         L2   IS-IS
router-03      PO2/2.1     DLCI 211            Up     27        L2   IS-IS
router-02      PO2/0.1     DLCI 131            Up     29        L2   IS-IS
router-11      Fa0/4       000e.d79d.7920      Up     7         L2   IS-IS
router-11      Fa0/5       000e.d79d.7921      Up     8         L2   IS-IS
router-11      PO3/2.1     DLCI 451            Up     24        L2   IS-IS
.
.
.

Router# show isis tagThird database level-2
Tag tagThird:
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
router-01.00-00       0x0000000A    0x5E73       914               0/0/0
router-01.03-00       0x00000001    0x8E41       894               0/0/0
router-01.04-00       0x00000001    0x8747       894               0/0/0
router-03.00-00     * 0x00000005    0x55AD       727               0/0/0
router-03.02-00     * 0x00000001    0x3B97       727               0/0/0
router-02.00-00       0x00000004    0xC1FB       993               0/0/0
router-02.01-00       0x00000001    0x448D       814               0/0/0
router-04.00-00       0x00000004    0x76D0       892               0/0/0
Router# show isis tagThird database level-1
Tag tagThird:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
router-03.00-00      * 0x0000000B   0xBDF6        1005              1/0/0
router-03.02-00      * 0x00000001   0xC473        940               0/0/0
router-07.00-00        0x00000006   0x403A        940               0/0/0
Router# show clns tagSecond protocol
IS-IS Router: tagSecond
```

```
  System Id: 0000.0001.0002.00  IS-Type: level-2-only
  Manual area address(es):
        49.000b
  Routing for area address(es):
        49.000b
  Interfaces supported by IS-IS:
        FastEthernet4/1 - IP
        FastEthernet4/0 - IP
        Ethernet0/2 - IP
        FastEthernet4/3 - IP
  Redistributing:
    static
  Distance: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
Router# show clns tagThird protocol
IS-IS Router: tagThird
  System Id: 0000.0001.0001.00  IS-Type: level-1-2
  Manual area address(es):
        49.000b
  Routing for area address(es):
        49.000b
  Interfaces supported by IS-IS:
        POS2/2.1 - IP
        FastEthernet0/2 - IP
        FastEthernet0/4 - IP
        POS2/0.1 - IP
        FastEthernet0/5 - IP
        POS3/2.1 - IP
  Redistributing:
    static
  Distance: 110
  RRR level: none
  Generate narrow metrics: none
  Accept narrow metrics:   none
  Generate wide metrics:   level-1-2
  Accept wide metrics:     level-1-2
```

Example: Creating an IS-IS Instance Without a Process Tag

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

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

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

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

Example: Redistributing Routes from an IS-IS Instance

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

In order to redistribute between two different IS-IS instances they must be configured in the same VRF context.

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

Example: Changing the Interface Ownership

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

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

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

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

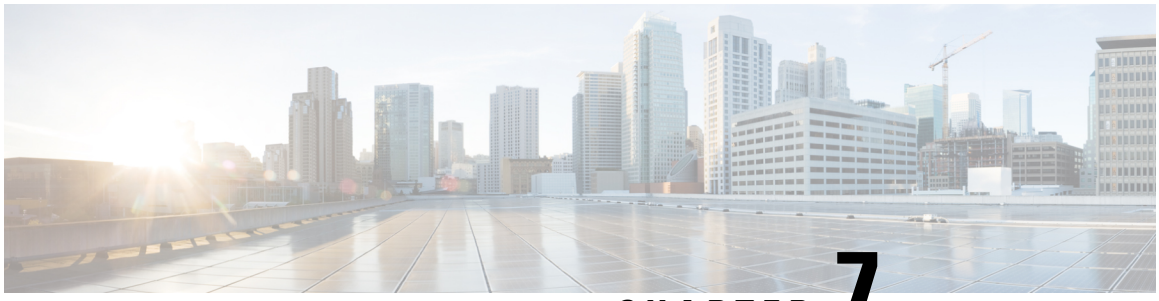
Feature Information for IS-IS Support for an IS-IS Instance per VRF for IP

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

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

Table 6: Feature Information for IS-IS Support for an IS-IS Instance per VRF for IP

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



CHAPTER 7

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, on page 93
- Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, on page 94
- Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , on page 94
- How to Create, Monitor and Make Changes to Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , on page 95
- Configuration Examples for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , on page 103
- ""Where to Go Next, on page 106
- Additional References for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, on page 107
- Feature Information for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters , on page 108

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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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`	Assigns a tag to an IS-IS process. Enters router configuration mode. • Configure tags to identify multiple IS-IS processes by giving a meaningful name for each routing process. If the tag is not specified, a null tag (0) is assumed and the process is referenced with a null tag. The tag name must be unique among all IP router processes for the device.
Step 4	**net** *network-entity-title* **Example:** `Device(config-router)# net 49.0001.0000.0000.000b.00`	Configures the NET on the device. • The NET identifies the device for IS-IS.
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:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [*secondary*] **Example:** `Device(config-if)# ip address 172.16.1.27 255.255.255.0`	Sets the primary IP address on the interface.
Step 5	**ip router isis** [*area-tag*] **Example:** `Device(config-if)# ip router isis company1`	Enables IS-IS on the interfaces that are to use IS-IS to distribute their IP information (and additionally that might be used to establish IS-IS adjacencies). • Use the *area-tag* argument to specify to which IS-IS process the 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	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring IS-IS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **isis display delimiter** [**return** *count* | **character** *count*]
4. **exit**
5. **show ip protocols**
6. **show clns** *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**] [**l1**] [**l2**] [**detail**] [**lspid**]
12. **show isis database verbose**
13. **show isis lsp-log**
14. **show isis** [*area-tag*] [**ipv6** | *] **spf-log**
15. **show isis** [*process-tag*] [**ipv6** | *] **topology**
16. **show isis** [*area-tag*] **neighbors** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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	**isis display delimiter** [**return** *count*	**character** *count*] **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.
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. • 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** [*type number*] [**detail**] **Example:** `Device# show clans is-neighbors detail`	Displays IS-IS information for IS-IS device adjacencies.
Step 7	**show clns interface** [*type number*] **Example:**	List the CLNS-specific information about each interface.

	Command or Action	Purpose
	`Device# show clns interface`	
Step 8	**show clns** *area-tag* **neighbors** [*type number*] [**area**] [**detail**] **Example:** `Device# show clns area3 neighbors`	Displays both ES and IS neighbors. • The **show clns neighbor** command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your 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: • The number of link-state PDUs (LSPs) can help you determine the stability of the IS-IS network. The number of LSPs should never be zero. However, an LSP count that keeps increasing over a short time period indicates a network issue. • LSP retransmissions should stay low. A later execution of the **show clns traffic** command that shows an increase in LSP retransmissions, as compared to an earlier execution of the command, can indicate instability or traffic problems. • To check for partial route calculations (PRCs), enter the **show clns traffic** command. PRCs are flooded when a change that does not affect topology is reported through an LSP; typical examples include the addition or removal of a prefix or metric changes for external or passive interfaces. A PRC update queue that remains full or increases to the maximum value for long periods of time indicates network instability. • LSP checksum errors indicate a problem. • The update queue should not stay full and should not drop much.
Step 10	**show ip route** [*ip-address* [*mask*]] [[**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]]	Displays the current state of the routing table.

	Command or Action	Purpose
	Example: `Device# show ip route 172.16.0.21`	
Step 11	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Device# show isis database detail`	Displays additional information about the IS-IS database. • Displays the link-state database for Level-1 and Level-2, the contents for each LSP, and the link-state protocol PDU identifier.
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** [*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. • 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.
Step 15	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **Example:** `Device# show isis topology`	Displays a list of all connected devices in all areas.
Step 16	**show isis** [*area-tag*] **neighbors** [**detail**] **Example:** `Device# show isis neighbors detail`	Displays IS-IS adjacency information. • The **show isis neighbor detail** command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your 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 reenable the protocol at a suitable time.

Before the introduction of the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature, there was no nondestructive way to disable IS-IS operation. The only way to disable IS-IS at the 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	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.
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. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router isis** *area-tag* **Example:** `Device(config)# router isis 1`	Enables the IS-IS routing protocol and specifies an IS-IS process. • Enters router configuration mode.
Step 4	**protocol shutdown** **Example:** `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.
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
```

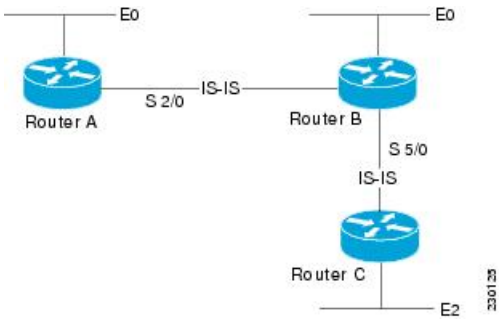
The **show isis spf-log** command displays logs of Level 1 and Level 2 LSPs including time of occurrence, duration, count, and the event that triggered the LSP.

```
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)#
```

```
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 area1
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 area1
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	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of IS-IS concepts	"Integrated IS-IS Routing Protocol Overview" module
Customizing IS-IS for achieving fast convergence and scalability	"Overview of IS-IS Fast Convergence" module

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* (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

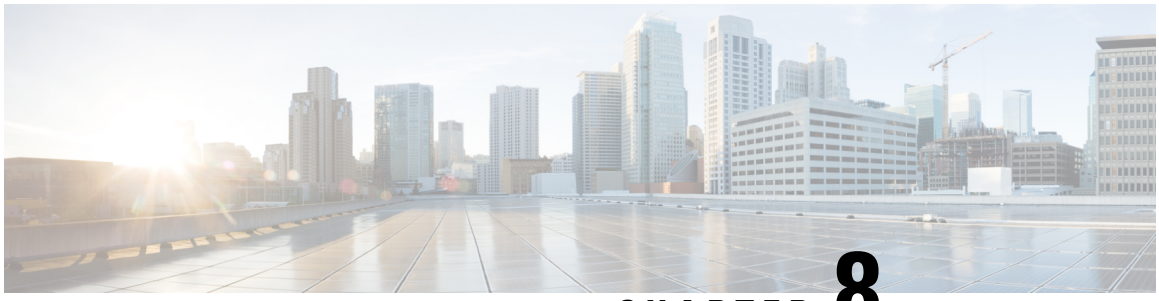
Feature Information for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: 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		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.



CHAPTER 8

Overview of IS-IS Fast Convergence

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

- Finding Feature Information, on page 109
- Prerequisites for IS-IS Fast Convergence, on page 109
- Information About IS-IS Fast Convergence, on page 109
- Where to Go Next, on page 110
- Additional References, on page 111

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 Fast Convergence

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

Information About IS-IS Fast Convergence

Network Convergence

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

routes as well as the network topology. Fast convergence benefits network performance. Routing algorithms that converge slowly may cause temporary routing loops or temporary network unavailability.

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

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

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

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

Design Recommendations for Achieving Faster Network Convergence

A faster processor can provide better performance for network convergence.

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

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

Where to Go Next

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

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

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

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

Additional References

Related Documents

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

Standards

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

MIBs

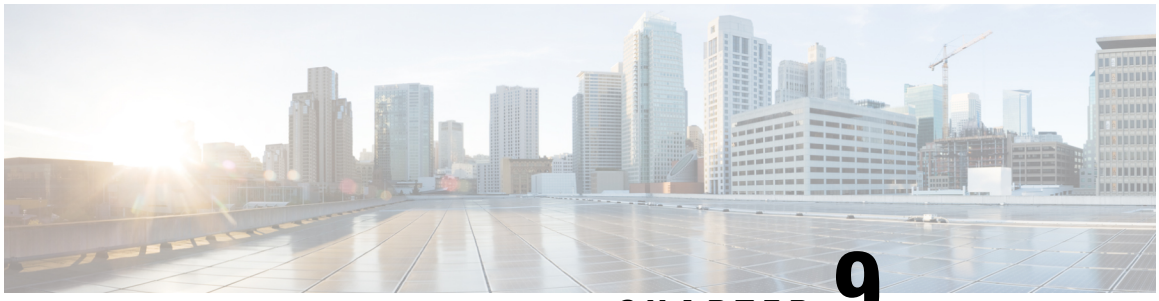
MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

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



CHAPTER 9

Setting Best Practice Parameters for IS-IS Fast Convergence

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

- Finding Feature Information, on page 113
- Prerequisites for Setting Best Practice Parameters for IS-IS Fast Convergence, on page 113
- Information About Setting Best Practice Parameters for IS-IS Fast Convergence, on page 114
- How to Set Best Practice Parameters for IS-IS Fast Convergence, on page 114
- Configuration Examples for Setting Best Practice Parameters for IS-IS Fast Convergence, on page 116
- Where to Go Next, on page 117
- Additional References, on page 117
- Feature Information for Setting Best Practice Parameters for IS-IS Fast Convergence, on page 118

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 Setting Best Practice Parameters for IS-IS Fast Convergence

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

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

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

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

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

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

Setting Best Practice Parameters for IS-IS Fast Convergence

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**router isis [area-** *tag* **]** **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**is-type** [**level-1** | **level-1-2** | **level-2-only**] **Example:** `Router(config-router)# is-type level-1`	Configures the routing level for an instance of the IS-IS routing process. • It is recommended that IS-IS nodes that operate at a single level be configured as Level 1 to minimize the number of adjacencies, LDSBs, and related SPF and PRC calculations. **Note** You can also set the IS-IS level type on the interface by entering the **isis circuit-type** command.
Step 5	**metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**] **Example:** `Router(config-router)# metric-style wide`	Globally changes the metric value for all IS-IS interfaces. • Wide style metrics are required for prefix tagging.
Step 6	**set-overload-bit** [**on-startup** {*seconds* | **wait-for-bgp**}] [**suppress** {**interlevel**| **external**}] **Example:** `Router(config-router)# set-overload-bit on-startup 360`	Configures the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations. • Setting the overload bit gives the router enough time to build its BGP and CEF tables prior to the router being used as a transit node.
Step 7	**no hello padding** **Example:** `Router(config-router)# no hello padding`	Disables IS-IS hello padding at the router level. • By default the IS-IS Hello PDUs are padded to the full MTU size, possibly having a negative impact on time-sensitive application traffic that travels across low-bandwidth interfaces or on interface buffer resources when frequent hellos are configured. It is recommended to globally disable hello padding.
Step 8	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 9	**show clns** [*domain* | *area-tag*] **protocol** **Example:**	Lists the protocol-specific information for each ISO IGRP or IS-IS routing process in the router.

	Command or Action	Purpose
	`Router(config-if)# show clns protocol`	

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

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

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

Router A

```
!
clns routing
process-max-time 50
ip routing protocol purge interface
router isis
 passive-interface Loopback0
 net 49.1962.XXXX.XXXX.XXXX.00
 is-type level-2-only
 ispf level-2
 log-adjacency-changes
 ignore-lsp-errors
 metric-style wide level-2
 external overload signalling !Configure on Cisco 12000 series Internet routers
 set-overload-bit on-startup 180
 max-lsp-lifetime 65535
 lsp-refresh-interval 65000
 spf-interval 5 1 50
 prc-interval 5 1 50
 lsp-gen-interval 5 1 50
 no hello padding
 authentication mode md5 level-2
 authentication key-chain ON
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
interface GigabitEthernet x/x
 negotiation auto
 ip router isis
 mtu 4470
 isis network point-to-point
 isis metric <metric> level-2
 isis circuit-type level-2-only
 isis authentication mode md5 level-2
 isis authentication key-chain ON
 carrier-delay ms 0
 dampening
interface POSx/y
```

```
 carrier-delay msec 0
 dampening
 ip router isis
 no peer neighbor-route
 isis metric 1 level-2
 isis circuit-type level-2-only
 isis authentication mode md5 level-2
 isis authentication key-chain ON
 pos ais-shut
 pos report lais
 pos report lrdi
 pos report pais
 pos report prdi
 pos report slos
 pos report slof
!
key chain ON
 key 1
  key-string mypassword
```

Where to Go Next

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

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

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

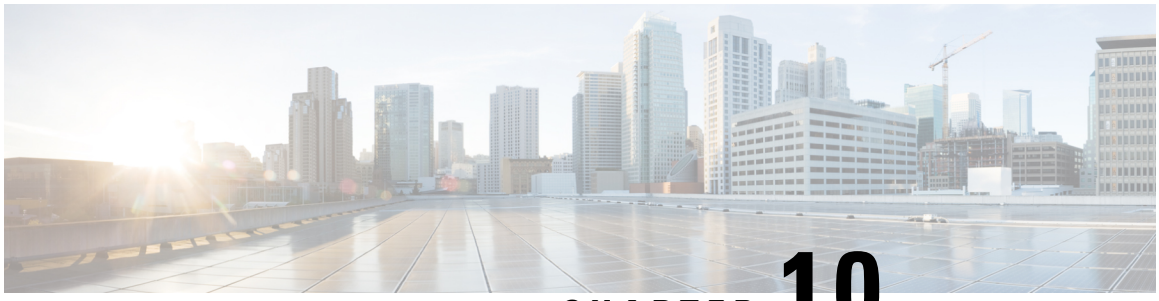
Feature Information for Setting Best Practice Parameters for IS-IS Fast Convergence

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

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

Table 8: Feature Information for Setting Best Practice Parameters for IS-IS Fast Convergence

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



CHAPTER 10

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, on page 119
- Prerequisites for Reducing Failure Detection Times in IS-IS Networks, on page 119
- Information About Reducing Failure Detection Times in IS-IS Networks, on page 120
- How to Reduce Failure Detection Times in IS-IS Networks, on page 120
- Configuration Examples for Reducing Failure Detection Times in IS-IS Networks, on page 126
- Where to Go Next, on page 126
- Additional References, on page 126
- Feature Information for Reducing Failure Detection Times in IS-IS Networks, on page 127

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 resignaled with the default hello interval. A faster hello interval prevents this resignaling. To configure a faster hello interval, you need to decrease the ISIS hello interval manually using the **isis hello-interval**command.

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

Importance of Fast Network Failure Detection

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Enters interface configuration mode.
Step 4	**dampening** [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress-time* [*restart-penalty*]] **Example:** `Device(config-if)# dampening`	Enables interface dampening. • Entering the **dampening** command without any keywords or arguments enables interface dampening with the default configuration parameters. **Note** The default values for the *half-life-period*, *reuse-threshold*, *suppress-threshold*, *max-suppress-time*, and *restart-penalty* arguments are 5, 1000, 2000, 20, and 2000, respectively. • When the timer for the *restart-penalty* argument is manually configured, the values must be manually entered for all arguments.
Step 5	**end** **Example:** `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.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:**	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. • 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.

	Command or Action	Purpose
		Note A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network, due to false failure detection events. A slower hello interval saves bandwidth and CPU. Especially when used in combination with a higher hello multiplier, this configuration may increase overall network stability, but has typical slower network convergence as a consequence.
Step 5	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**] **Example:** `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. • 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** *interface-type interface-number* **Example:**	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.
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**] [**l1**] [**l2**] [**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. • Enter your password if prompted.

	Command or Action	Purpose
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.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**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. • 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	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview"

Standards

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

RFCs

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

Technical Assistance

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

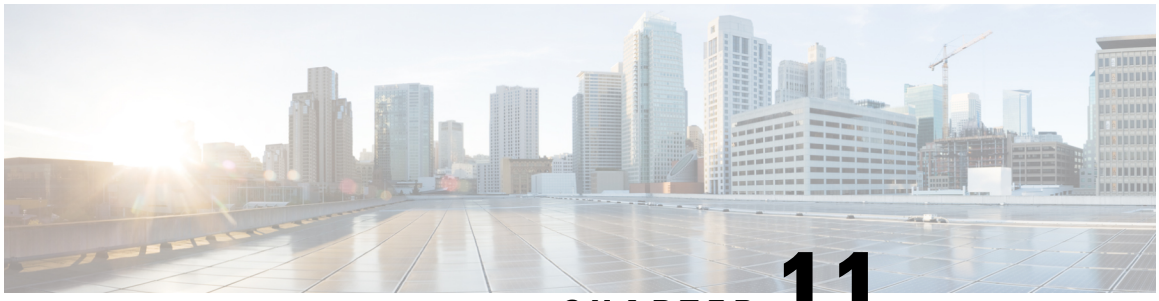
Feature Information for Reducing Failure Detection Times in IS-IS Networks

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

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

Table 9: Feature Information for Reducing Failure Detection Times in IS-IS Networks

Feature Name	Software Releases	Feature Information
IS-IS Support for BFD over IPv4	12.4(4)T	Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.
Integrated IS-IS Point-to-Point Adjacency over Broadcast Media		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.



CHAPTER 11

IPv6 Routing: IS-IS Multitopology Support for IPv6

IS-IS multitopology support for IPv6 allows IS-IS to maintain a set of independent topologies within a single area or domain.

- Finding Feature Information, on page 129
- IPv6 Routing: IS-IS Multitopology Support for IPv6, on page 129
- How to Configure IPv6 Routing: IS-IS Multitopology Support for IPv6, on page 130
- Configuration Examples for IPv6 Routing: IS-IS Multitopology Support for IPv6, on page 135
- Additional References, on page 138
- Feature Information for IPv6 Routing: IS-IS Multitopology Support for IPv6, on page 139

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.

IPv6 Routing: IS-IS Multitopology Support for IPv6

IS-IS Enhancements for IPv6

IS-IS in IPv6 functions the same and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. Extensions to the IS-IS command-line interface (CLI) allow configuration of IPv6-specific parameters. IPv6 IS-IS extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

IS-IS in IPv6 supports either single-topology mode or multiple topology mode.

IS-IS Multitopology Support for IPv6

IS-IS multitopology support for IPv6 allows IS-IS to maintain a set of independent topologies within a single area or domain. This mode removes the restriction that all interfaces on which IS-IS is configured must support the identical set of network address families. It also removes the restriction that all routers in the IS-IS area (for Level 1 routing) or domain (for Level 2 routing) must support the identical set of network layer address families. Because multiple SPFs are performed, one for each configured topology, it is sufficient that connectivity exists among a subset of the routers in the area or domain for a given network address family to be routable.

You can use the **isis ipv6 metric** command to configure different metrics on an interface for IPv6 and IPv4.

When multitopology support for IPv6 is used, use the **metric-style wide**command to configure IS-IS to use new-style TLVs because TLVs used to advertise IPv6 information in link-state packets (LSPs) are defined to use only extended metrics.

Transition from Single-Topology to Multitopology Support for IPv6

All routers in the area or domain must use the same type of IPv6 support, either single-topology or multitopology. A router operating in multitopology mode will not recognize the ability of the single-topology mode router to support IPv6 traffic, which will lead to holes in the IPv6 topology. To transition from single-topology support to the more flexible multitopology support, a multitopology transition mode is provided.

The multitopology transition mode allows a network operating in single-topology IS-IS IPv6 support mode to continue to work while upgrading routers to include multitopology IS-IS IPv6 support. While in transition mode, both types of TLVs (single-topology and multitopology) are sent in LSPs for all configured IPv6 addresses, but the router continues to operate in single-topology mode (that is, the topological restrictions of the single-topology mode are still in effect). After all routers in the area or domain have been upgraded to support multitopology IPv6 and are operating in transition mode, transition mode can be removed from the configuration. Once all routers in the area or domain are operating in multitopology IPv6 mode, the topological restrictions of single-topology mode are no longer in effect.

How to Configure IPv6 Routing: IS-IS Multitopology Support for IPv6

Configuring Multitopology IS-IS for IPv6

When multitopology IS-IS for IPv6 is configured, the **transition** keyword allows a user who is working with the single-topology SPF mode of IS-IS IPv6 to continue to work while upgrading to multitopology IS-IS. After every router is configured with the **transition** keyword, users can remove the **transition** keyword on each router. When transition mode is not enabled, IPv6 connectivity between routers operating in single-topology mode and routers operating in multitopology mode is not possible.

You can continue to use the existing IPv6 topology while upgrading to multitopology IS-IS. The optional **isis ipv6 metric** command allows you to differentiate between link costs for IPv6 and IPv4 traffic when operating in multitopology mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**
5. **address-family ipv6** [**unicast** | **multicast**]
6. **multi-topology** [**transition**]

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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**metric-style wide** [**transition**] [**level-1**	**level-2**	**level-1-2** **Example:** `Device(config-router)# metric-style wide level-1`	Configures a router running IS-IS to generate and accept only new-style TLVs.
Step 5	**address-family ipv6** [**unicast**	**multicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. • The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 6	**multi-topology** [**transition**] **Example:** `Device(config-router-af)# multi-topology`	Enables multitopology IS-IS for IPv6. • The optional **transition** keyword allows an IS-IS IPv6 user to continue to use single-topology mode while upgrading to multitopology mode.

Customizing IPv6 IS-IS

Perform this task to configure a new administrative distance for IPv6 IS-IS, configure the maximum number of equal-cost paths that IPv6 IS-IS will support, configure summary prefixes for IPv6 IS-IS, and configure an IS-IS instance to advertise the default IPv6 route (::/0). It also explains how to configure the hold-down period between partial route calculations (PRCs) and how often Cisco IOS software performs the SPF calculation when using multitopology IS-IS.

You can customize IS-IS multitopology for IPv6 for your network, but you likely will not need to do so. The defaults for this feature are set to meet the requirements of most customers and features. If you change the defaults, refer to the IPv4 configuration guide and the IPv6 command reference to find the appropriate syntax.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **default-information originate** [**route-map** *map-name*]
6. **distance** *value*
7. **maximum-paths** *number-paths*
8. **summary-prefix** *ipv6-prefix prefix-length* [**level-1** | **level-1-2**| **level-2**]
9. **prc-interval** *seconds* [*initial-wait*] [*secondary-wait*]
10. **spf-interval** [**level-1** | **level-2**] *seconds initial-wait*] [*secondary-wait*]
11. **exit**
12. **interface** *type number*
13. **isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**]

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** *area-tag* **Example:** `Device(config)# router isis area2`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 4	**address-family ipv6** [**unicast**	**multicast**] **Example:**	Specifies the IPv6 address family, and enters address family configuration mode.

	Command or Action	Purpose
	`Device(config-router)# address-family ipv6`	• The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**default-information originate** [**route-map** *map-name*] **Example:** `Device(config-router-af)# default-information originate`	(Optional) Injects a default IPv6 route into an IS-IS routing domain. • The **route-map** keyword and *map-name* argument specify the conditions under which the IPv6 default route is advertised. • If the **route map** keyword is omitted, then the IPv6 default route will be unconditionally advertised at Level 2.
Step 6	**distance** *value* **Example:** `Device(config-router-af)# distance 90`	(Optional) Defines an administrative distance for IPv6 IS-IS routes in the IPv6 routing table. • The *value*argument is an integer from 10 to 254. (The values 0 to 9 are reserved for internal use).
Step 7	**maximum-paths** *number-paths* **Example:** `Device(config-router-af)# maximum-paths 3`	(Optional) Defines the maximum number of equal-cost routes that IPv6 IS-IS can support. • This command also supports IPv6 Border Gateway Protocol (BGP) and Routing Information Protocol (RIP). • The *number-paths* argument is an integer from 1 to 64. The default for BGP is one path; the default for IS-IS and RIP is 16 paths.
Step 8	**summary-prefix** *ipv6-prefix prefix-length* [**level-1** | **level-1-2**| **level-2**] **Example:** `Device(config-router-af)# summary-prefix 2001:DB8::/24`	(Optional) Allows a Level 1-2 router to summarize Level 1 prefixes at Level 2, instead of advertising the Level 1 prefixes directly when the router advertises the summary. • The *ipv6-prefix* argument in the **summary-prefix** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. • The *prefix-length* argument is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Step 9	**prc-interval** *seconds* [*initial-wait*] [*secondary-wait*] **Example:**	(Optional) Configures the hold-down period between PRCs for multitopology IS-IS for IPv6.

	Command or Action	Purpose
	`Device(config-router-af)# prc-interval 20`	
Step 10	**spf-interval** [**level-1** | **level-2**] *seconds initial-wait* [*secondary-wait*] **Example:** `Device(config-router-af)# spf-interval 30`	(Optional) Configures how often Cisco IOS software performs the SPF calculation for multitopology IS-IS for IPv6.
Step 11	**exit** **Example:** `Device(config-router-af)# exit`	Exits address family configuration mode, and returns the router to router configuration mode. • Repeat this step to exit router configuration mode and return the router to global configuration mode.
Step 12	**interface** *type number* **Example:**	Specifies the interface type and number, and enters interface configuration mode.
Step 13	**isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**] **Example:** `Device(config-if)# isis ipv6 metric 20`	(Optional) Configures the value of an multitopology IS-IS for IPv6 metric.

Verifying IPv6 IS-IS Configuration and Operation

SUMMARY STEPS

1. **enable**
2. **show ipv6 protocols** [**summary**]
3. **show isis** [*process-tag*] [**ipv6** | *****] **topology**
4. **show clns** [*process-tag*] **neighbors** *interface-type interface-number*] [**area**] [**detail**]
5. **show clns** *area-tag* **is-neighbors** [*type number*] [**detail**]
6. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
7. **show isis ipv6 rib** [*ipv6-prefix*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 protocols** [**summary**] **Example:**	Displays the parameters and current state of the active IPv6 routing processes.

	Command or Action	Purpose
	`Device# show ipv6 protocols`	
Step 3	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **Example:** `Device# show isis topology`	Displays a list of all connected routers running IS-IS in all areas.
Step 4	**show clns** [*process-tag*] **neighbors** *interface-type interface-number*] [**area**] [**detail**] **Example:** `Device# show clns neighbors detail`	Displays end system (ES), intermediate system (IS), and multitopology IS-IS (M-ISIS) neighbors.
Step 5	**show clns** *area-tag* **is-neighbors** [*type number*] [**detail**] **Example:** `Device# show clns is-neighbors detail`	Displays IS-IS adjacency information for IS-IS neighbors. • Use the **detail** keyword to display the IPv6 link-local addresses of the neighbors.
Step 6	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Device# show isis database detail`	Displays the IS-IS link-state database. • In this example, the contents of each LSP are displayed using the **detail** keyword.
Step 7	**show isis ipv6 rib** [*ipv6-prefix*] **Example:** `Device# show isis ipv6 rib`	Displays the IPv6 local RIB.

Configuration Examples for IPv6 Routing: IS-IS Multitopology Support for IPv6

Example: Configuring the IS-IS IPv6 Metric for Multitopology IS-IS

The following example sets the value of an IS-IS IPv6 metric to 20:

```
interface Ethernet 0
 isis ipv6 metric 20
```

Example: Configuring IS-IS for IPv6

In the following example, output information about the parameters and current state of that active IPv6 routing processes is displayed using the **show ipv6 protocols**command:

```
Device# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    GigabitEthernet0/0/3
    GigabitEthernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Address Summarization:
    L2: 2001:DB8:33::/16  advertised with metric 0
    L2: 2001:DB8:44::/16  advertised with metric 20
    L2: 2001:DB8:66::/16  advertised with metric 10
    L2: 2001:DB8:77::/16  advertised with metric 10
```

In the following example, output information about all connected routers running IS-IS in all areas is displayed using the **show isis topology**command:

```
Device# show isis topology
IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000C
0000.0000.000D  20      0000.0000.00AA  Se1/0/1         *HDLC*
0000.0000.000F  10      0000.0000.000F  GE0/0/1         0050.e2e5.d01d
0000.0000.00AA  10      0000.0000.00AA  Se1/0/1         *HDLC*
IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000A  10      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000B  20      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000C  --
0000.0000.000D  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
0000.0000.000E  30      0000.0000.000A  GE0/0/3         0010.f68d.f063
```

In the following example, output information to confirm that the local router has formed all the necessary IS-IS adjacencies with other IS-IS neighbors is displayed using the **show clns is-neighbors**command. To display the IPv6 link-local addresses of the neighbors, specify the **detail** keyword.

```
Device# show clns is-neighbors detail
System Id      Interface   State  Type Priority  Circuit Id         Format
0000.0000.00AA Se1/0/1     Up     L1   0         00                 Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::YYYY:D37C:C854:5
  Uptime: 17:21:38
0000.0000.000F Et0/0/1     Up     L1   64        0000.0000.000C.02  Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::XXXX:E2FF:FEE5:D01D
  Uptime: 17:21:41
0000.0000.000A Et0/0/3     Up     L2   64        0000.0000.000C.01  Phase V
  Area Address(es): 49.000b
  IPv6 Address(es): FE80::ZZZZ:F6FF:FE8D:F063
  Uptime: 17:22:06
```

In the following example, detailed output information that displays both end system (ES) and intermediate system (IS) neighbors is displayed using the **show clns neighbors** command with the **detail** keyword.

```
Device# show clns neighbors detail
System Id          Interface    SNPA            State  Holdtime  Type Protocol
0000.0000.0007     GE3/3        aa00.0400.6408  UP     26        L1   IS-IS
Area Address(es): 20
IP Address(es): 172.16.0.42*
Uptime: 00:21:49
0000.0C00.0C35     GE3/2        0000.0c00.0c36  Up     91        L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.42*
Uptime: 00:21:52
0800.2B16.24EA     GE3/3        aa00.0400.2d05  Up     27        L1   M-ISIS
Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
0800.2B14.060E     GE3/2        aa00.0400.9205  Up     8         L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52
```

In the following example, detailed output information about LSPs received from other routers and the IPv6 prefixes they are advertising is displayed using the **show isis database**command with the **detail** keyword specified:

```
Device# show isis database detail
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
 --More--
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:DB8::/64
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.000A.00-00  0x00000059   0x378A        949               0/0/0
  Area Address: 49.000b
  NLPID:        0x8E
  IPv6 Address: 2001:DB8:1:1:1:1:1:1
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IPv6 2001:DB8:3:YYYY::/64
  Metric: 10         IPv6 2001:DB8:2:YYYY::/64
  Metric: 10         IS-Extended 0000.0000.000A.01
  Metric: 10         IS-Extended 0000.0000.000B.00
  Metric: 10         IS-Extended 0000.0000.000C.01
```

```
  Metric: 0           IPv6 11:1:YYYY:1:1:1:1:1/128
  Metric: 0           IPv6 11:2:YYYY:1:1:1:1:1/128
  Metric: 0           IPv6 11:3:YYYY:1:1:1:1:1/128
  Metric: 0           IPv6 11:4:YYYY:1:1:1:1:1/128
  Metric: 0           IPv6 11:5:YYYY:1:1:1:1:1/128
0000.0000.000A.01-00  0x00000050   0xB0AF        491               0/0/0
  Metric: 0           IS-Extended 0000.0000.000A.00
  Metric: 0           IS-Extended 0000.0000.000B.00
```

The following example shows output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.

```
Device# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  2001:DB8:88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
* 2001:DB8:1357:1::/64
    via FE80::202:7DFF:FE1A:9471/GigabitEthernet2/1/0, type L2  metric 10 LSP [4/9]
* 2001:DB8:45A::/64
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACC9/GigabitEthernet2/0/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/GigabitEthernet2/1/0, type L2  metric 20 LSP [3/7]
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
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	" *Reducing Link Failure and Topology Change Notification Times in IS-IS Networks* " module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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

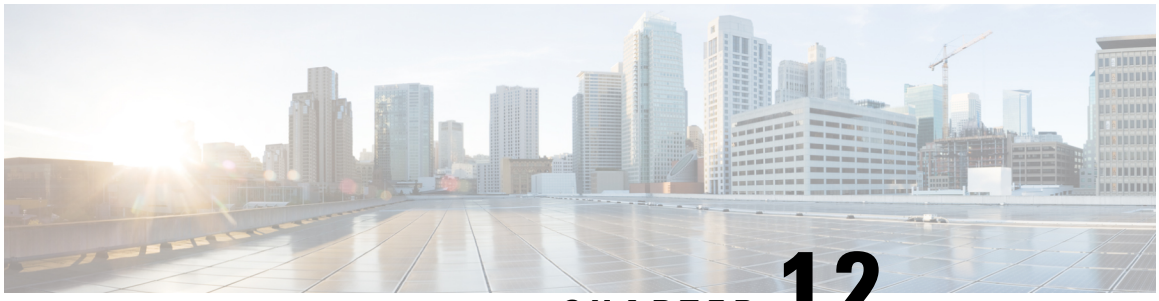
Feature Information for IPv6 Routing: IS-IS Multitopology Support for IPv6

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

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

Table 10: Feature Information for IPv6 Routing: IS-IS Multitopology Support for IPv6

Feature Name	Releases	Feature Information
IPv6 Routing: IS-IS Multitopology Support for IPv6		IS-IS multitopology support for IPv6 allows IS-IS to maintain a set of independent topologies within a single area or domain. The following commands were introduced or modified: **address-family ipv6**, **multi-topology**, **router isis**.



CHAPTER 12

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

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

- Finding Feature Information, on page 141
- Prerequisites for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks, on page 141
- Information About Reducing Link Failure and Topology Change Notification Times in IS-IS Networks, on page 142
- How to Reduce Link Failure and Topology Change Notification Times in IS-IS Networks, on page 144
- Configuration Examples for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks, on page 148
- Where to Go Next, on page 149
- Additional References, on page 149
- Feature Information for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks, on page 150

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

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

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

IS-IS LSP Generation Interval and Lifetime

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

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

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

IS-IS Throttling Timers That Affect Fast Convergence

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

IS-IS PDUs

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

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

LSP-Related Intervals and Exponential Backoff Timers

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

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

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

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

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

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

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

IS-IS Hello PDU Timers

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

- **Hello interval** --Number of seconds during two consecutive transmissions of IIH PDUs.
- **Hello interval minimum** --When the hello interval is configured, the hold time is set to one second. The significance of the hello multiplier changes if Fast Hellos are used; the hello multiplier becomes the number of hellos that will be sent per second.
- **Hello multiplier** --An integer from 1 to 300 that is used to calculate the hold time. The hold time is the number of seconds during which the router will wait for an IIH before declaring that its neighbor is lost.

The router multiplies the hello interval by the hello multiplier to determine the hold time. To avoid unnecessary adjacency resets, increase the default value of 3 on interfaces where frequent losses of IIH PDUs are detected.

- **IS-IS retransmit interval** --Specifies the number of seconds between the resending of IS-IS link-state PDU transmissions for point-to-point links.

CSNP Interval

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

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

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

If you are using a routing algorithm based on SPF and if you use values for the initial required delay that are fewer than 40 milliseconds, SPF may start before the LSP that triggered SPF is flooded to neighbors. The router should always flood, at least, the LSP that triggered SPF before the router runs the SPF computation. LSP flooding is required in order to guarantee that the network update in the LSP is propagated around the network as quickly as possible.

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

Tuning SPF PRC and LSP Generation Exponential Backoff Timers

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**spf-interval** [**level-1** | **level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*] **Example:** `Router(config-router)# spf-interval 5 1 20`	Customizes IS-IS throttling of SPF calculations. **Note** The recommended values for the *spf-max-wait*, *spf-initial-wait*, and *spf-second-wait* arguments are 5, 1, and 20, respectively.
Step 5	**prc-interval** *prc-max-wait* [*prc-initial-wait prc-second-wait*] **Example:** `Router(config)# prc-interval 5 1 20`	Customizes IS-IS throttling of PRC calculations. **Note** The recommended values for the *prc-max-wait*, *prc-initial-wait*, and *prc-second-wait* arguments are 5, 1, and 20, respectively.
Step 6	lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*] **Example:** `Router(config-router)# lsp-gen-interval 5 1 20`	Sets the minimum interval at which link-state PDUs (LSPs) are generated. **Note** The recommended values for the *lsp-max-wait*, *lsp-initial-wait*, and *lsp-second-wait* arguments are 5, 1, and 20, respectively.
Step 7	**max-lsp-lifetime** [**hours**] *value* **Example:** `Router(config-router)# max-lsp-lifetime 65535`	Sets the maximum time for which LSPs persist without being refreshed. • To reduce network resources used for LSP generation, increase the LSP maximum lifetime value of 65535.
Step 8	**lsp-refresh-interval** *seconds* **Example:** `Router(config-router)# lsp-refresh-interval 65535`	Sets the minimum interval at which LSPs are refreshed. • To reduce network resources used for LSP refresh, increase the value to the LSP refresh interval to maximum value of 65535 seconds.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

Enabling IS-IS Fast-Flooding of LSPs

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required, and enters router configuration mode.
Step 4	**fast-flood** *lsp-number* **Example:** `Router(config-router)# fast-flood 20`	Fast-floods LSPs. • Keep the default values for the **isis retransmit-interval** and **isis retransmit-throttle-interval** commands when you configure the **fast-flood** command.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show running-config** **Example:** `Router# show running-config`	(Optional) Verifies that fast-flooding has been enabled.

Monitoring IS-IS Network Convergence Time

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**isis display delimiter** [**return** *count*	**character** *count*] **Example:** `Router(config)# isis display delimiter return 2`	(Optional) Makes output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information.
Step 4	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:**	(Optional) Displays the IS-IS link-state database.

	Command or Action	Purpose
	`Router# show isis database detail`	
Step 6	**show isis** [*area-tag*] **routes** **Example:** `Router# show isis financetag routes`	(Optional) Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
Step 7	**show isis spf-log** **Example:** `Router# show isis spf-log`	(Optional) Displays how often and why the router has run a full SPF calculation.
Step 8	**show isis** [*process-tag*] **topology** **Example:** `Router# show isis financetag topology`	(Optional) Displays a list of all connected routers in all areas. • If a process tag is specified, output is limited to the specified routing process. When "null" is specified for the process tag, output is displayed only for the router process that has no tag specified. If a process tag is not specified, output is displayed for all processes.

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

Example Tuning IS-IS LSP Generation

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

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

Example Tuning IS-IS Fast Flooding of LSPs

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

```
Router> enable
```

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

fast-flood 7
```

Where to Go Next

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

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

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: ISIS Command Reference*
Overview of Cisco IS-IS conceptual information with links to all the individual IS-IS modules	"Integrated IS-IS Routing Protocol Overview" module
Customizing IS-IS for fast convergence and scalability	"Overview of IS-IS Fast Convergence" module
IPv6 Routing: IS-IS Multitopology Support for IPv6	" *IPv6 Routing: IS-IS Multitopology Support for IPv6*" module

RFCs

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

Technical Assistance

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

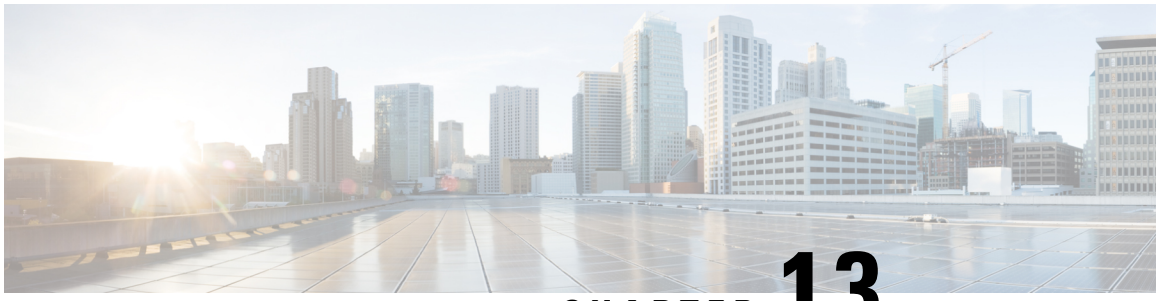
Feature Information for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

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

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

Table 11: Feature Information for Reducing Link Failure and Topology Change Notification Times in IS-IS Networks

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



CHAPTER 13

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, on page 151
- Prerequisites for IS-IS Support for Route Tags, on page 151
- Information About IS-IS Support for Route Tags, on page 152
- How to Configure IS-IS Support for Route Tags, on page 153
- Configuration Examples for IS-IS Support for Route Tags, on page 162
- Where to Go Next, on page 165
- Additional References, on page 165
- Feature Information for IS-IS Support for Route Tags, on page 166

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 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.

How to Configure IS-IS Support for Route Tags

Tagging Routes for Networks Directly Connected to an Interface

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-number*
7. **end**
8. **show isis database verbose**
9. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*]]

DETAILED STEPS

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	Sets a primary IP address for an interface.
Step 5	**ip address** *ip-address mask* **secondary** **Example:** `Device(config-if)# ip address 10.2.2.1 255.255.255.0 secondary`	(Optional) Sets a secondary IP address for an interface.
Step 6	**isis tag** *tag-number* **Example:** `Device(config-if)# isis tag 120`	Sets a tag on the IP addresses configured under this interface when those IP prefixes are put into an Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP). • The tag must be an integer.
Step 7	**end** **Example:** `Device(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.
Step 8	**show isis database verbose** **Example:** `Device# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.
Step 9	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*]] **Example:** `Device# show ip route 10.1.1.1 255.255.255.0`	(Optional) Displays the current state of the routing table. • Perform this step if you want to verify the tag.

What to Do Next

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:** `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	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** `Device(config)# route-map static-color permit 15`	Defines the conditions for redistributing routes from one routing protocol into another or from one Intermediate System-to-Intermediate System (IS-IS) level to another. • This command causes the device to enter route-map configuration mode.
Step 4	**match tag** *tag-value* [*...tag-value*] **Example:**	(Optional) Matches routes tagged with the specified tag numbers.

	Command or Action	Purpose
	`Device(config-route-map)# match tag 15`	• If you are setting a tag for the first time, you cannot match on a 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.	(Optional) See the appropriate **match** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference.* • Repeat this step for each match criterion you that want.
Step 6	**set tag** *tag-value* **Example:** `Device(config-route-map)# set tag 10`	Specifies the tag number to set.
Step 7	Set another value, depending on what else you want to do with the tagged routes.	(Optional) See the following **set** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference*. • **set level** • **set metric** • **set metric-type**
Step 8	Repeat Step 7 for each value that you want to set.	(Optional)
Step 9	Repeat Steps 3 through 8 for each route-map statement that you want.	(Optional)
Step 10	**end** **Example:** `Device(config-route-map)# end`	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 11	**show isis database verbose** **Example:** `Device# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.
Step 12	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** [*access-list-number* | *access-list-name*]] **Example:** `Device# show ip route 10.1.1.1 255.255.255.0`	(Optional) Displays the current state of the routing table. • Perform this step if you want to verify the tag.

What to Do Next

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

If a tagged route is summarized and the tag is not explicitly configured in the **summary-address** command, the tag is lost.

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-number*] [**metric** *metric-value*]
6. **end**
7. **show isis database verbose**
8. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** [*access-list-number* | *access-list-name*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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** [*area-tag*] **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. • Enters router configuration mode.
Step 4	**metric-style wide** **Example:** `Device(config-router)# metric-style wide`	Configures a device running IS-IS so that it generates and accepts type, length, values (TLV) object 135 for IP addresses.
Step 5	**summary-address** *address mask* [**level-1**	**level-1-2**	**level-2**] [**tag** *tag-number*] [**metric** *metric-value*]	Creates aggregate addresses for IS-IS.

	Command or Action	Purpose
	Example: `Device(config-router)# summary-address 192.168.0.0 255.255.0.0 tag 12345 metric 321`	
Step 6	**end** **Example:** `Device(config-router)# end`	(Optional) Exits configuration mode and returns to privileged EXEC mode.
Step 7	**show isis database verbose** **Example:** `Device# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.
Step 8	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | [**list** [*access-list-number* | *access-list-name*]] **Example:** `Device# show ip route 10.1.1.1 255.255.255.0`	(Optional) Displays the current state of the routing table. • Perform this step if you want to verify the tag.

What to Do Next

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 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 section "Tagging IS-IS Routes to Control Their Distribution."

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:** `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	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map static-color permit 15`	Defines the conditions for redistributing routes from one routing protocol into another or from one Intermediate System-to-Intermediate System (IS-IS) level to another. • This command causes the device to enter route-map configuration mode.
Step 4	**match tag** *tag-value* **Example:** `Device(config-route-map)# match tag 120`	(Optional) Applies the subsequent **set** commands to routes that match routes tagged with this tag number.
Step 5	Specify a **match** command for each match criterion that you want.	(Optional) Reference the appropriate **match** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference*.
Step 6	Set a value, depending on what you want to do with the tagged routes.	(Optional) See the following **set** commands in the *Cisco IOS IP Routing: Protocol-Independent Command Reference*. • **set level** • **set metric** • **set metric-type**
Step 7	Repeat Step 6 for each value that you want to set.	(Optional)
Step 8	Repeat Steps 3 through 7 for each route-map statement that you want.	(Optional)
Step 9	**exit** **Example:**	(Optional) Returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-route-map)# exit`	
Step 10	**router isis** **Example:** `Device(config)# router isis`	(Optional) Enables the IS-IS routing protocol, specifies an IS-IS process, and puts the device in router configuration mode.
Step 11	**metric-style wide** **Example:** `Device(config-router)# metric-style wide`	Configures a device running IS-IS so that it generates and accepts type, length, values (TLV) object 135 for IP addresses.
Step 12	**redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-tag*] **Example:** `Device(config-router)# redistribute static ip metric 2 route-map static-color`	(Optional) Redistributes routes from one routing domain into another routing domain.

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
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.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show isis database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **Example:** `Device# show isis database detail`	Displays the Intermediate System-to-Intermediate System (IS-IS) link-state database.
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. • 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 SPFs 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: 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 Intermediate System-to-Intermediate System (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.

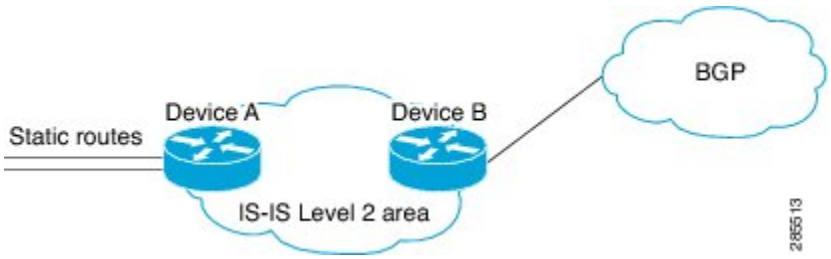
```
interface Gigabitethernet 1/0/0
 ip address 192.168.129.1 255.255.255.0
 ip router isis
 isis tag 120
interface Gigabitethernet 1/1/0
 ip address 172.16.10.5 255.255.255.0
 ip router isis
 isis tag 110
router isis
 net 49.0001.0001.0001.0001.00
 redistribute isis ip level-1 into level-2 route-map 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

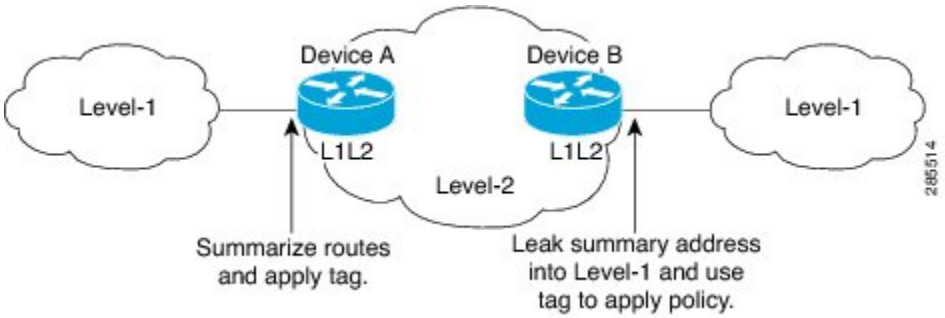
```
router bgp 100
 redistribute isis level-2 route-map tag-policy
route-map tag-policy permit 20
 match tag 10
 set metric 1000
```

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: 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 are 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 are redistributed from Level 2 into Level 1.

```
interface Gigabitethernet 1/0/0
 ip address 192.168.130.5 255.255.255.0
 ip router isis
 isis tag 60
!
interface Gigabitethernet 2/0/0
 ip address 192.168.130.15 255.255.255.0
 ip router isis
 isis tag 90
!
interface Gigabitethernet 3/0/0
 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
```

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
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*
Improving IS-IS network convergence times	• "Overview of IS-IS Fast Convergence" module in the *IP Routing: IS-IS Configuration Guide* • "Reducing Failure Detection Times in IS-IS Networks" 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

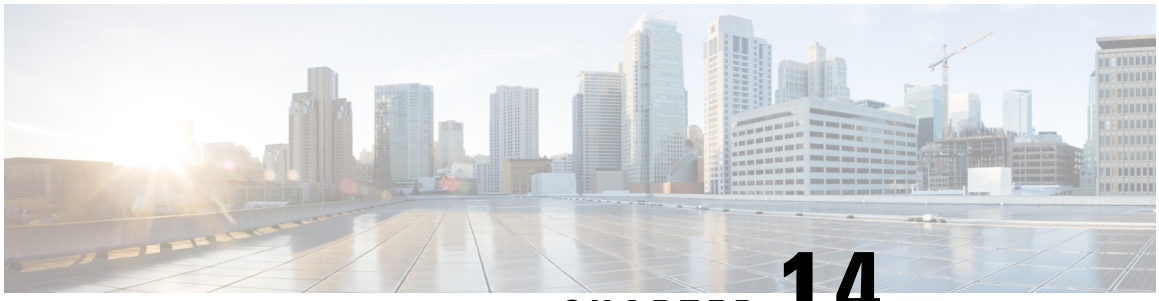
Feature Information for IS-IS Support for Route Tags

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

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

Table 12: Feature Information for IS-IS Support for Route Tags

Feature Name	Releases	Feature Information
IS-IS Support for Route Tags	Cisco IOS XE Release 3.1.0SG	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 following commands were introduced or modified: **isis tag**, **match tag**, **metric-style wide**, **router isis**, **route-map**, **set tag**, **show ip route**, **show isis database verbose**, **summary-address**.



CHAPTER 14

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, on page 167
- Prerequisites for Enhancing Security in an IS-IS Network, on page 167
- Information About Enhancing Security in an IS-IS Network, on page 168
- How to Enhance Security in an IS-IS Network, on page 170
- Configuration Examples for Enhancing Security in an IS-IS Network, on page 180
- Additional References, on page 181
- Feature Information for Enhancing Security in an IS-IS Network, on page 182

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 routers from injecting false routing information into the link-state database, or you can configure a type of IS-IS authentication--either IS-IS HMAC-MD5 or enhanced clear text authentication.

Configuring IS-IS Authentication

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

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

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

IS-IS Authentication Functionality

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

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

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

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

Benefits of IS-IS Clear Text Authentication

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

Benefits of IS-IS HMAC-MD5 Authentication

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

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

Migrating to a New Authentication Type

Before you migrate from using one type of security authentication to another, all routers must be loaded with the new image that supports the new authentication type. The routers will continue to use the original authentication method until all routers have been loaded with the new image that supports the new authentication method, and all routers have been configured to use the new authentication method. Once all routers are loaded with the required image, you must follow the configuration steps for the desired new authentication method as described in the previous Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance, on page 173. You also must decide whether to configure authentication for the IS-IS area or for individual IS-IS interfaces. Both tasks are included in the referenced section.

Migration from Old Clear Text Authentication to HMAC-MD5 Authentication

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

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

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

- Passwords are easier to change and maintain.

- Passwords can be encrypted when the system configuration is being displayed (if you use key management).

How to Enhance Security in an IS-IS Network

Setting an Authentication Password for each Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Enters interface configuration mode.
Step 4	**isis password** *password* [**level-1**| **level-2**] **Example:** `Router(config-if)# isis password sjpass level-1`	Configures the authentication password for an interface. • Different passwords can be assigned for different routing levels using the **level-1** and **level-2** keywords.

	Command or Action	Purpose
		• Specifying the **level-1** or **level-2** keyword disables the password only for Level 1 or Level 2 routing, respectively.
Step 5	Repeat Step 4 for each interface password that you want to set.	--
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show ip interface** [*type number*] [**brief**] **Example:** `Router# show ip interface serial 1`	Displays the usability status of interfaces configured for IP.

Setting a Password at Level 1

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Setting a Password at Level 2

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**router isis** [*area-tag*] **Example:** `Router(config)# router isis salesarea`	Enables IS-IS as an IP routing protocol and assigns a tag to a process, if required. • Enters router configuration mode.
Step 4	**domain-password** *password* [**authenticate snp** {**validate** | **send-only**}] **Example:** `Router(config-router)# domain-password company2`	Configures the IS-IS routing domain authentication password, preventing unauthorized routers from injecting false routing information into the link-state database. **Note** This password is inserted in Level 2 PDU link-state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs). If you specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, the IS-IS routing protocol will insert the password into sequence number PDUs (SNPs). **Note** If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, the IS-IS routing protocol does not insert the password into SNPs.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **exit**

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

DETAILED STEPS

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

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

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

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

SUMMARY STEPS

1. **enable**

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain multistate87723`	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 201`	Identifies an authentication key on a key chain. • The *key-id* argument must be a number.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string idaho`	Specifies the authentication string for a key. • The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to keychain configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-keychain)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface.
Step 9	**isis authentication send-only** [**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication send-only`	Specifies that authentication is performed only on PDUs being sent (not received) on a specified IS-IS interface.
Step 10	Repeat Steps 1 through 9 on each router that will communicate.	Use the same key string on each router.
Step 11	**isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication mode md5`	Specifies the type of authentication used for an IS-IS interface. • Specify **md5** for MD5 authentication. • Specify **text** for clear text authentication.
Step 12	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication key-chain multistate87723`	Enables MD5 authentication for an IS-IS interface.
Step 13	Repeat Steps 11 and 12 on each router that will communicate.	--
Step 14	**no isis authentication send-only** **Example:** `Router(config-if)# no isis authentication send-only`	Specifies that authentication is performed on PDUs being sent and received on a specified IS-IS interface.
Step 15	Repeat Step 14 on each router that will communicate.	--

Migrating to a New Authentication Method

SUMMARY STEPS

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

2. Configure the new authentication mode on both the interface and the IS-IS area by following the appropriate tasks in the Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time, on page 173.

DETAILED STEPS

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

Step 2 Configure the new authentication mode on both the interface and the IS-IS area by following the appropriate tasks in the Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time, on page 173.

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 201`	Identifies an authentication key on a key chain. • The *key-id* argument must be a number.
Step 5	**key-string** *text* **Example:** `Router(config-keychain-key)# key-string idaho`	Specifies the authentication string for a key. • The *text* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to keychain configuration mode.
Step 7	**exit** **Example:** `Router(config-keychain)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface ethernet 0`	Configures an interface.
Step 9	**isis authentication mode** {**md5** | **text**}[**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication mode md5`	Specifies the type of authentication used for an IS-IS interface. • Specify **md5** for MD5 authentication. • Specify **text** for clear text authentication.
Step 10	**isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**] **Example:** `Router(config-if)# isis authentication key-chain multistate87723`	Enables MD5 authentication for an IS-IS interface.

Configuration Examples for Enhancing Security in an IS-IS Network

Example Configuring IS-IS HMAC-MD5 Authentication

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

```
!
key chain cisco
 key 100
 key-string tasman-drive
!
interface Ethernet3
 ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication mode md5 level-1
 isis authentication key-chain cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 authentication key-chain cisco level-1
!
```

Example Configuring IS-IS Clear Text Authentication

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

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

Additional References

Related Documents

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

Standards

Standard	Title
None	--

RFCs

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

Technical Assistance

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

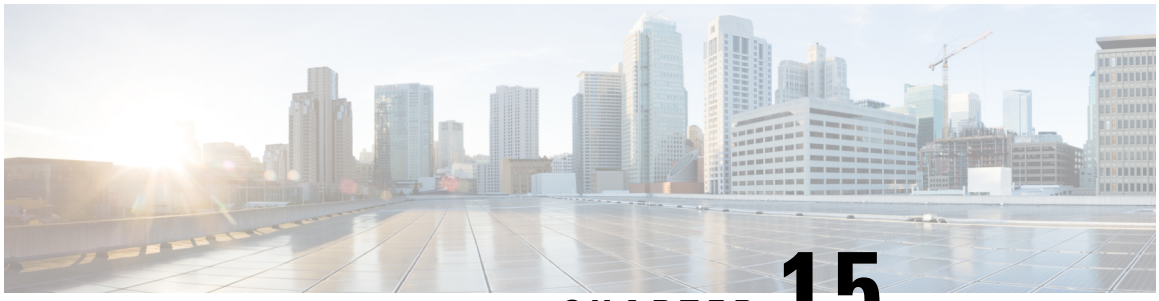
Feature Information for Enhancing Security in an IS-IS Network

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

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

Table 13: Feature Information for Enhancing Security in an IS-IS Network

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



CHAPTER 15

IS-IS IPv6 Multi-Process Support

The IS-IS IPv6 Multi-Process Support feature enables support for mutual redistribution of IPv6 routes between multiple IS-IS IPv6 instances and allows the IS-IS IPv6 instances to install routes in non-default virtual routing and forwarding (VRF) instances.

- Finding Feature Information, on page 183
- Prerequisites for IS-IS IPv6 Multi-Process Support, on page 183
- Information About IS-IS IPv6 Multi-Process Support, on page 184
- How to Configure IS-IS IPv6 Multi-Process Support, on page 184
- Configuration Examples for IS-IS IPv6 Multi-Process Support, on page 188
- Additional References for IS-IS IPv6 Multi-Process Support, on page 189
- Feature Information for IS-IS IPv6 Multi-Process Support, on page 189

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 IPv6 Multi-Process Support

- You must enable IPv6 unicast routing before ISIS IPv6 configuration.
- You must enable IPv6 on an interface, by assigning an IPv6 address to the interface or by using the **ipv6 enable** command, before associating the interface with an ISIS IPv6 instance.
- You must define a virtual routing and forwarding (VRF) and enable an IPv6 address family in the VRF before associating an ISIS IPv6 instance with that VRF.

Information About IS-IS IPv6 Multi-Process Support

IS-IS IPv6 Multi-Process Support Overview

The IS-IS IPv6 Multi-Process Support feature allows you to create up to 28 IPv6-enabled IS-IS instances and enables these IPv6 instances to be associated with any VRF and not only the default VRF. The device can redistribute IPv6 routes between multiple IPv6 IS-IS instances in the same VRF including the default VRF. The device can also redistribute routes between an IS-IS instance and other routing protocols such as RIP and OSPFv3 operating in the same VRF, including routing protocols in the default VRF.

How to Configure IS-IS IPv6 Multi-Process Support

Configuring IS-IS IPv6 Multi-Process Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family ipv6** [**unicast**]
5. **exit**
6. **exit**
7. **interface** *type number*
8. (Optional) **vrf forwarding** *vrf-name*
9. **ipv6 address** *ipv6-prefix/prefix-length*
10. **ipv6 router isis** *process-tag*
11. **exit**
12. Repeat Step 7 to Step 11 to configure IS-IS routing process and VRFs for IPv6 on different interfaces.
13. **router isis** *process-tag*
14. (Optional) **vrf** *vrf-name*
15. **net** *network-entity-title*
16. **is-type** [**level-1** | **level-1-2** | **level-2-only**]
17. **log-adjacency-changes**
18. **address-family ipv6** [**unicast**]
19. **redistribute source-protocol** [*process-id*] [**route-map** *map-tag*]
20. **redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*
21. **exit**
22. **exit**
23. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
24. **match route-type** {**level-1** | **level-2**}
25. **set metric** *metric-value*
26. **set level** {**level-1** | **level-2** | **level-1-2**}

27. **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	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition v1`	Configure a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode
Step 4	**address-family ipv6** [**unicast**] **Example:** `Device(config-vrf)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. **Note** The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the device is placed in configuration mode for the unicast IPv6 address family if the unicast keyword is not specified with the **address-family ipv6** command.
Step 5	**exit** **Example:** `Device(config-vrf-af)# exit`	Exits the address family configuration mode and enters VRF configuration mode.
Step 6	**exit** **Example:** `Device(config-vrf)# exit`	Exits the VRF configuration mode and enters global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 0/2`	Configures an interface type and enters interface configuration mode.
Step 8	(Optional) **vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding v1`	Associates a Virtual Routing and Forwarding (VRF) or a virtual network with an interface or subinterface

	Command or Action	Purpose
Step 9	**ipv6 address** *ipv6-prefix/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8::/32`	Sets an IPv6 address for an interface.
Step 10	**ipv6 router isis** *process-tag* **Example:** `Device(config-if)# ipv6 router isis v1a`	Configures an IS-IS routing process for IPv6 on an interface and attaches a tag to the routing process. **Note** The configuration of the interface-mode **ipv6 router isis** command will overwrite the prior configuration on that interface, but only if the new configuration is attempting to change the interface ownership to a different instance that is in the same VRF as the currently configured owner instance. The configuration will be rejected if the attempted change is between two instances that are associated with different VRFs.
Step 11	**exit** **Example:** `Device(config-if)# exit`	Exits the interface configuration mode and enters global configuration mode.
Step 12	Repeat Step 7 to Step 11 to configure IS-IS routing process and VRFs for IPv6 on different interfaces. **Example:**	--
Step 13	**router isis** *process-tag* **Example:** `Device(config)# router isis v1a`	Enables IS-IS for the specified IS-IS routing process, and enters router configuration mode.
Step 14	(Optional) **vrf** *vrf-name* **Example:** `Device(config-if)# vrf v1`	Associates a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface or subinterface
Step 15	**net** *network-entity-title* **Example:** `Device(config-router)# net 49.000b.0000.0001.0002.00`	Configures IS-IS network entity title (NET) for a CLNS routing process.
Step 16	**is-type** [**level-1** | **level-1-2** | **level-2-only**] **Example:** `Device(config-router)# is-type level-1`	Configures the routing level for an instance of the IS-IS routing process.

	Command or Action	Purpose
Step 17	**log-adjacency-changes** **Example:** `Device(config-router)# log-adjacency-changes`	Configure the device to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down.
Step 18	**address-family ipv6** [**unicast**] **Example:** `Device(config-router)# address-family ipv6`	Specifies the IPv6 address family, and enters address family configuration mode. **Note** The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the device is placed in configuration mode for the unicast IPv6 address family if the unicast keyword is not specified with the **address-family ipv6** command.
Step 19	**redistribute source-protocol** [*process-id*] [**route-map** *map-tag*] **Example:** `Device(config-router-af)# redistribute isis v1a route-map abc`	Specifies the route map that should be checked to filter the importation of routes from this source routing protocol to the current routing protocol.
Step 20	**redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name* **Example:** `Device(config-router-af)# redistribute isis level-1 into level-2 distribute-list xyz`	Redistributes IPv6 routes from one IS-IS level into another IS-IS level. By default, the routes learned by Level 1 instances are redistributed by the Level 2 instance.
Step 21	**exit** **Example:** `Device(config-router-af)# exit`	Exits the address family configuration mode and enters router configuration mode.
Step 22	**exit** **Example:** `Device(config-router)# exit`	Exits the router configuration mode and enters global configuration mode.
Step 23	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map abc permit 10`	Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another and enters route-map configuration mode.
Step 24	**match route-type** {**level-1** | **level-2**} **Example:** `Device(config-route-map)# match route-type level-1`	Defines the route-type match criterion.

	Command or Action	Purpose
Step 25	**set metric** *metric-value* **Example:** `Device(config-route-map)# set metric 56`	Configures the metric value used to redistribute routes.
Step 26	**set level** {**level-1** | **level-2** | **level-1-2**} **Example:** `Device(config-route-map)# set level level-2`	Specifies the routing level of routes to be advertised into a specified area of the routing domain.
Step 27	**end** **Example:** `Device(config-route-map)# end`	Exits the route-map configuration mode and enters privileged EXEC mode.

Configuration Examples for IS-IS IPv6 Multi-Process Support

Example: IS-IS IPv6 Multi-Process Support Configuration

```
Device> enable
Device# configure terminal
Device(config)# vrf definition v1
Device(config-vrf)# address-family ipv6
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# interface FastEthernet 0/2
Device(config-if)# ipv6 address 2001:DB8::/32
Device(config-if)# vrf forwarding v1
Device(config-if)# ipv6 router isis v1a
Device(config-if)# exit
Device(config)# interface FastEthernet 0/3
Device(config-if)# ipv6 address 2001:DB8::/48
Device(config-if)# vrf forwarding v1
Device(config-if)# ipv6 router isis v1b
Device(config-if)# exit
Device(config)# router isis v1a
Device(config-router)# vrf v1
Device(config-router)# net 49.000b.0000.0001.0002.00
Device(config-router)# is-type level-1
Device(config-router)# log-adjacency-changes
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute isis v1b route-map abc
Device(config-router-af)# redistribute isis level-1 into level-2 distribute-list xyz
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# router isis v1b
Device(config-router)# vrf v1
Device(config-router)# net 49.000b.0000.000a.0001.00
Device(config-router)# log-adjacency-changes
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute isis v1a route-map abc
```

```
Device(config-router-af)# exit
Device(config-router)# exit
Device(config)# route-map abc permit 10
Device(config-route-map)# match route-type level-1
Device(config-route-map)# set metric 56
Device(config-route-map)# set level level-2
```

Additional References for IS-IS IPv6 Multi-Process Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*

Technical Assistance

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

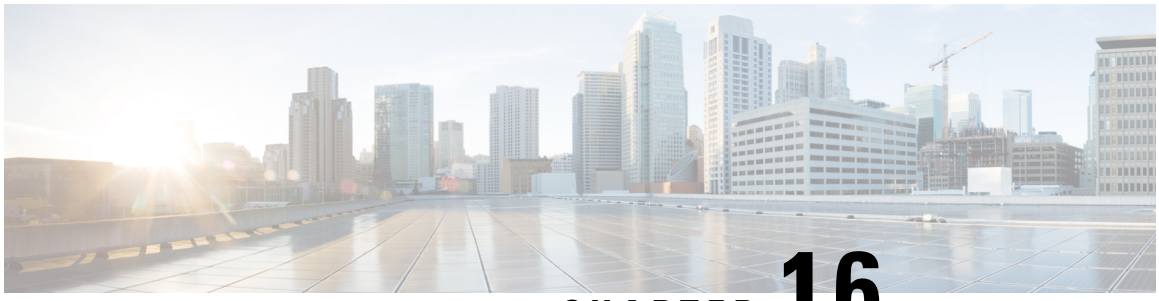
Feature Information for IS-IS IPv6 Multi-Process Support

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14: Feature Information for IS-IS IPv6 Multi-Process Support

Feature Name	Releases	Feature Information
IS-IS IPv6 Multi-Process Support	15.5(2)T	The IS-IS IPv6 Multi-Process Support feature enables support for mutual redistribution of IPv6 routes between multiple IS-IS IPv6 instances and allows the IS-IS IPv6 instances to install routes in non-default virtual routing and forwarding (VRF) instances. No new commands were introduced or modified.



CHAPTER 16

IS-IS IPv6 Administrative Tag

The IS-IS IPv6 Administrative Tag feature allows you to assign a tag to IPv6 prefixes that you can use to apply administrative policies with a route map. For example, you can control routes redistributed between area and domain boundaries and between different routing protocols, or apply policies on Intermediate System-to-Intermediate System (IS-IS) routes.

- Finding Feature Information, on page 191
- Information About IS-IS IPv6 Administrative Tag, on page 191
- How to Configure an IS-IS IPv6 Administrative Tag, on page 192
- Configuration Examples for IS-IS IPv6 Administrative Tag, on page 200
- Additional References, on page 202
- Feature Information for IS-IS IPv6 Administrative Tag, on page 203

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.

Information About IS-IS IPv6 Administrative Tag

IS-IS Administrative Tags in IPv6 Prefixes

You can configure an IS-IS administrative tag value for IPv6 prefixes. You can then specify the tag value of IPv6 prefixes that IS-IS inserts into the link-state protocol data units (PDUs) it generates and those that it retrieves from LSPs.

How to Configure an IS-IS IPv6 Administrative Tag

Assigning a Tag to an IS-IS IPv6 Prefix

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **net** *net1*
5. **metric-style wide**
6. **interface** [*type number*]
7. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **ipv6 router isis** [*area-tag*]
9. **isis ipv6 tag** *tag-value*
10. **end**
11. **show isis database verbose**

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** [*area-tag*] **Example:** `Device(config)# router isis tag13`	Enables the IS-IS routing protocol, specifies an IS-IS process, and enters router configuration mode.
Step 4	**net** *net1* **Example:** `Device(config-router)# net 49.0000.0000.0100.00`	Configures an IS-IS network entity table (NET) for the routing process.
Step 5	**metric-style wide** **Example:** `Device(config-router)# metric-style wide`	Configures a router running IS-IS so that it generates and accepts only new-style type, length, value objects (TLVs).

	Command or Action	Purpose
Step 6	**interface** [*type number*] **Example:** `Device(config-router)# interface GigabitEthernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 7	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **Example:** `Device(config-if)# ipv6 address 2005::1/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 8	**ipv6 router isis** [*area-tag*] **Example:** `Device(config-if)# ipv6 router isis area1`	Configures an IS-IS routing process for IPv6 on an interface and attaches an area designator to the routing process.
Step 9	**isis ipv6 tag** *tag-value* **Example:** `Device(config-if)# isis ipv6 tag 200`	Configures an administrative tag value that will be associated with an IPv6 address prefix and applied to an IS-IS LSP.
Step 10	**end** **Example:** `Device(config-if)# end`	(Optional) Saves configuration commands to the running configuration file and returns to privileged EXEC mode.
Step 11	**show isis database verbose** **Example:** `Device# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Enter this command if you want to verify the tag.

Assigning a High Priority Administrative Tag to an IS-IS IPv6 Prefix

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **address-family ipv6**
5. **ipv6 route priority high tag** *tag-value*
6. **exit**
7. **exit**

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** [*area-tag*] **Example:** `Device(config)# router isis`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 4	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode.
Step 5	**ipv6 route priority high tag** *tag-value* **Example:** `Device(config-router-af)# ipv6 route priority high tag 200`	Assigns a high priority tag to an IS-IS IPv6 prefix.
Step 6	**exit** **Example:** `Device(config-router-af)# exit`	(Optional) Exits address family configuration mode, and returns to router configuration mode.
Step 7	**exit** **Example:** `Device(config-router)# exit`	(Optional) Exits router configuration mode, and returns to global configuration mode.

Using an IS-IS IPv6 Administrative Tag to Redistribute Routes

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **address-family ipv6**

5. **redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} [**distribute-list** *list-name*] [**route-map** *map-tag*]
6. **exit**
7. **exit**
8. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
9. **match tag** *tag-value* [*...tag-value*]
10. **exit**

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** [*area-tag*] **Example:** `Device(config)# router isis`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 4	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode.
Step 5	**redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} [**distribute-list** *list-name*] [**route-map** *map-tag*] **Example:** `Device(config-router-af)# redistribute isis level-1 into level-2 route-map IPV6-PERMIT-TAG`	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.
Step 6	**exit** **Example:** `Device(config-router-af)# exit`	(Optional) Exits address family configuration mode, and returns to router configuration mode.
Step 7	**exit** **Example:** `Device(config-router)# exit`	(Optional) Exits router configuration mode, and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map match-tag`	Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another. • This command causes the router to enter route-map configuration mode.
Step 9	**match tag** *tag-value* [*...tag-value*] **Example:** `Device(config-route-map)# match tag 100`	Matches routes tagged with the specified tag numbers. • If you are setting a tag for the first time, you cannot match on tag; this step is an option if you are changing tags.
Step 10	**exit** **Example:** `Device(config-route-map)# exit`	(Optional) Exits route-map configuration mode, and returns to global configuration mode.

Using an IS-IS IPv6 Administrative Tag to Configure Routes

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]
4. **router isis** [*area-tag*]
5. **address-family ipv6**
6. **redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} [**distribute-list** *list-name*] [**route-map** *map-tag*
7. **exit**
8. **exit**
9. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
10. **set tag** *tag-value*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables 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	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **Example:** `Router(config)# ipv6 route 2033::1/64 GigabitEthernet 0/0/0`	Establishes a static IPv6 routes.
Step 4	**router isis** [*area-tag*] **Example:** `Device(config)# router isis`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 5	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode.
Step 6	**redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} [**distribute-list** *list-name*] [**route-map** *map-tag* **Example:** `Device(config-router-af)# redistribute isis level-1 into level-2 route-map IPV6-PERMIT-TAG`	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.
Step 7	**exit** **Example:** `Device(config-router-af)# exit`	(Optional) Exits address family configuration mode, and returns to router configuration mode.
Step 8	**exit** **Example:** `Device(config-router)# exit`	(Optional) Exits router configuration mode, and returns to global configuration mode.
Step 9	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map set-tag`	Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another.

	Command or Action	Purpose
		• This command causes the router to enter route-map configuration mode.
Step 10	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 300`	Sets a tag value of the destination routing protocol.
Step 11	**exit** **Example:** `Device(config-route-map)# exit`	(Optional) Exits route-map configuration mode, and returns to global configuration mode.

Applying an IS-IS IPv6 Tag to a Summary Prefix

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **address-family ipv6**
5. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix / prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]
6. **exit**
7. **exit**
8. **router isis** [*area-tag*]
9. **address-family ipv6**
10. **redistribute isis** [*process-id*] {**level-1**| **level-2**} **into** {**level-1** |**level-2**} **distribute-list** *list-name*
11. **summary-prefix** *ipv6-prefix/ prefix-length* {**level-1** | **level-1-2**| **level-2**} **tag** *tag-value*
12. **end**
13. **show isis database verbose**

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**router isis** [*area-tag*] **Example:** `Device(config)# router isis`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 4	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode.
Step 5	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix* / *prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **Example:** `Device(config-router-af)# ipv6 route 11:1:1:1:1:1::/96 GigabitEthernet 0/0/0`	Establishes a static IPv6 routes.
Step 6	**exit** **Example:** `Device(config-router-af)# exit`	(Optional) Exits address family configuration mode, and returns to router configuration mode.
Step 7	**exit** **Example:** `Device(config-router)# exit`	(Optional) Exits router configuration mode, and returns to global configuration mode.
Step 8	**router isis** [*area-tag*] **Example:** `Device(config)# router isis`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 9	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode.
Step 10	**redistribute isis** [*process-id*] {**level-1**| **level-2**} **into** {**level-1** |**level-2**} **distribute-list** *list-name* **Example:**	Redistributes IPv6 routes from one routing domain into another routing domain using IS-IS as both the target and source protocol.

	Command or Action	Purpose
	`Device(config-router-af)# redistribute static level-2 metric 50`	
Step 11	**summary-prefix** *ipv6-prefix/ prefix-length* {**level-1** | **level-1-2**| **level-2**} **tag** *tag-value* **Example:** `Device(config-router-af)# summary-prefix 11:1:1:1::/64 tag 600`	Allows a Level 1-2 router to summarize Level 1 prefixes at Level 2, instead of advertising the Level 1 prefixes directly when the router advertises the summary. • The *ipv6-prefix* argument in the **summary-prefix** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. • The *prefix-length* argument is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Step 12	**end** **Example:** `Device(config-router-af)# end`	(Optional) Saves configuration commands to the running configuration file and returns to privileged EXEC mode.
Step 13	**show isis database verbose** **Example:** `Device# show isis database verbose`	(Optional) Displays details about the IS-IS link-state database, including the route tag. • Perform this step if you want to verify the tag.

Configuration Examples for IS-IS IPv6 Administrative Tag

Example: Assigning a Tag to an IS-IS IPv6 Prefix

```
Device(config)# router isis
Device(config-router)# net 49.0000.0000.0100.00
Device(config-router)# metric-style wide
Device(config-router)# interface GigabitEthernet 0/0/0
Device(config-if)# ipv6 address 2005::1/64
Device(config-if)# ipv6 router isis
Device(config-if)# isis ipv6 tag 200
Device(config-if)# end
Device# show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
Device.00-00        * 0x00000001   0xD27D        1189              0/0/0
  Area Address: 49
  NLPID:        0x8E
  Hostname: Device
```

```
  IPv6 Address: 2005::1
  Metric: 10         IPv6 2005::/64
    Route Admin Tag: 200
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
Device.00-00     * 0x00000001   0xD27D        1189              0/0/0
  Area Address: 49
  NLPID:        0x8E
  Hostname: Device
  IPv6 Address: 2005::1
  Metric: 10         IPv6 2005::/64
    Route Admin Tag: 200
```

Example: Assigning a High Priority Administrative Tag to an IS-IS IPv6 Prefix

```
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# ipv6 route priority high tag 200
```

Example: Using an IS-IS IPv6 Administrative Tag to Redistribute Routes

```
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute isis level-1 into level-2 route-map match-tag
Device(config-router-af)# route-map match-tag
Device(config-route-map)# match tag 100
```

Example: Using an IS-IS IPv6 Administrative Tag to Configure Routes

```
Device(config)# ipv6 route 2033::1/64 GigabitEthernet 0/0/0
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute static level-2 route-map set-tag
Device(config-router-af)# route-map set-tag
Device(config-route-map)# set tag 300
Device(config-route-map)# end
Device# show isis database verbose level-2

Device.00-00     * 0x0000004E   0x9805        1197              0/0/0
  Area Address: 33
  NLPID:        0xCC 0x8E
  Hostname: Device
  IP Address:   10.100.100.20
  IPv6 Address: 2001:DB8::100
  IPv6 Address: 2001:DB8::200
  Metric: 10         IS-Extended route500.01
  Metric: 10         IP 10.100.100.0/24
  Metric: 10         IPv6 2001:DB8::/64
```

```
  Metric: 10         IPv6 2001:DB8::/64
  Metric: 10         IPv6-Interarea 11:1:1:1:1:1:1:1/128
  Metric: 20         IPv6-Interarea 2003:DB8::/64
  Metric: 0          IPv6 2033::/64
    Route Admin Tag: 300
```

Example: Applying an IS-IS IPv6 Administrative Tag to a Summary Prefix

```
Device(config)# router isis
Device(config)# ipv6 route 11:1:1:1:1:1::/96 GigabitEthernet 0/0/0
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute static level-2 metric 50
Device(config-router-af)# summary-prefix 11:1:1:1::/64 tag 600
Device(config-route-map)# end
Device# show isis database verbose level-2

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
Device.00-00     * 0x00000007   0x4AA7        1174              0/0/0
  Area Address: 33
  NLPID:        0xCC 0x8E
  Hostname: Device
  IP Address:   10.100.100.20
  IPv6 Address: 2001:DB8::100
  IPv6 Address: 2001:DB8::200
  Metric: 10         IS-Extended route500.01
  Metric: 10         IP 10.100.100.0/24
  Metric: 10         IPv6 2001:DB8::/64
  Metric: 10         IPv6 2001:DB8::/64
  Metric: 10         IPv6 11:1:1:1::/64
    Route Admin Tag: 600
(Summary route 11:1:1:1::/64 is advertised with tag 600)
Device(config-router-af)#
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
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*

Standards and RFCs

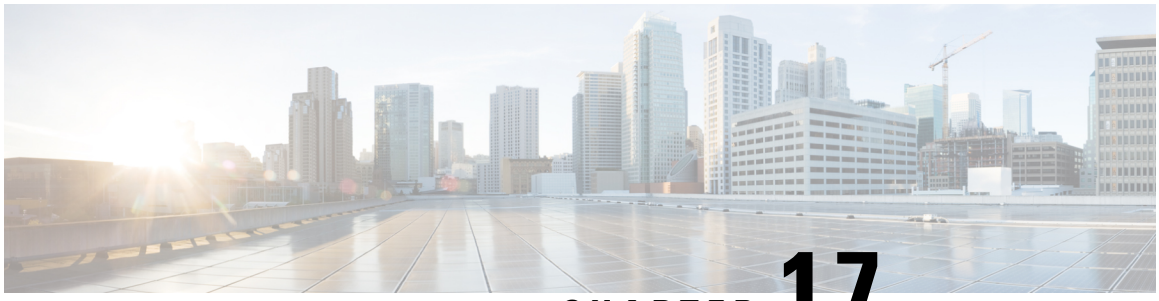
Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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 IPv6 Administrative Tag

Feature Name	Releases	Feature Information
IS-IS IPv6 Administrative Tag	15.2(4)M 15.2(4)S 15.2(1)SY	Allows you to assign a tag to IPv6 prefixes that you can use to apply administrative policy with a route map. The following commands were introduced or modified: **ipv6 route priority high**, **isis ipv6 tag**, **redistribute isis (ipv6)**, **show isis database verbose**, **summary-prefix (ipv6 IS-IS)**.



CHAPTER 17

IS-IS IPv6 Advertise Passive Only

The IS-IS IPv6 Advertise Passive Only feature allows you to configure the Intermediate System-to-Intermediate System (IS-IS) instance on a device to advertise only IPv6 prefixes that belong to passive interfaces and exclude other connected IPv6 prefixes.

- Finding Feature Information, on page 205
- Prerequisites for IS-IS IPv6 Advertise Passive Only, on page 205
- Information About IS-IS IPv6 Advertise Passive Only, on page 206
- How to Configure IS-IS IPv6 Advertise Passive Only, on page 206
- Configuration Examples for IS-IS IPv6 Advertise Passive Only, on page 208
- Additional References, on page 209
- Feature Information for IS-IS IPv6 Advertise Passive Only, on page 210

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 IPv6 Advertise Passive Only

Before you can use the IS-IS IPv6 Advertise Passive Only feature to exclude IPv6 prefixes of connected networks from IS-IS link-state protocol (LSP) data unit advertisements, the integrated IS-IS routing protocol must be configured. See the “Configuring a Basic IS-IS Network” section of the *IP Routing: ISIS Configuration Guide*.

Information About IS-IS IPv6 Advertise Passive Only

IPv6 Prefixes Only Allowed on Passive Interfaces

You can configure the IS-IS instance on a device to allow only IPv6 prefixes that belong to passive interfaces in its LSP advertisements. This configuration reduces the number of IPv6 prefixes carried in the LSP advertisement.

How to Configure IS-IS IPv6 Advertise Passive Only

Configuring IS-IS Instances on a Device to Advertise Passive Interface IPv6 Prefixes Only

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **net** *net1*
5. **interface loopback** *number*
6. **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
7. **exit**
8. **interface** *type number*
9. **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
10. **ipv6 router isis** [*area-tag*]
11. **exit**
12. **router isis** [*area-tag*]
13. **passive-interface** [**default**] *type number*
14. **address-family ipv6**
15. **advertise passive-only**
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables 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	**router isis** [*area-tag*] **Example:** `Device(config)# router isis area1`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 4	**net** *net1* **Example:** `Device(config-router)# net 47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00`	Configures an IS-IS network entity table (NET) for the routing process.
Step 5	**interface loopback** *number* **Example:** `Device(config-router)# interface loopback 0`	Configures a loopback interface and enters interface configuration mode.
Step 6	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:688:1001:1000::1/128`	Sets a primary IPv6 address for an interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 9	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:688:1001:100A::1/64`	Configures an IPv6 address for the interface.
Step 10	**ipv6 router isis** [*area-tag*] **Example:** `Device(config-if)# ipv6 router isis area1`	Configures an IS-IS routing process for IPv6 on an interface, attaches an area designator to the routing process, and enters router configuration mode.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 12	**router isis** [*area-tag*] **Example:** `Device(config)# router isis area1`	Configures an IS-IS routing process for IP on an interface, attaches an area designator to the routing process, and enters router configuration mode.
Step 13	**passive-interface** [**default**] *type number* **Example:** `Device(config-router)# passive-interface loopback 0`	Disables sending routing updates on an interface.
Step 14	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enters address family configuration mode.
Step 15	**advertise passive-only** **Example:** `Device(config-router-af)# advertise passive-only`	Configures IS-IS to advertise only IPv6 prefixes that belong to passive interfaces.
Step 16	**end** **Example:** `Device(config-router-af)# end`	(Optional) Saves the configuration commands to the running configuration file and returns to privileged EXEC mode.

Configuration Examples for IS-IS IPv6 Advertise Passive Only

Example: Configuring IS-IS Instances on a Device to Advertise Only Passive Interfaces

```
Device> enable
Device# configure terminal
Device(config)# router isis area1
Device(config-router)# net 47.0010.0000.0000.0000.0001.0001.1111.1111.1111.00
Device(config-router)# interface loopback 0
Device(config-if)# ipv6 address 2001:688:1001:1000::1/128
Device(config-if)# exit
Device(config)# interface Ethernet 0/0
```

```
Device(config-if)# ipv6 address 2001:688:1001:100A::1/64
Device(config-if)# ipv6 router isis area1
Device(config-if)# exit
Device(config)# router isis area1
Device(config-router)# passive-interface loopback 0
Device(config-router)# address-family ipv6
Device(config-router-af)# advertise passive-only
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
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*
IS-IS commands	*Cisco IOS IS-IS Command Reference*
Configuring the integrated IS-IS routing protocol	"Configuring a Basic IS-IS Network" module of the *IP Routing: ISIS Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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

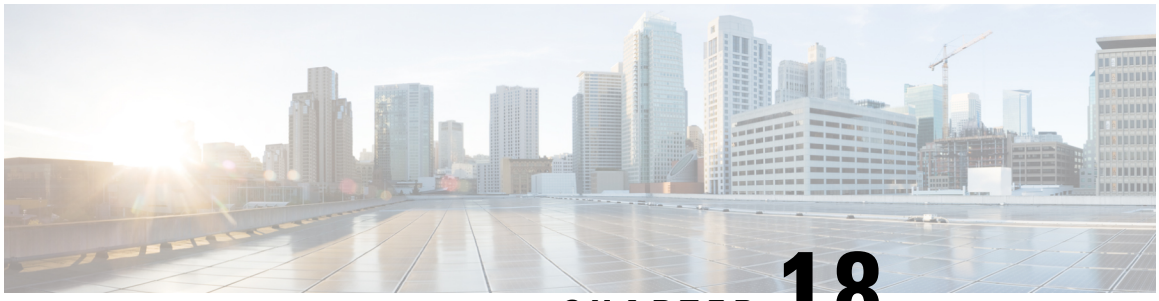
Feature Information for IS-IS IPv6 Advertise Passive Only

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

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

Table 15: Feature Information for IS-IS IPv6 Advertise Passive Only

Feature Name	Releases	Feature Information
IS-IS IPv6 Advertise Passive Only	15.2(4)M Cisco IOS XE Release 3.6S	Allows you to configure the IS-IS instance on a device to advertise only IPv6 prefixes that belong to passive interfaces and exclude other connected IPv6 prefixes. The following command was introduced or modified: **advertise passive-only (IPv6)**.



CHAPTER 18

IS-IS Inbound Filtering

The Intermediate System-to-Intermediate System (IS-IS) Inbound Filtering feature prevents unwanted IS-IS routes from being installed in a routing table. A user can deny or permit a route from being installed in a routing table using the feature in combination with access lists, prefix lists, route maps, or gateways.

- Finding Feature Information, on page 211
- Prerequisites for IS-IS Inbound Filtering, on page 211
- Information About IS-IS Inbound Filtering, on page 211
- How to Configure IS-IS Inbound Filtering, on page 212
- Configuration Examples for IS-IS Inbound Filtering, on page 218
- Verifying IS-IS Inbound Filtering, on page 220
- Additional References, on page 221
- Feature Information for IS-IS Inbound Filtering, on page 221

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 Inbound Filtering

IS-IS must be configured on the network.

Information About IS-IS Inbound Filtering

You can deny or permit Intermediate System-to-Intermediate System (IS-IS) routes from being installed in the routing table.

Devices configured with IS-IS run Shortest Path First (SPF) on the routes received through link-state packet (LSP) updates and install updated routes in a routing table. You can configure access lists, prefix lists, gateways, or route maps with permit or deny rules and apply these to the routing table using the **distribute-list** command.

The distribution list can be applied globally or to routes using a specific interface as the outgoing interface.

Filtering Based on a Route Tag

Users can assign tags to external routes when they are redistributed to IS-IS routes. Then, the user can deny or permit those routes in the IS-IS domain by identifying that tag in the **route-map** and **distribute-list in** commands.

In the route map, you can create rules for specific route attributes that are defined using the match command. The match options are as follows:

- **match interface**
- **match ip address**
- **match ip next-hop**
- **match ip route-source**
- **match metric**
- **match route-type**
- **match tag**

One application of filtering based on route tags is on Autonomous System Boundary Routers (ASBRs), where users can tag prefixes when they are distributed on the ASBRs, and later use the tags to filter the prefixes and prevent them from getting installed on the routing table of other external devices.

Filtering Based on an Interface

When a match is done on the interface, the interface represents the outgoing interface of the route that IS-IS is trying to install in the routing table.

Filtering Based on Next Hop/Source of Updates

When a match is done on the next hop, the next hop represents the next-hop IP address of the route that IS-IS is trying to install in the routing table. You can thus filter routes based on the source of the updates.

How to Configure IS-IS Inbound Filtering

Configuring Route Filtering by Route Destination Using an Access List

Perform this task to filter a route by route destination. An access list is defined to permit or deny a destination IP address and this access list is applied to the routing table.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} **ip any** *destination-address destination-wildcard*
4. **interface** *type number*
5. **ip router isis** *route-tag*
6. **router isis** *route-tag*
7. **distribute-list** *access-list-number* **in** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**permit** | **deny**} **ip any** *destination-address destination-wildcard* **Example:** `Device(config)# access-list 101 deny ip any 198.51.100.15 0.0.0.63`	Defines an access list permitting or denying an IP address or a subnet. • 1 in the source-wildcard indicates that the corresponding position in the source-address need not be considered.
Step 4	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 5	**ip router isis** *route-tag* **Example:** `Device(config-if)# ip router isis 121`	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
Step 6	**router isis** *route-tag* **Example:** `Device(config-if)# router isis 121`	Enables an Intermediate System-to-Intermediate System (IS-IS) routing protocol and enters router configuration mode.
Step 7	**distribute-list** *access-list-number* **in** [*interface-type interface-number*] **Example:** `Device(config-router)# distribute-list 101 in`	Filters the routing table based on the access list.

Configuring Route Filtering by Next Hop (or Route Source)

Perform this task to filter a route by the next-hop IP address of the route (source of routing updates). A prefix list is defined to permit or deny a next-hop IP address and applied to the routing table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *prefix-list-name* [**seq** *number*] {**permit** | **deny**} *network/length* [**ge** *ge-length*] [**le** *le-length*]
4. **interface** *type number*
5. **ip router isis** *route-tag*
6. **router isis** *route-tag*
7. **distribute-list gateway** *prefix-list-name* **in** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** *prefix-list-name* [**seq** *number*] {**permit** | **deny**} *network/length* [**ge** *ge-length*] [**le** *le-length*] **Example:** `Device(config)# ip prefix-list List2 seq 5 deny 198.51.100.21/24`	Defines a prefix list permitting or denying an IP address or a subnet. • The optional **ge** keyword represents the greater than or equal to operator. • The optional **le** keyword represents the lesser than or equal to operator.
Step 4	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 5	**ip router isis** *route-tag* **Example:** `Device(config-if)# ip router isis 125`	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
Step 6	**router isis** *route-tag* **Example:** `Device(config-if)# router isis 125`	Enables an IS-IS routing protocol and enters router configuration mode.
Step 7	**distribute-list gateway** *prefix-list-name* **in** [*interface-type interface-number*] **Example:** `Device(config-router)# distribute-list gateway List2 in`	Filters the routing table based on the next hop (or route source).

Configuring Route Filtering by Route Destination Using a Prefix List

Perform this task to filter a route by route destination. A prefix list is defined to permit or deny a destination IP address and applied to the routing table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *prefix-list-name* [**seq** *number*] {**permit** | **deny**} *network/length* [**ge** *ge-length*] [**le** *le-length*]
4. **interface** *type number*
5. **ip router isis** *route-tag*
6. **router isis** *route-tag*
7. **distribute-list prefix** *prefix-list-name* **in** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** *prefix-list-name* [**seq** *number*] {**permit** | **deny**} *network/length* [**ge** *ge-length*] [**le** *le-length*] **Example:** `Device(config)# ip prefix-list List1 seq 5 deny 198.51.100.23/24`	Defines a prefix list permitting or denying an IP address or a subnet. • The optional **ge** keyword represents the greater than or equal to operator. • The optional **le** keyword represents the lesser than or equal to operator.
Step 4	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 5	**ip router isis** *route-tag* **Example:** `Device(config-if)# ip router isis 122`	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
Step 6	**router isis** *route-tag* **Example:** `Device(config-if)# router isis 122`	Enables an IS-IS routing protocol and enters router configuration mode.

	Command or Action	Purpose
Step 7	**distribute-list prefix** *prefix-list-name* **in** [*interface-type interface-number*] **Example:** `Device(config-router)# distribute-list prefix List1 in`	Filters the routing table based on the prefix list.

Configuring Route Filtering Using Tags

Perform this task to filter a route using route tags. A route map is defined to permit or deny a route tag and applied to the routing table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *route-map-name* [**permit** | **deny**] *sequence-number*
4. **match tag** *tag-value*
5. **exit**
6. **interface** *type number*
7. **ip router isis** *route-tag*
8. **router isis** *route-tag*
9. **distribute-list route-map** *route-map-name* **in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *route-map-name* [**permit**	**deny**] *sequence-number* **Example:** `Device(config)# route-map Map1 deny 10`	Creates a route map, associates a permit or deny condition with it, and enters route-map configuration mode
Step 4	**match tag** *tag-value* **Example:** `Device(config-route-map)# match tag 200`	Associates a match tag rule with the route map and matches routes with a specified name to be used as the route map is referenced. • At least one **match** command is required, but it need not be this **match** command. This is just an example.

	Command or Action	Purpose
		• The list of **match** commands available to be used in this type of route map appears on the **distribute-list in** command reference page. • This type of route map will have no **set** commands.
Step 5	**exit** **Example:** `Device(config-route-map)# exit`	Enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 7	**ip router isis** *route-tag* **Example:** `Device(config-if)# ip router isis 150`	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
Step 8	**router isis** *route-tag* **Example:** `Device(config-if)# router isis 150`	Enables an IS-IS routing protocol and enters router configuration mode.
Step 9	**distribute-list route-map** *route-map-name* **in** **Example:** `Device(config-router)# distribute-list route-map Map1 in`	Filters the routing table based on the route tags specified in the route map.

Configuring Route Filtering by IPv6 Route Destination Using a Prefix List

Perform this task to filter a route by IPv6 route destination. A prefix list is defined to permit or deny a destination IPv6 address and applied to the routing table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 prefix-list** *prefix-list-name* [**seq** *number*] {**permit** | **deny**} *network/length* [**ge** *ge-length*] [**le** *le-length*]
4. **router isis**
5. **address-family ipv6**
6. **distribute-list prefix-list** *prefix-list-name* **in** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 prefix-list** *prefix-list-name* [**seq** *number*] {**permit** | **deny**} *network/length* [**ge** *ge-length*] [**le** *le-length*] **Example:** `Device(config)# ipv6 prefix-list 101 seq 5 deny 2001:DB8::/32`	Defines a prefix list permitting or denying an IPv6 address or a subnet. • The optional **ge** keyword represents the greater than or equal to operator. • The optional **le** keyword represents the lesser than or equal to operator.
Step 4	**router isis** **Example:** `Device(config)# router isis`	Enters router configuration mode.
Step 5	**address-family ipv6** **Example:** `Device(config-router)# address-family ipv6`	Enables configuration of IS-IS routing sessions for IPv6 address prefixes and enters address family configuration mode.
Step 6	**distribute-list prefix-list** *prefix-list-name* **in** [*interface-type interface-number*] **Example:** `Device(config-router-af)# distribute-list prefix-list 101 in`	Filters the routing table based on the prefix list.

Configuration Examples for IS-IS Inbound Filtering

Example: Configuring Route Filtering by Route Destination Using an Access List

The following example shows how to filter three routes from the routing table using a specified access list:

```
Device(config)# access-list 101 deny ip any 192.168.4.0 0.0.0.127
Device(config)# access-list 101 deny ip any 192.168.4.128 0.0.0.63
Device(config)# access-list 101 deny ip any 192.168.4.192 0.0.0.63
Device(config)# interface fastethernet 0/0
```

```
Device(config-if)# ip router isis 121
Device(config-if)# router isis 121
Device(config-router)# distribute-list 101 in
```

Example: Configuring Route Filtering by Next Hop (or Route Source)

The following example shows how to enable IS-IS inbound filtering using next hop or a route source:

```
Device(config)# ip prefix-list List2 seq 5 deny 198.51.100.31/24
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 125
Device(config-if)# router isis 125
Device(config-router)# distribute-list gateway List2 in
```

Example: Configuring Route Filtering by Route Destination Using a Prefix List

The following example shows how to filter three routes from a routing table using a prefix list.

```
Device(config)# ip prefix-list List1 seq 3 deny 192.0.2.1/24
Device(config)# ip prefix-list List1 seq 5 deny 192.168.4.0/24 ge 25 le 26
Device(config)# ip prefix-list List1 seq 10 permit 0.0.0.0/le 32
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 122
Device(config-if)# router isis 122
Device(config-router)# distribute-list prefix List1 in
```

Example: Configuring Route Filtering Using Tags

The following example shows how to enable IS-IS inbound filtering using a route map:

```
Device(config)# route-map Map1 deny 10
Device(config-route-map)# match tag 200
Device(config-route-map)# exit
Device(config)# interface fastethernet 0/0
Device(config-if)# ip router isis 150
Device(config-if)# router isis 150
Device(config-router)# distribute-list route-map Map1 in
```

Example: Configuring Route Filtering by IPv6 Route Destination Using a Prefix List

The following example shows how to enable IS-IS inbound filtering for routes that use standard IPv6 address prefixes:

```
Device(config)# ipv6 prefix-list 101 seq 5 deny 2001:DB8::/32
Device(config)# ipv6 prefix-list 102 seq 4 permit 2001:DB8::1/48 le 56
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# distribute-list prefix-list 101 in
Device(config-router-af)# distribute-list prefix-list 102 in ethernet 0/0
```

Verifying IS-IS Inbound Filtering

Perform this task to display the local Intermediate System-to-Intermediate System (IS-IS) routing information base (RIB). The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show isis ip rib**
3. **show isis ipv6 rib**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show isis ip rib

Displays the IPv4 local RIB.

Example:

```
Device# show isis ip rib

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x0) =================

1.1.1.1/32
  [115/L2/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[3/3]
  [115/L2/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[3/3]

2.2.2.2/32
  [115/L1/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[4/2] -
  [115/L1/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[4/2] -
  [115/L2/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[3/3] -
  [115/L2/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[3/3] -

20.20.20.0/24
  [115/L1/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[4/2]
  [115/L1/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[4/2]
  [115/L2/20] via 30.30.30.20(Serial3/0), from 2.2.2.2, tag 0, LSP[3/3]
  [115/L2/20] via 100.100.100.20(Ethernet0/0), from 2.2.2.2, tag 0, LSP[3/3]
```

Step 3 show isis ipv6 rib

Displays the IPv6 local RIB.

Example:

```
Device# show isis ipv6 rib

IS-IS IPv6 process , local RIB
  11::1/128
```

```
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
  20::/64
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2]
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
* 22::2/128
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2] -
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3] -
  2001:DB8::/64
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L1  metric 20 tag 0 LSP [4/2]
    via FE80::A8BB:CCFF:FE00:C800/Ethernet0/0, type L2  metric 20 tag 0 LSP [3/3]
```

Additional References

Related Documents

Related Topic	Document Title
IS-IS commands	Cisco IOS IP Routing: IS-IS Command Reference
Cisco IOS Commands	Cisco IOS Master Command List, All Releases

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 Inbound Filtering

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

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

Table 16: Feature Information for IS-IS Inbound Filtering

Feature Name	Releases	Feature Information
IS-IS Inbound Filterng	15.3(3)M	The Intermediate System-to-Intermediate System (IS-IS) Inbound Filtering feature allows users to define a route map to permit or deny IS-IS routes from being added to a routing table. You can configure access lists, prefix lists, gateways, or route maps with permit or deny rules, and apply these to the routing table using the **distribute-list** command. The following command was modified: **distribute-list in (IP)**.