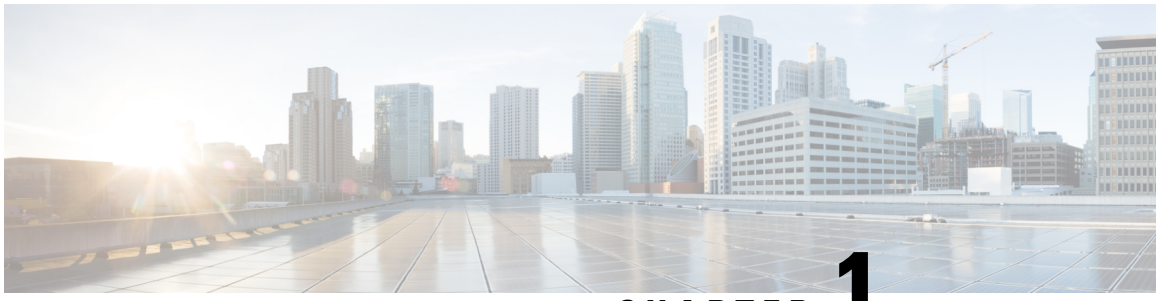
IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE 16 (Cisco ASR 900 Series)

First Published: 2018-08-01

Last Modified: 2020-04-20

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

CONTENTS



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

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 https://cfnng.cisco.com/. 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.

Restrictions for IS-IS on Cisco ASR 900 Series Routers

- Maximum number of sessions for IS-IS is 350

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.

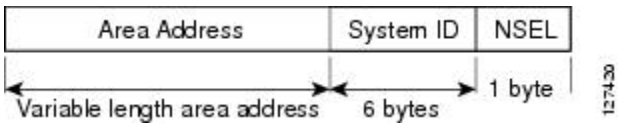
- System ID—This field is 6 octets long and immediately follows the area address. When the IS operates at Level 1, the system ID must be unique among all the Level-1 devices in the same area. When the IS operates at Level 2, the system ID must be unique among all devices in the domain.

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.

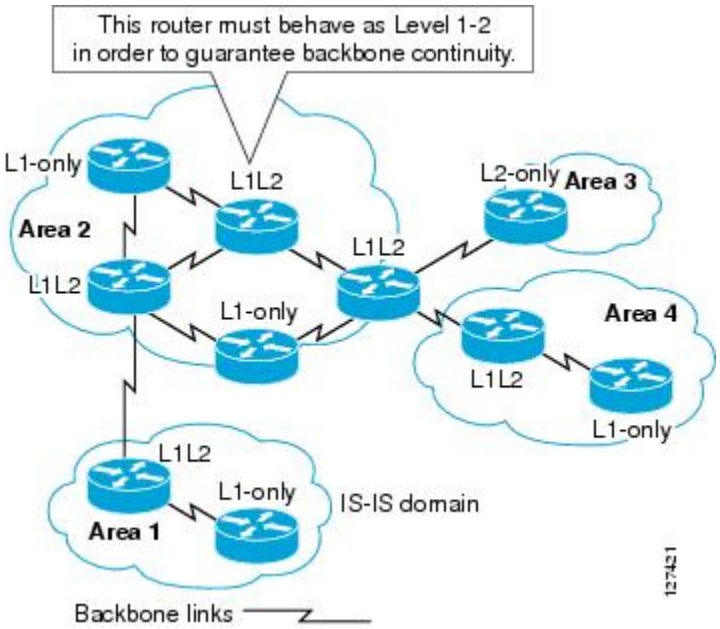
ISs form separate adjacencies for each level with neighbor ISs on the circuit.

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.

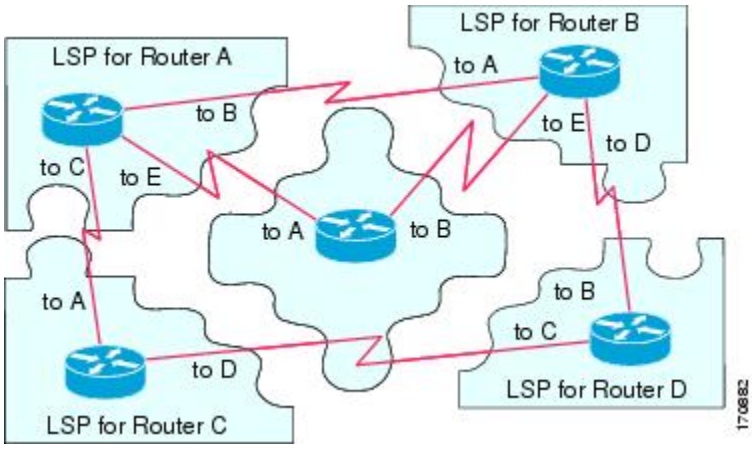
On a point-to-point circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

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.

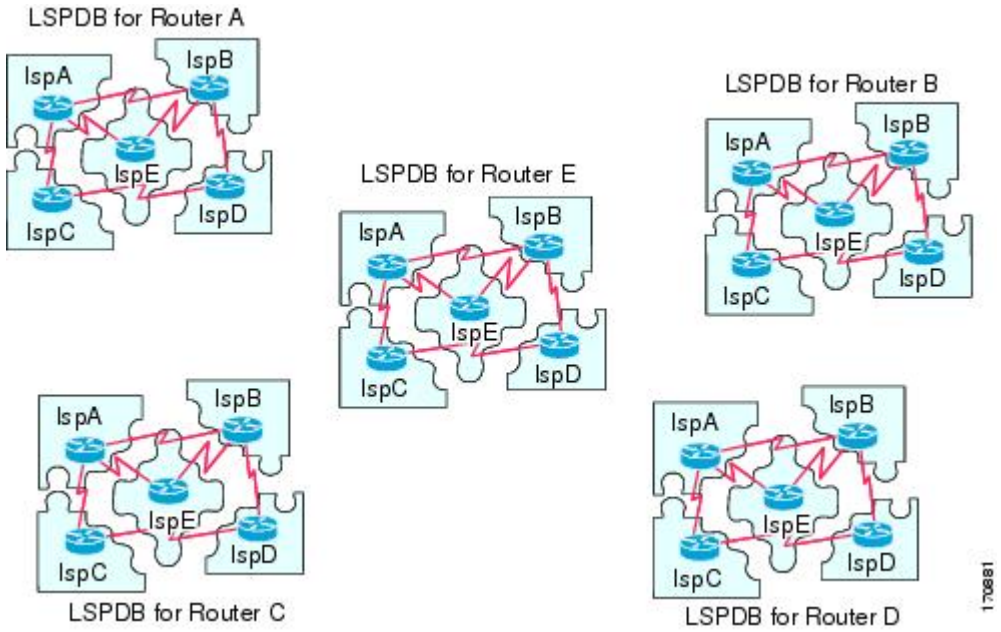
Figure 3: IS-IS Network Map



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 clns 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
```

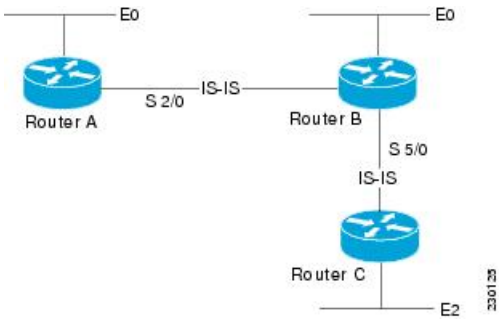
The **show isis spf-log** command displays logs of Level 1 and Level 2 LSPs including time of occurrence, duration, count, and the event that triggered the LSP.

```
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



On-Change Notifications for IS-IS State

Table 1: Feature History

Feature Name	Release Information	Description
On-Change Notifications for IS-IS State	Cisco IOS XE Bengaluru 17.4.1	This feature allows you to externalize the internal state of the router for the operational data and thus enables you to access the internal state of the router. It helps in sending on-change notifications to the receiver for any change of state, for example, when the adjacency goes up or down.

Prior to Cisco IOS XE Bengaluru Release 17.4.1, it was not possible to externalize the internal IOS state for operational data. Thus, the on-change notifications were not generated for any change of state.

Starting with Cisco IOS XE Bengaluru Release 17.4.1, you can access the internal IOS state of the router to configure or view the running state of the router. The feature allows the externalization of the internal state of the router for the operational data. It helps in sending on-change notifications to the receiver for any change of state, for example, when the adjacency goes up or down.

IOS State

The IOS state can be divided into the following conceptual groups:

- Configuration or config state includes:
  - Feature default config state (use **show running-config all** command with no user configuration)
  - Non-default config state (use **show running-config** command
  - Nonvisible non-persistent feature config state (subscriber profiles)
- Operational state includes:
  - Feature state that is not config state (adjacency, Link-State Protocol Data Units or LSPs, and so on)

Telemetry and IS-IS

Telemetry is the process of measuring the state of the components in a system and transmitting it to a remote location for further processing and analysis. Event-driven Telemetry (EDT) optimizes data collected at the receiver by streaming data only when a state transition occurs (for example, stream data only when an interface state transitions, IP route updates, and so on). For IS-IS, the on-change notifications are sent when the adjacency state changes.

For more information on the Telemetry feature, see the Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.1.x.

The following events are supported:

- IS-IS Neighbor UP
- IS-IS Neighbor DOWN
- IS-IS Neighbor INIT

Configuration Examples: On-Change Notifications for IS-IS State

The following examples show the configurations for on-change notifications for IS-IS:

Router 1

Configuration for IPv4/IPv6 Adjacency

```
interface GigabitEthernet 0/1/5
ip address <ipv4 address>
ip router isis 1
shutdown
negotiation auto
cdp enable
no cdp tlv app
ipv6 address 10:1:1::1/64
ipv6 router isis 1
isis network point-to-point
end

router isis 1
net 49.0009.0000.0000.0001.00
is-type level-1
metric-style wide
log-adjacency-changes
```

Sample Configuration for Notification

```
telemetry ietf subscription 11
encoding encode-tdl
filter tdl-uri /services;serviceName=ios_emul_oper/isis_instance;tag=CORE/isis_neighbor
source-vrf Mgmt-intf
stream native
update-policy on-change
receiver ip address 173.39.61.144 45000 protocol native
```

Router 2

Configuration for IPv4/IPv6 Adjacency

```
interface GigabitEthernet 0/1/5
ip address <ipv4 address>
ip router isis 1
negotiation auto
cdp enable
```

```
no cdp tlv app
ipv6 address 10:1:1::2/64
ipv6 router isis 1
isis network point-to-point
end

router isis 1
net 49.0009.0000.0000.0002.00
is-type level-1
metric-style wide
log-adjacency-changes
```

Configuration for Notification

```
telemetry ietf subscription <subscription_id>
encoding encode-tdl
filter <uri path>
/services;serviceName=ios_emul_oper/isis_instance;tag=<isis_tag>/isis_neighbor
source-vrf Mgmt-intf
stream native
update-policy on-change
receiver ip address <ip address> <port number> protocol <protocol name>
```

Verification of On-Change Notifications for IS-IS State Configuration

The following output shows the verification of on-change notifications for IS-IS State configuration:

```
INFO:__main__:Message TYPE CNDP_SESSION_MSG - ENCODING CNDP_MSG_ENCODING_TDL - VERSION 1 -
 FLAGS NO_FLAG - LENGTH 175
INFO:__main__:Cndp session request received: Request_id 1 - {
    "request_id": 1,
    "device_id": "ASR-903:FOC2042NFR2",
    "sw_version": "17.04.01.0.1182.1602302245..Bengaluru",
    "src_ip": "ip address",
    "capability_flag": [
        "CNDP_SESSION_CAPABILITY_KEEP_ALIVE",
        "CNDP_SESSION_CAPABILITY_SESSION_RESPONSE"
    ],
    "ch_serial_num": "ASR-903:FOX2046P1MP",
    "serial_num": "ASR-903:FOC2042NFR2"
} -
INFO:__main__:Sending cndp session request: Request_id 1 - {
    "request_id": 1,
    "status": 0,
    "capability": {
        "capability": [
            "CNDP_SESSION_CAPABILITY_KEEP_ALIVE"
        ],
        "capability_union": {
            "ka_params": {
                "ka_frequency": 30,
                "ka_max_timeout": 90
            }
        }
    }
} -
INFO:__main__:Telemetry message received from <ip address> at 2020-10-15 10:51:49
INFO:__main__:Message TYPE CNDP_KEEPALIVE_MSG - ENCODING CNDP_MSG_ENCODING_TDL - VERSION 1
 - FLAGS NO_FLAG - LENGTH 28
INFO:__main__:SEQUENCE_ID 222028829 TIMESTAMP 2020-10-15 16:21:46.304162
INFO:__main__:Sending keep_alive response with sequence id 222028829
INFO:__main__:Telemetry message received from <ip address> at 2020-10-15 10:51:49
INFO:__main__:Message TYPE CNDP_TELEMETRY_EVENT_MSG - ENCODING CNDP_MSG_ENCODING_TDL -
```

```
VERSION 1 - FLAGS NO_FLAG - LENGTH 391
INFO:__main__:{
    "subscription_id": 11,
    "capture_time": {
        "second": 1602759106,
        "microsec": 937026
    },
    "data": {
        "result": {
            "exec_ctx": "ios_emul_oper_db_context",
           "params_id": {
                "which": [],
                "which_union": {}
            },
            "result_code": "GREEN_RES_OK",
            "notf_str": "",
            "err_str": "",
            "num_entry": 0
        },
        "data": {
            "table_luid": [
                "tbl_isis_neighbor",
                "190 55 188 213 227 103 66 189 42 56 218 39 4 45 119 7"
            ],
            "cursor": {
                "len": 0,
                "data": "",
                "issu_checking": 0
            },
            "num_entry": 1,
            "entry": [
                {
                    "keys": {
                        "num_key_field_ids": 0,
                        "num_key_luids": 0,
                        "num_key": 0,
                        "field_ids": "",
                        "luids": [],
                        "keys": [],
                        "num_src_ids": 0,
                        "src_ids": ""
                    },
                    "op": "GREEN_RECORD_UPDATE",
                    "len": 164,
                    "entry_data": {
                        "isis_neighbor_rec": {
                            "ipv4_address": "ip address",
                            "ipv6_address": null,
                            "state": "ISIS_INIT",
                            "holdtime": 29
                        },
                        "isis_neighbor_key": {
                            "system_id": {
                                "addr_len": 6,
                                "addr": "0 0 0 0 0 50"
                            },
                            "level": "ISIS_LEVEL_1",
                            "if_name": "GigabitEthernet0/1/5"
                        }
                    },
                    "e": [],
                    "ext_metadata": {
                        "t": "GREEN_EXT_META_NONE",
                        "t_union": {}
```

```
                    },
                    "link_entry_info_list": []
                }
            ]
        }
    },
    "location": {
        "fru": "BINOS_FRU_RP",
        "slot": 0,
        "bay": 0,
        "chassis": -1,
        "node": 0
    }
}
INFO:__main__:Telemetry message received from <ip address> at 2020-10-15 10:51:50
INFO:__main__:Message TYPE CNDP_TELEMETRY_EVENT_MSG - ENCODING CNDP_MSG_ENCODING_TDL -
VERSION 1 - FLAGS NO_FLAG - LENGTH 391
INFO:__main__:{
    "subscription_id": 11,
    "capture_time": {
        "second": 1602759107,
        "microsec": 977053
    },
    "data": {
        "result": {
            "exec_ctx": "ios_emul_oper_db_context",
            "params_id": {
                "which": [],
                "which_union": {}
            },
            "result_code": "GREEN_RES_OK",
            "notf_str": "",
            "err_str": "",
            "num_entry": 0
        },
        "data": {
            "table_luid": [
                "tbl_isis_neighbor",
                "190 55 188 213 227 103 66 189 42 56 218 39 4 45 119 7"
            ],
            "cursor": {
                "len": 0,
                "data": "",
                "issu_checking": 0
            },
            "num_entry": 1,
            "entry": [
                {
                    "keys": {
                        "num_key_field_ids": 0,
                        "num_key_luids": 0,
                        "num_key": 0,
                        "field_ids": "",
                        "luids": [],
                        "keys": [],
                        "num_src_ids": 0,
                        "src_ids": ""
                    },
                    "op": "GREEN_RECORD_UPDATE",
                    "len": 164,
                    "entry_data": {
                        "isis_neighbor_rec": {
                            "ipv4_address": "ip address",
                            "ipv6_address": null,
```

```
                            "state": "ISIS_UP",
                            "holdtime": 9
                        },
                        "isis_neighbor_key": {
                            "system_id": {
                                "addr_len": 6,
                                "addr": "0 0 0 0 0 50"
                            },
                            "level": "ISIS_LEVEL_1",
                            "if_name": "GigabitEthernet0/1/5"
                        }
                    },
                    "e": [],
                    "ext_metadata": {
                        "t": "GREEN_EXT_META_NONE",
                        "t_union": {}
                    },
                    "link_entry_info_list": []
                }
            ]
        }
    },
    "location": {
        "fru": "BINOS_FRU_RP",
        "slot": 0,
        "bay": 0,
        "chassis": -1,
        "node": 0
    }
}
INFO:__main__:Telemetry message received from <ip address> at 2020-10-15 10:51:50
INFO:__main__:Message TYPE CNDP_TELEMETRY_EVENT_MSG - ENCODING CNDP_MSG_ENCODING_TDL -
VERSION 1 - FLAGS NO_FLAG - LENGTH 391
INFO:__main__:{
    "subscription_id": 11,
    "capture_time": {
        "second": 1602759107,
        "microsec": 977747
    },
    "data": {
        "result": {
            "exec_ctx": "ios_emul_oper_db_context",
            "params_id": {
                "which": [],
                "which_union": {}
            },
            "result_code": "GREEN_RES_OK",
            "notf_str": "",
            "err_str": "",
            "num_entry": 0
        },
        "data": {
            "table_luid": [
                "tbl_isis_neighbor",
                "190 55 188 213 227 103 66 189 42 56 218 39 4 45 119 7"
            ],
            "cursor": {
                "len": 0,
                "data": "",
                "issu_checking": 0
            },
            "num_entry": 1,
            "entry": [
                {
```

```
                        "keys": {
                            "num_key_field_ids": 0,
                            "num_key_luids": 0,
                            "num_key": 0,
                            "field_ids": "",
                            "luids": [],
                            "keys": [],
                            "num_src_ids": 0,
                            "src_ids": ""
                        },
                        "op": "GREEN_RECORD_UPDATE",
                        "len": 164,
                        "entry_data": {
                            "isis_neighbor_rec": {
                                "ipv4_address": "ip address",
                                "ipv6_address": null,
                                "state": "ISIS_INIT",
                                "holdtime": 30
                            },
                            "isis_neighbor_key": {
                                "system_id": {
                                    "addr_len": 6,
                                    "addr": "0 0 0 0 0 50"
                                },
                                "level": "ISIS_LEVEL_2",
                                "if_name": "GigabitEthernet0/1/5"
                            }
                        },
                        "e": [],
                        "ext_metadata": {
                            "t": "GREEN_EXT_META_NONE",
                            "t_union": {}
                        },
                        "link_entry_info_list": []
                    }
                ]
            }
        },
        "location": {
            "fru": "BINOS_FRU_RP",
            "slot": 0,
            "bay": 0,
            "chassis": -1,
            "node": 0
        }
}
INFO:__main__:Telemetry message received from <ip address> at 2020-10-15 10:51:51
INFO:__main__:Message TYPE CNDP_TELEMETRY_EVENT_MSG - ENCODING CNDP_MSG_ENCODING_TDL -
VERSION 1 - FLAGS NO_FLAG - LENGTH 391
INFO:__main__:{
    "subscription_id": 11,
    "capture_time": {
        "second": 1602759108,
        "microsec": 963576
    },
    "data": {
        "result": {
            "exec_ctx": "ios_emul_oper_db_context",
            "params_id": {
                "which": [],
                "which_union": {}
            },
            "result_code": "GREEN_RES_OK",
            "notf_str": "",
```

```
            "err_str": "",
            "num_entry": 0
        },
        "data": {
            "table_luid": [
                "tbl_isis_neighbor",
                "190 55 188 213 227 103 66 189 42 56 218 39 4 45 119 7"
            ],
            "cursor": {
                "len": 0,
                "data": "",
                "issu_checking": 0
            },
            "num_entry": 1,
            "entry": [
                {
                    "keys": {
                        "num_key_field_ids": 0,
                        "num_key_luids": 0,
                        "num_key": 0,
                        "field_ids": "",
                        "luids": [],
                        "keys": [],
                        "num_src_ids": 0,
                        "src_ids": ""
                    },
                    "op": "GREEN_RECORD_UPDATE",
                    "len": 164,
                    "entry_data": {
                        "isis_neighbor_rec": {
                            "ipv4_address": "ip address",
                            "ipv6_address": null,
                            "state": "ISIS_UP",
                            "holdtime": 9
                        },
                        "isis_neighbor_key": {
                            "system_id": {
                                "addr_len": 6,
                                "addr": "0 0 0 0 0 50"
                            },
                            "level": "ISIS_LEVEL_2",
                            "if_name": "GigabitEthernet0/1/5"
                        }
                    },
                    "e": [],
                    "ext_metadata": {
                        "t": "GREEN_EXT_META_NONE",
                        "t_union": {}
                    },
                    "link_entry_info_list": []
                }
            ]
        }
    },
    "location": {
        "fru": "BINOS_FRU_RP",
        "slot": 0,
        "bay": 0,
        "chassis": -1,
        "node": 0
    }
}
```

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

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.

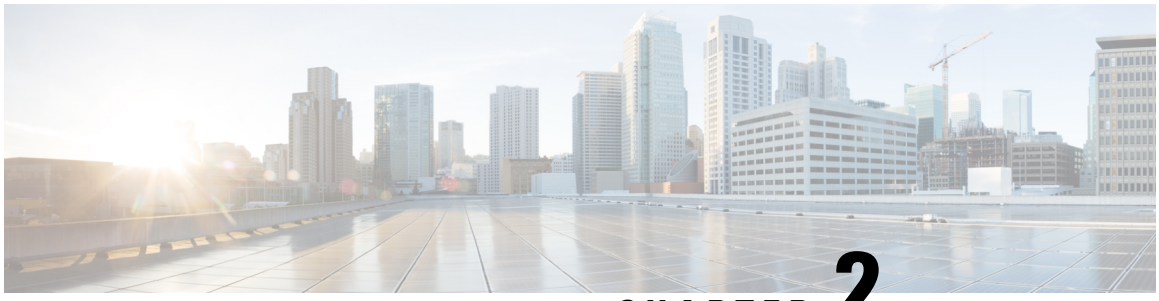
Level-2 router —An IS that supports Level-2 routing.

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

Loop-Free Alternate Fast Reroute

Loop-Free Alternate (LFA) Fast Reroute (FRR) is a mechanism that provides local protection for unicast traffic in order to rapidly converge traffic flows around link and/or node failures.

Prerequisites for Loop-Free Alternate Fast Reroute

- Any of the following protocols must be supported for Loop-Free Alternate Fast Reroute:
  - Intermediate System-to-Intermediate System (IS-IS)
  - Open Shortest Path First (OSPF)
- While configuring ISIS protocol, **isis network point-to-point** must be configured.

Restrictions for Loop-Free Alternate Fast Reroute

- Logical interfaces namely Port-channel (PoCH) support LFA FRR and remote LFA-FRR, with a single member link. Port-channel can be used as a backup path.
- Micro loops may form due to traffic congestion.
- A Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel cannot be used as a protected interface. However, an MPLS-TE tunnel can be a protecting (repair) interface as long as the TE tunnel is used as a primary path.

Note VPLS over TE Tunnel or TE FRR is not supported on the Cisco ASR 900 RSP3 module.

- For TDM psuedowires, the interfaces supported are CEM (CESoP, SAToP) and IMA (PVC,PVP); supported both on OC-3 and T1/E1 controllers. A maximum of 500 VCs can be configured per OC-3 controller.

Note This restriction is applicable only on the Cisco RSP1 and RSP2 Modules.

- For TDM psuedowires, the interfaces supported are CEM on OC-3.

Note This restriction is applicable only on the Cisco RSP3 Modules.

- Each bridge domain interface (BDI) protected by FRR can have only one EFP.
- Remote LFA FRR provides better convergence with SFP ports rather than copper ports. As a workaround for copper ports, BFD triggered FRR can be used.
- FRR is *not* supported with POS and serial interfaces.
- Scale limit for FRR-protected global prefixes is 1500 and for layer 3 VPNs, scale limit is 4000.

Information About Loop-Free Alternate Fast Reroute

The Loop-Free Alternate (LFA) Fast Reroute (FRR) feature offers an alternative to the MPLS Traffic Engineering Fast Reroute feature to minimize packet loss due to link or node failure.

LFA FRR enables a backup route to avoid traffic loss if a network fails. The backup routes (repair paths) are precomputed and installed in the router as the backup for the primary paths. After the router detects a link or adjacent node failure, it switches to the backup path to avoid traffic loss.

LFA is a node other than the primary neighbor. Traffic is redirected to an LFA after a network failure. An LFA makes the forwarding decision without any knowledge of the failure. An LFA must neither use a failed element nor use a protecting node to forward traffic. An LFA must not cause loops. By default, LFA is enabled on all supported interfaces as long as the interface can be used as a primary path.

Advantages of using per-prefix LFAs are as follows:

- The repair path forwards traffic during transition when the primary path link is down.
- All destinations having a per-prefix LFA are protected. This leaves only a subset (a node at the far side of the failure) unprotected.

Supported Information

- LFA FRR is supported with equal cost multipath (ECMP).
- Fast Reroute triggered by Bidirectional Forwarding (BFD) is supported.
- Remote LFA tunnels are High Availability aware; hence, Stateful Switchover (SSO) compliant.

Benefits of Loop-Free Alternate Fast Reroute

- Same level of protection from traffic loss
- Simplified configuration
- Link and node protection
- Link and path protection
- LFA (loop-free alternate) paths
- Support for both IP and Label Distribution Protocol (LDP) core
- LFA FRR is supported with equal cost multipath (ECMP).
- Fast Reroute triggered by Bidirectional Forwarding (BFD).
- Remote LFA tunnels are High Availability aware; hence, Stateful Switchover (SSO) compliant.

LFA FRR and Remote LFA FRR over Bridge Domains Interfaces

The router supports bridge domain interfaces (BDI). For information on configuring bridge domains, see Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router.

LFA FRR and remote LFA FRR is supported on bridge domain interfaces on the router. For information on configuring Remote LFA FRR on BDI, see How to Configure Loop-Free Alternate Fast Reroute, on page 34.

IS-IS and IP FRR

When a local link fails in a network, IS-IS recomputes new primary next-hop routes for all affected prefixes. These prefixes are updated in the RIB and the Forwarding Information Base (FIB). Until the primary prefixes are updated in the forwarding plane, traffic directed towards the affected prefixes are discarded. This process can take hundreds of milliseconds.

In IP FRR, IS-IS computes LFA next-hop routes for the forwarding plane to use in case of primary path failures. LFA is computed per prefix.

When there are multiple LFAs for a given primary path, IS-IS uses a tiebreaking rule to pick a single LFA for a primary path. In case of a primary path with multiple LFA paths, prefixes are distributed equally among LFA paths.

Repair Paths

Repair paths forward traffic during a routing transition. When a link or a router fails, due to the loss of a physical layer signal, initially, only the neighboring routers are aware of the failure. All other routers in the

network are unaware of the nature and location of this failure until information about this failure is propagated through a routing protocol, which may take several hundred milliseconds. It is, therefore, necessary to arrange for packets affected by the network failure to be steered to their destinations.

A router adjacent to the failed link employs a set of repair paths for packets that would have used the failed link. These repair paths are used from the time the router detects the failure until the routing transition is complete. By the time the routing transition is complete, all routers in the network revise their forwarding data and the failed link is eliminated from the routing computation.

Repair paths are precomputed in anticipation of failures so that they can be activated the moment a failure is detected.

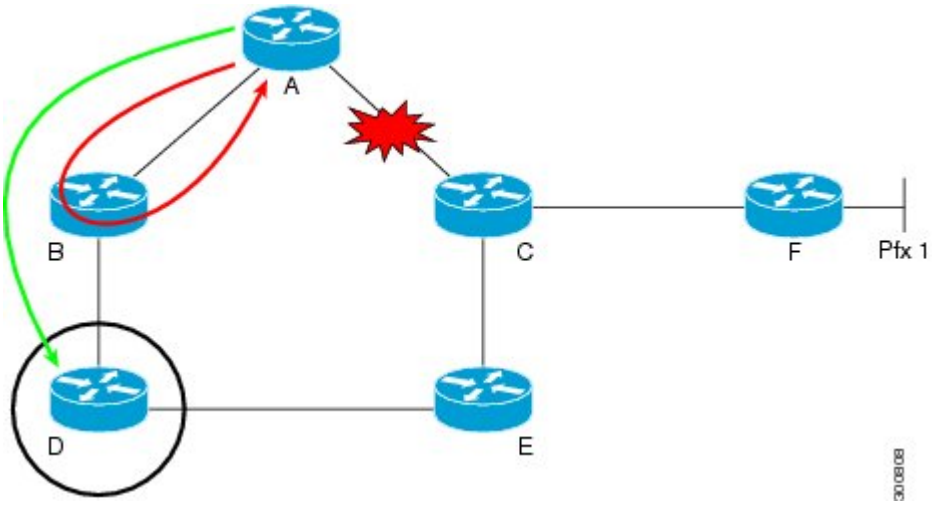
The IPv4 LFA FRR feature uses the following repair paths:

- Equal Cost Multipath (ECMP) uses a link as a member of an equal cost path-split set for a destination. The other members of the set can provide an alternative path when the link fails.
- LFA is a next-hop route that delivers a packet to its destination without looping back. Downstream paths are a subset of LFAs.

Remote LFA FRR

Some topologies (for example the commonly used ring-based topology) require protection that is not afforded by LFA FRR alone. Consider the topology shown in the figure below:

Figure 6: Remote LFA FRR with Ring Topology



The red looping arrow represents traffic that is looping immediately after a failure between node A and C (before network reconvergence). Device A tries to send traffic destined to F to next-hop B. Device B cannot be used as an LFA for prefixes advertised by nodes C and F. The actual LFA is node D. However, node D is not directly connected to the protecting node A. To protect prefixes advertised by C, node A must tunnel the packet around the failed link A-C to node D, provided that the tunnel does not traverse the failing link.

Remote LFA FRR enables you to tunnel a packet around a failed link to a remote loop-free alternate that is more than one hop away. In the figure above, the green arrow between A and D shows the tunnel that is automatically created by the remote LFA feature to bypass looping.

Remote LFA FRR for TDM and ATM Psuedowires

The Router supports two pseudowire types that utilize CEM transport: Structure-Agnostic TDM over Packet (SAToP) and Circuit Emulation Service over Packet-Switched Network (CESoPSN). Remote LFA FRR is supported on TDM and ATM pseudowires. For information on configuring TDM and ATM pseudowires on the Cisco ASR 903, see Configuring Pseudowire.

For information on configuring Remote LFA FRR on TDM and ATM pseudowires, see How to Configure Loop-Free Alternate Fast Reroute, on page 34.

Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC) and LFA FRR Integration

Both the Labeled Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC) feature and the Loop-Free Alternate (LFA) Fast Reroute (FRR) feature can be configured together on the router.

BGP PIC is supported for bridge domain interfaces (BDI) with FRR.

Note Each bridge domain interface (BDI) protected by FRR can have only one EFP.

For information on configuring BGP PIC, see BGP PIC Edge for IP and MPLS-VPN.

Remote LFA FRR with VPLS

VPLS (Virtual Private LAN Service) enables enterprises to link together their Ethernet-based LANs from multiple sites via the infrastructure provided by their service provider. For information on configuring VPLS, see Configuring Virtual Private LAN Services. Starting With Cisco IOS XE Release 3.10S, Remote LFA FRR is supported with VPLS.

For information on configuring remote LFA FRR with VPLS, see How to Configure Loop-Free Alternate Fast Reroute, on page 34.

Benefits of Remote LFA FRR

Effective with Cisco IOS XE Release 3.10S Remote LFA is supported on the router for these functions:

- Inverse Multiplexing over ATM (IMA) over MPLS; PVC and PVC sessions are supported for the ATM (IMA).

  Note Inverse Multiplexing over ATM (IMA) over MPLS is not supported on the Cisco ASR 900 RSP3 Module for Cisco IOS XE Release 3.16.

- Virtual Private LAN Services (VPLS)
- Circuit Emulation Service over Packet Switched Network (CESoPSN) over MPLS, and Structure-Agnostic Time Division Multiplexing over Packet (SAToP) over MPLS networks for T1, E1, SDH and SONET framing.

How to Configure Loop-Free Alternate Fast Reroute

To enable loop-free alternate fast reroute support for L2VPNs, VPLS, TDM pseudowires and VPWS, you must configure LFA FRR for the routing protocol. You can enable LFA FRR using ISIS or OSFP configurations.

- For information on configuring LFA FRR using OSPF, see OSPFv2 Loop-Free Alternate Fast Reroute in the *IP Routing: OSPF Configuration Guide*.
- For information on configuring Remote LFA FRR using OSPF, seeOSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute in the *IP Routing: OSPF Configuration Guide*.
- For information on configuring Remote LFA FRR using ISIS on the Cisco ASR 903, see Configuring IS-IS Remote Loop-Free Alternate Fast Reroute, on page 34.

Configuring IS-IS Remote Loop-Free Alternate Fast Reroute

The following additional configurations are mandatory:

- **mpls ldp discovery targeted-hello accept**

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **fast-reroute per-prefix** {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*}
5. **fast-reroute remote-lfa** {**level-1** | **level-2**} **mpls-ldp** [**maximum-metric** *metric-value*]
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 ipfrr`	Enables the IS-IS routing protocol and specifies an IS-IS process. • Enters router configuration mode.

	Command or Action	Purpose
Step 4	**fast-reroute per-prefix** {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*} **Example:** `Device (config-router)#  fast-reroute per-prefix level-1 all`	Enables per-prefix FRR. • Configure the **all** keyword to protect all prefixes.
Step 5	**fast-reroute remote-lfa** {**level-1** | **level-2**} **mpls-ldp** [**maximum-metric** *metric-value*] **Example:** `Device(config-router)# fast-reroute remote-lfa level-1 mpls-ldp`	Configures an FRR path that redirects traffic to a remote LFA tunnel for either level 1 or level 2 packets. • Use the **maximum-metric** *metric-value* keyword-argument pair to specify the maximum metric value required to reach the release node.
Step 6	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and enters privileged EXEC mode.

Recommended Configurations ISIS

For optimal results with remote LFA FRR, it is recommended that you use the following SFP timers:

- ISIS
  - spf-interval 5 50 200
  - prc-interval 5 50 200
  - sp-gen-interval 5 50 200
  - fast-flood 10
- Globally configure the MPLS IGP hold-down timer to avoid an indefinite wait by IGP for synchronization using the **mpls ldp igp sync holdown 2000** command.

Example: Configuring IS-IS Remote Loop-Free Alternate Fast Reroute

The following example shows how to enable remote LFA FRR:

```
Router(config)# router isis
Router(config)# fast-reroute per-prefix level-1 all
Router(config)# fast-reroute per-prefix level-2 all
Router(router-config)# fast-reroute remote-lfa level-1 mpls-ldp
Router(router-config)# fast-reroute remote-lfa level-2 mpls-ldp
```

Example: Configuring Remote LFA FRR with VPLS

Example: Configuration of Remote LFA FRR with Interior Gateway Protocol (IGP)

```
router isis hp
 net 49.0101.0000.0000.0802.00
 is-type level-2-only
 ispf level-2
 metric-style wide
 fast-flood
 set-overload-bit on-startup 180
 max-lsp-lifetime 65535
 lsp-refresh-interval 65000
 spf-interval 5 50 200
 prc-interval 5 50 200
 lsp-gen-interval 5 5 200
 no hello padding
 log-adjacency-changes
 nsf cisco
 fast-reroute per-prefix level-1 all
 fast-reroute per-prefix level-2 all
 fast-reroute remote-lfa level-1 mpls-ldp
 fast-reroute remote-lfa level-2 mpls-ldp
 passive-interface Loopback0
 mpls ldp sync
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
```

Example: Configuration of Remote LFA FRR with VPLS at the interface level.

```
!
interface GigabitEthernet0/3/3
 ip address 198.51.100.1 255.255.255.0
 ip router isis hp
 logging event link-status
 load-interval 30
 negotiation auto
 mpls ip
 mpls traffic-eng tunnels
 isis network point-to-point
end
!
```

Example: Configuration of remote LFA FRR with VPLS at the global level.

```
!
l2 vfi Test-2000 manual
 vpn id 2010
 bridge-domain 2010
 neighbor 192.0.2.1 encapsulation mpls
!
```

Example: Configuration of remote LFA FRR with VPLS at Access side.

```
!
interface TenGigabitEthernet0/2/0
 no ip address
 service instance trunk 1 ethernet
  encapsulation dot1q 12-2012
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
```

How to Configure OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

Configuring a Remote LFA Tunnel

Perform this task to configure a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix remote-lfa** [**area** *area-id*] **tunnel mpls-ldp**

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 ospf** *process-id* **Example:** `Device(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix remote-lfa** [**area** *area-id*] **tunnel mpls-ldp** **Example:** `Device(config-router)# fast-reroute per-prefix remote-lfa area 2 tunnel mpls-ldp`	Configures a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel via MPLS-LDP. • Use the **area** *area-id* keyword and argument to specify an area in which to enable LFA FRR.

Configuring the Maximum Distance to a Tunnel Endpoint

Perform this task to configure the maximum distance to the tunnel endpoint in a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*

4. **fast-reroute per-prefix remote-lfa** [**area** *area-id*] **maximum-cost** *distance*

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 ospf** *process-id* **Example:** `Device(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix remote-lfa** [**area** *area-id*] **maximum-cost** *distance* **Example:** `Device(config-router)# fast-reroute per-prefix remote-lfa area 2 maximum-cost 30`	Configures the maximum distance to the tunnel endpoint in a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel. • Use the **area** *area-id* keyword and variable to specify an area in which to enable LFA FRR.

Verifying Loop-Free Alternate Fast Reroute

Use one or more of the following commands to verify the LFA FRR configuration

- **show ip cef network-prefix internal**
- **show mpls infrastructure lfd pseudowire internal**
- **show platform hardware pp active feature cef database ipv4 network-prefix**

Example: Verifying LFA FRR with L2VPN

show ip cef internal

The following is sample output from the **show ip cef internal** command:

```
Device# show ip cef 16.16.16.16 internal
16.16.16.16/32, epoch 2, RIB[I], refcount 7, per-destination sharing
  sources: RIB, RR, LTE
  feature space:
   IPRM: 0x00028000
   Broker: linked, distributed at 1st priority
```

```
   LFD: 16.16.16.16/32 1 local label
   local label info: global/17
        contains path extension list
        disposition chain 0x3A3C1DF0
        label switch chain 0x3A3C1DF0
  subblocks:
   1 RR source [no flags]
    non-eos chain [16|44]
  ifnums:
   GigabitEthernet0/0/2(9): 7.7.7.2
   GigabitEthernet0/0/7(14): 7.7.17.9
  path 35D61070, path list 3A388FA8, share 1/1, type attached nexthop, for IPv4, flags
has-repair
    MPLS short path extensions: MOI flags = 0x20 label 16
  nexthop 7.7.7.2 GigabitEthernet0/0/2 label [16|44], adjacency IP adj out of
GigabitEthernet0/0/2, addr 7.7.7.2 35E88520
    repair: attached-nexthop 7.7.17.9 GigabitEthernet0/0/7 (35D610E0)
  path 35D610E0, path list 3A388FA8, share 1/1, type attached nexthop, for IPv4, flags
repair, repair-only
  nexthop 7.7.17.9 GigabitEthernet0/0/7, repair, adjacency IP adj out of GigabitEthernet0/0/7,
 addr 7.7.17.9 3A48A4E0
  output chain: label [16|44]
  FRR Primary (0x35D10F60)
  <primary:  TAG adj out of GigabitEthernet0/0/2, addr 7.7.7.2 35E88380>
  <repair:  TAG adj out of GigabitEthernet0/0/7, addr 7.7.17.9 3A48A340>
Rudy17#show mpls infrastructure lfd pseudowire internal
PW ID: 1VC ID: 4, Nexthop address: 16.16.16.16
SSM Class: SSS HW
Segment Count: 1
VCCV Types Supported:  cw ra ttl
Imposition details:
 Label stack {22 16}, Output interface: Gi0/0/2
 Preferred path: not configured
 Control Word: enabled, Sequencing: disabled
 FIB Non IP entry: 0x35D6CEEC
 Output chain:  AToM Imp (locks 4) label 22 label [16|44]
  FRR Primary (0x35D10F60)
  <primary:  TAG adj out of GigabitEthernet0/0/2, addr 7.7.7.2 35E88380>
Disposition details:
 Local label: 16
 Control Word: enabled, Sequencing: disabled
 SSS Switch: 3976200193
 Output chain:  mpls_eos( connid router-alert AToM Disp (locks 5)/ drop)
```

show mpls infrastructure lfd pseudowire internal

The following is sample output from the **show mpls infrastructure lfd pseudowire internal** command:

```
Device# show mpls infrastructure lfd pseudowire internal
PW ID: 1VC ID: 4, Nexthop address: 16.16.16.16
SSM Class: SSS HW
Segment Count: 1
VCCV Types Supported:  cw ra ttl
Imposition details:
 Label stack {22 16}, Output interface: Gi0/0/2
 Preferred path: not configured
 Control Word: enabled, Sequencing: disabled
 FIB Non IP entry: 0x35D6CEEC
 Output chain:  AToM Imp (locks 4) label 22 label [16|44]
  FRR Primary (0x35D10F60)
  <primary:  TAG adj out of GigabitEthernet0/0/2, addr 7.7.7.2 35E88380>
```

```
Disposition details:
 Local label: 16
 Control Word: enabled, Sequencing: disabled
 SSS Switch: 3976200193
 Output chain:  mpls_eos( connid router-alert AToM Disp (locks 5)/ drop)
```

show platform hardware pp active feature cef database

The following is sample output from the **show platform hardware pp active feature cef database** command:

```
Device# show platform hardware pp active feature cef database ipv4 16.16.16.16/32
=== CEF Prefix ===
16.16.16.16/32 -- next hop: UEA Label OCE (PI:0x104abee0, PD:0x10e6b9c8)
                Route Flags: (0)
                Handles (PI:0x104ab6e0) (PD:0x10e68140)

  HW Info:
    TCAM handle: 0x0000023f    TCAM index: 0x0000000d
    FID index  : 0x0000f804    EAID      : 0x0000808a
    MET        : 0x0000400c    FID Count : 0x00000000

=== Label OCE ===
  Label flags: 4
  Num Labels: 1
  Num Bk Labels: 1
  Out Labels: 16
  Out Backup Labels: 44
  Next OCE Type: Fast ReRoute OCE; Next OCE handle: 0x10e6f428

=== FRR OCE ===
  FRR type         : IP FRR
  FRR state        : Primary
  Primary IF's gid : 3
  Primary FID      : 0x0000f801
  FIFC entries     : 32
  PPO handle       : 0x00000000
  Next OCE         : Adjacency (0x10e63b38)
  Bkup OCE         : Adjacency (0x10e6e590)

=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 7.7.7.2
  Interface: GigabitEthernet0/0/2   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x00000039) (PI:0x1041d410) (PD:0x10e63b38)
  Rewrite Str: d0:c2:82:17:8a:82:d0:c2:82:17:f2:02:88:47

  HW Info:
    FID index: 0x0000f486    EL3 index: 0x00001003    EL2 index: 0x00000000
    El2RW    : 0x00000107    MET index: 0x0000400c    EAID     : 0x00008060
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: d0:c2:82:17:8a:82:08:00:40:00:0d:02

=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 7.7.17.9
  Interface: GigabitEthernet0/0/7   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x00000012) (PI:0x104acbd0) (PD:0x10e6e590)
  Rewrite Str: d0:c2:82:17:c9:83:d0:c2:82:17:f2:07:88:47

  HW Info:
    FID index: 0x0000f49d    EL3 index: 0x00001008    EL2 index: 0x00000000
```

```
El2RW    : 0x00000111    MET index: 0x00004017    EAID     : 0x0000807d
HW ADJ FLAGS: 0x40
Hardware MAC Rewrite Str: d0:c2:82:17:c9:83:08:00:40:00:0d:07
```

Configuration Examples for OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

Example: Configuring a Remote LFA Tunnel

The following example shows how to configure a remote per-prefix LFA FRR in area 2. The remote tunnel type is specified as MPLS-LDP:

```
Router(config-router)# fast-reroute per-prefix remote-lfa area 2 tunnel mpls-ldp
```

Example: Configuring the Maximum Distance to a Tunnel Endpoint

The following example shows how to set a maximum cost of 30 in area 2:

```
Router(config-router)# fast-reroute per-prefix remote-lfa area 2 maximum-cost 30
```

Example: Verifying Tunnel Interfaces Created by OSPF IPv4 Remote LFA IPFRR

The following example displays information about about tunnel interfaces created by OSPF IPv4 LFA IPFRR:

```
Router# show ip ospf fast-reroute remote-lfa tunnels

      OSPF Router with ID (192.168.1.1) (Process ID 1)
      Area with ID (0)
      Base Topology (MTID 0)

Interface MPLS-Remote-Lfa3
 Tunnel type: MPLS-LDP
 Tailend router ID: 192.168.3.3
 Termination IP address: 192.168.3.3
 Outgoing interface: Ethernet0/0
 First hop gateway: 192.168.14.4
 Tunnel metric: 20
 Protects:
  192.168.12.2 Ethernet0/1, total metric 30
```

Verifying Remote Loop-Free Alternate Fast Reroute with VPLS

Example: Verifying Remote LFA FRR with VPLS

show ip cef internal

The following is sample output from the **show ip cef internal** command:

```
Router# show ip cef 198.51.100.2/32 internal

198.51.100.2/32, epoch 2, RIB[I], refcount 7, per-destination sharing
  sources: RIB, RR, LTE
  feature space:
   IPRM: 0x00028000
   Broker: linked, distributed at 1st priority
   LFD: 198.51.100.2/32 1 local label
   local label info: global/2033
        contains path extension list
        disposition chain 0x46764E68
        label switch chain 0x46764E68
  subblocks:
   1 RR source [heavily shared]
    non-eos chain [explicit-null|70]
  ifnums:
   TenGigabitEthernet0/1/0(15): 192.0.2.10
   MPLS-Remote-Lfa2(46)
  path 44CE1290, path list 433CF8C0, share 1/1, type attached nexthop, for IPv4, flags
has-repair
    MPLS short path extensions: MOI flags = 0x21 label explicit-null
  nexthop 192.0.2.10 TenGigabitEthernet0/1/0 label [explicit-null|70], adjacency IP adj out
 of TenGigabitEthernet0/1/0, addr 192.0.2.10 404B3960
    repair: attached-nexthop 192.0.2.1 MPLS-Remote-Lfa2 (44CE1300)
  path 44CE1300, path list 433CF8C0, share 1/1, type attached nexthop, for IPv4, flags
repair, repair-only
  nexthop 192.0.2.1 MPLS-Remote-Lfa2, repair, adjacency IP midchain out of MPLS-Remote-Lfa2
 404B3B00
  output chain: label [explicit-null|70]
  FRR Primary (0x3E25CA00)
  <primary:  TAG adj out of TenGigabitEthernet0/1/0, addr 192.168.101.22 404B3CA0>
  <repair:  TAG midchain out of MPLS-Remote-Lfa2 404B37C0 label 37 TAG adj out of
GigabitEthernet0/3/3, addr 192.0.2.14 461B2F20>
```

show ip cef detail

The following is sample output from the **show ip cef detail** command:

```
Router# show ip cef 198.51.100.2/32 detail

198.51.100.2/32, epoch 2
  local label info: global/2033
  1 RR source [heavily shared]
  nexthop 192.0.2.14 TenGigabitEthernet0/1/0 label [explicit-null|70]
    repair: attached-nexthop 192.0.2.1 MPLS-Remote-Lfa2
  nexthop 192.0.2.1 MPLS-Remote-Lfa2, repair
!
```

show platform hardware pp active feature cef databas

The following is sample output from the **show platform hardware pp active feature cef database** command:

```
Router# show platform hardware pp active feature cef database ipv4 198.51.100.2/32

=== CEF Prefix ===
198.51.100.2/32 -- next hop: UEA Label OCE (PI:0x10936770, PD:0x12dd1cd8)
                Route Flags: (0)
                Handles (PI:0x109099c8) (PD:0x12945968)

  HW Info:
    TCAM handle: 0x00000266    TCAM index: 0x00000015
    FID index  : 0x00008e7f    EAID      : 0x0001d7c4
    MET        : 0x0000401c    FID Count : 0x00000000
=== Label OCE ===
  Label flags: 4
  Num Labels: 1
  Num Bk Labels: 1
  Out Labels: 0
  Out Backup Labels: 70
=== FRR OCE ===
  FRR type         : IP FRR
  FRR state        : Primary
  Primary IF's gid : 52
  Primary FID      : 0x00008cb6
  FIFC entries     : 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0
  PPO handle       : 0x00000000
  Next OCE         : Adjacency (0x130e0df0)
  Bkup OCE         : Adjacency (0x130de608)

=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 192.168.101.22
  Interface: TenGigabitEthernet0/1/0   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x000016ac) (PI:0x1090cc10) (PD:0x130e0df0)
  Rewrite Str: 18:33:9d:3d:83:10:c8:f9:f9:8d:04:10:88:47
HW Info:
    FID index: 0x00008e7e    EL3 index: 0x00001034    EL2 index: 0x00000000
    El2RW    : 0x0000010d    MET index: 0x00004012    EAID     : 0x0001d7c1
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: 18:33:9d:3d:83:10:08:00:40:00:0d:10
=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 0
  Interface: MPLS-Remote-Lfa2   Protocol: TAG
  mtu:17940, flags:0x40, fixups:0x0, encap_len:0
  Handles (adj_id:0xf80002e8) (PI:0x10da2150) (PD:0x130de608)
  Rewrite Str:

  HW Info:
    FID index: 0x00008ca8    EL3 index: 0x0000101c    EL2 index: 0x00000000
    El2RW    : 0x00000003    MET index: 0x00004024    EAID     : 0x0001d7cb
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: 00:00:00:00:00:00:00:00:00:00:00:00

=== Label OCE ===
  Label flags: 4
  Num Labels: 1
Num Bk Labels: 1
  Out Labels: 37
  Out Backup Labels: 37
```

```
  Next OCE Type: Adjacency; Next OCE handle: 0x12943a00
=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 30.1.1.1
  Interface: GigabitEthernet0/3/3   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x0000378e) (PI:0x10909738) (PD:0x12943a00)
  Rewrite Str: c8:f9:f9:8d:01:b3:c8:f9:f9:8d:04:33:88:47

  HW Info:
    FID index: 0x00008c78    EL3 index: 0x0000101c    EL2 index: 0x00000000
    El2RW    : 0x00000109    MET index: 0x0000400e    EAID     : 0x0001cf4b
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: c8:f9:f9:8d:01:b3:08:00:40:00:0d:33
```

show mpls l2transport detail

The following is sample output from the **show mpls l2transport detail** command:

```
Router# show mpls l2transport vc 2000 detail

Local interface: VFI Test-1990 vfi up
  Interworking type is Ethernet
  Destination address: 192.0.2.1, VC ID: 2000, VC status: up
    Output interface: Te0/1/0, imposed label stack {0 2217}
    Preferred path: not configured
    Default path: active
    Next hop: 192.51.100.22
  Create time: 1d08h, last status change time: 1d08h
    Last label FSM state change time: 1d08h
  Signaling protocol: LDP, peer 192.0.51.1:0 up
    Targeted Hello: 192.51.100.2(LDP Id) -> 192.51.100.200, LDP is UP
    Graceful restart: configured and enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
```

Verifying Tunnel Interfaces Created by OSPF IPv4 Remote LFA IPFRR

SUMMARY STEPS

1. **enable**
2. **show ip ospf fast-reroute remote-lfa tunnels**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip ospf fast-reroute remote-lfa tunnels** **Example:** `Device# show ip ospf fast-reroute remote-lfa tunnels`	Displays information about the OSPF per-prefix LFA FRR configuration.

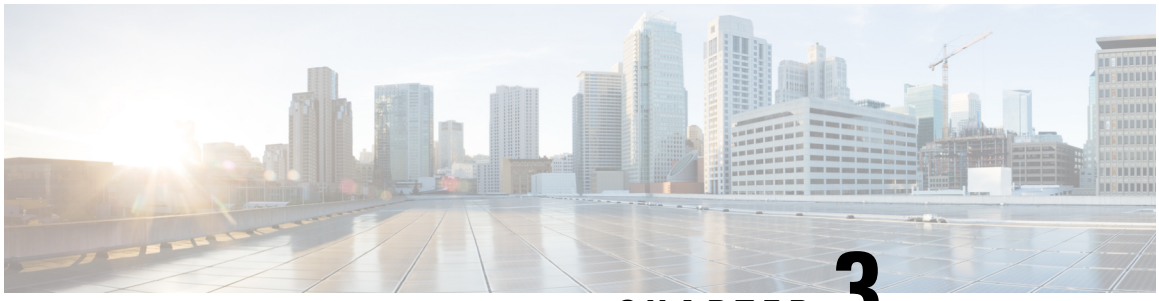
Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Multiprotocol Label Switching Command Reference

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 3

Policy-Based Routing

Note This feature is not applicable on the Cisco RSP3 module.

The Policy-Based Routing feature is a process whereby a device puts packets through a route map before routing the packets. The route map determines which packets are routed next to which device. Policy-based routing is a more flexible mechanism for routing packets than destination routing.

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Information About Policy-Based Routing

Policy-Based Routing

Policy-based routing is a process whereby the device puts packets through a route map before routing them. The route map determines which packets are routed next to which device. You might enable policy-based routing if you want certain packets to be routed in a certain way other than the obvious shortest path. Possible applications for policy-based routing are to provide equal access, protocol-sensitive routing, source-sensitive

routing, routing based on interactive versus batch traffic, and routing based on dedicated links. Policy-based routing is a more flexible mechanism for routing packets than destination routing.

To enable policy-based routing, you must identify which route map to use for policy-based routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met.

To enable policy-based routing on an interface, indicate which route map the device should use by using the **ip policy route-map** *map-tag* command in interface configuration mode. A packet arriving on the specified interface is subject to policy-based routing except when its destination IP address is the same as the IP address of the device's interface. This **ip policy route-map** command disables fast switching of all packets arriving on this interface.

To define the route map to be used for policy-based routing, use the **route-map** *map-tag* [**permit**] [*sequence-number*] global configuration command.

To define the criteria by which packets are examined to learn if they will be policy-based routed, use the **match ip address** {*access-list-number* | *access-list-name*} command or both in route map configuration mode. No match clause in the route map indicates no packet match.

To display the cache entries in the policy route cache, use the **show ip cache policy** command.

Note PBR is supported only in a video template.

Restrictions for Policy-Based Routing

- The following command is not supported:

```
ip local policy route-map <route-map_name>
```

Note Local Policy based routing is not supported.

How to Configure Policy-Based Routing

Configuring Policy-Based Routing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sdm prefer video**
4. **ip access-list extended <name>**
5. **permit protocol source [source-wildcard] destination [destination-wildcard]**
6. **exit**
7. **Route-map <route_map_name> permit <sequence_number>**

8. **match ip address <match_criteria_name>**
9. **set ip next-hop <ip_address> set ip vrf <vrf_name> next-hop <ip_address> set vrf <vrf_name>**
10. **exit**
11. **interface type number**
12. **ip policy route-map <route_map_name>**
13. **exit**

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	**sdm prefer video** **Example:** `Router(config)#sdm prefer video`	Configures the video mode. **Note** This requires a reload of the system. The configuration of the following steps will only be effective after the SDM template is changed to video template.
Step 4	**ip access-list extended <name>** **Example:** `Router(config)#ip access-list extended pbr-acl1`	Configures an Extended ACL named "pbr-acl1" and enters extended-acl configuration mode.
Step 5	**permit protocol source [source-wildcard] destination [destination-wildcard]** **Example:** `Router(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 200.0.0.0 0.255.255.255`	Creates a match statement to match the specified source & destination IP address.
Step 6	**exit** **Example:** `Router(config-ext-nacl)#exit`	Returns to global configuration mode.
Step 7	**Route-map <route_map_name> permit <sequence_number>** **Example:** `Router(config)#route-map pbr permit 10`	Creates a Route-map statement named "pbr" for redistributing routes from one routing protocol into another routing protocol or enables policy-based routing and enters route-map configuration mode.

	Command or Action	Purpose
Step 8	**match ip address <match_criteria_name>** **Example:** `Router(config-route-map)#match ip address pbr-acl1`	Defines the match criteria by which packets are examined to learn if they will be policy-based routed.

Step 9	**set ip next-hop <ip_address> set ip vrf <vrf_name> next-hop <ip_address> set vrf <vrf_name>**
	Example:
	`Router(config-route-map)#set ip next-hop 30.0.0.2`
	`Router(config-route-map)#set ip vrf vrf1 next-hop 30.0.0.1`
	`Router(config-route-map)#set vrf vrf1`
		Specifies where to output packets that pass a match clause of a route map for policy routing.

Step 10	**exit** **Example:** `Router(config-route-map)#exit`	Returns to global configuration mode.
Step 11	**interface type number** **Example:** `Router(config)#interface Gi0/0/10`	Configures an interface type and enters interface configuration mode.
Step 12	**ip policy route-map <route_map_name>** **Example:** `Router(config-if)#ip policy route-map pbr`	Identifies a route map to use for policy routing on an interface.
Step 13	**exit** **Example:** `Router(config-if)#exit`	Returns to global configuration mode.

Verifying Policy-Based Routing

Use this command to verify that the SDM template is changed to video template.

show sdm prefer current

```
PE1#show sdm prefer current
The current template is "video" template
```

Use this command to display the cache entries in the policy route cache.

show ip cache policy

```
CE1#show ip policy
Interface      Route map
Gi0/0/10       equal-access
CE1#
```

Configuration Examples for Policy-Based Routing

This section shows sample configuration for Policy-Based Routing.

Example: Policy-Based Routing

The following is a sample configuration for Policy-Based Routing.

```
Device# conf t
Device(config)# access-list 1 permit host 10.1.1.1
Device(config)# access-list 2 permit host 172.17.2.2
Device(config)# exit

Device# conf t
Device(config)# route-map equal-access permit 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip next-hop 172.16.6.6
Device(config-route-map)# exit
Device(config)# route-map equal-access permit 20
Device(config-route-map)# match ip address 2
Device(config-route-map)# set ip next-hop 192.168.7.7
Device(config-route-map)# exit
Device(config)#exit

Device# conf t
Device(config)# interface GigabitEthernet0/0/2
Device(config-if)# ip policy route-map equal-access
Device(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
IP routing protocol-independent commands	Cisco IOS IP Routing: Protocol-Independent Command Reference

Technical Assistance

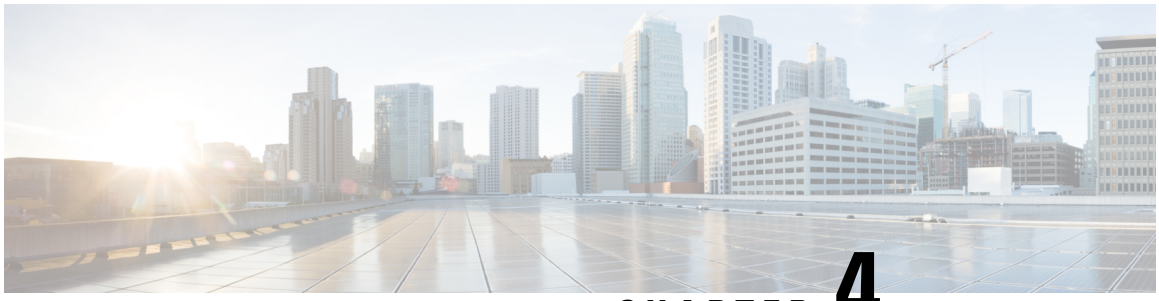
Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools 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 Policy-Based Routing

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 Policy-Based Routing

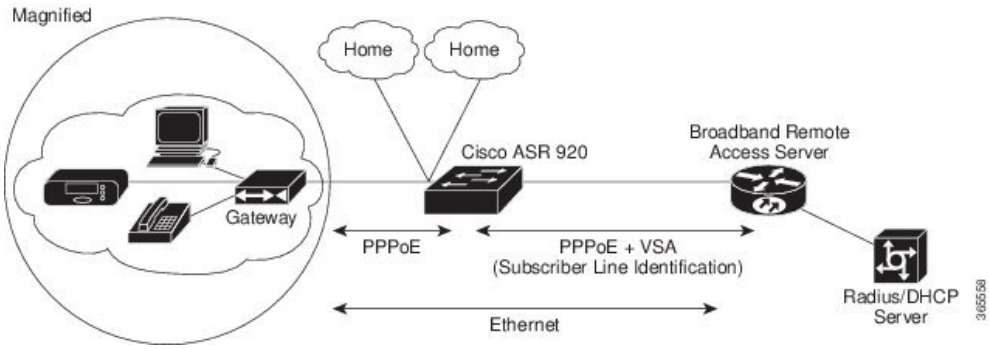


CHAPTER 4

PPPoE Intermediate Agent

Point-to-point protocol over Ethernet intermediate agent (PPPoE IA) is placed between a subscriber and broadband remote access server (BRAS). PPPoE IA helps the service provider BRAS to distinguish between end hosts connected over Ethernet and an access device. The topology of a typical PPPoE implementation is shown in the figure below.

Figure 7: PPP in an Ethernet Scenario



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 Toolkit 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 at the end of this module.

Information About PPPoE Intermediate Agent

On the access switch, PPPoE IA enables subscriber line identification by appropriately tagging Ethernet frames of different users. The tag contains specific information such as, which subscriber is connected to the switch and ethernet flow point (EFP).

PPPoE IA acts as mini security firewall between host and BRAS by intercepting all PPPoE Active Discovery (PAD) messages on a per-port per-EFP basis. It provides specific security feature such as, verifying the intercepted PAD message from untrusted port, performing per-port PAD message rate limiting, inserting and removing VSA Tags into and from PAD messages respectively.

Prerequisites for PPPoE Intermediate Agent

- Interface and per-Bridge Domain(per-BD) based PPPoE IA configurations take effect only when the PPPoE IA feature is enabled globally. Discovery packets are switched or bridged if PPPoE IA is disabled globally.
- PPPoE IA feature supports global/per-port/per-BD based format configuration for generating the circuit-id and remote-id. Choose the appropriate option to meet the requirements.
- To configure a large number of intermediate agent devices for PPPoE IA, use the **pppoe intermediate-agent** command for automatically generating subscriber-line information in the VSA tag by the feature.
- Enable PPoE IA globally, per-Interface and per-BD.

Restrictions for PPPoE Intermediate Agent

- PPPoE IA is not supported on routed interfaces.
- PPPoE IA is not supported on Port-Channel.
- You can enable either PPPoE IA or PPPoE client on the device. You can not have PPPoE IA and PPPoE client on the same device.
- More than 6000 PPPoE sessions are not supported in the device acting as an intermediate agent.
- PPoE IA is only supported on physical interface and Bridge Domain.
- BRAS connected ports are configured as trusted and Host connected port as untrusted.
- When PPPoE IA is enabled globally on the device, the discovery packets received on the Interface, which has PPPoE IA disabled, is dropped.
- Circuit-id and remote-id is configured globally, at interface or at the Bridge Domain level. PPPoE IA uses this to create tag in the following way:
    - If PPoE IA is enabled per-BD, the circuit-id and remote-id configured for that BD is used. If not global values are used.

- If PPoE IA is enabled per-interface, the circuit-id and remote-id configured for that interface is used. If not global values are used.

How to Configure PPPoE Intermediate Agent

The following tasks describe how to configure PPPoE IA on a device:

Enabling or Disabling PPPoE IA on a Device

To enable or disable PPPoE IA globally on the device, complete the following steps:

```
enable
configure terminal
pppoe intermediate-agent
end
```

Configuring the Access Node Identifier for PPPoE IA

Note If you do not specify the access node identifier of the switch, the value is automatically set as 0.0.0.0.

```
enable
configure terminal
pppoe intermediate-agent format-type access-node-id string switch123
end
```

Configuring the Generic Error Message for PPPoE IA

Note PPPoE IA sends a generic error message only on specific error condition. If you do not specify **string** {*message*}, the error message is not added.

```
enable
configure terminal
pppoe intermediate-agent format-type generic-error-message string
end
```

Configuring the Identifier String, Option, and Delimiter for PPPoE IA

The **pppoe intermediate-agent format-type identifier-string string circuit1 option** command has the following options

- pv Port + Vlan
- sp Slot + Port
- spv Slot + Port + Vlan
- sv Slot + Vlan

```
enable
configure terminal
pppoe intermediate-agent format-type identifier-string string circuit1 option spv delimiter
 :
end
```

Enabling or Disabling PPPoE IA on an Interface

Note This setting applies to all frames passing through this interface, regardless of the EFP to which they belong. By default the PPPoE IA feature is disabled on all interfaces. You need to run this command on every interface that requires this feature.

Before You Begin

You must enable PPPoE IA on the device in the global configuration mode.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent
end
```

Enabling or Disabling PPPoE IA on BD

PPPoE IA can be configured to add specific information as part of subscriber identification. This can be configured on a per-port and per-port-per-bridge domain basis. When specific packets received on a particular Bridge-domain need to be differentiated with other packets received on that interface.

To enable or disable PPPoE IA on BD, complete the following steps:

Before You Begin

You must enable PPPoE IA on the device in the global configuration mode.

```
enable
configure terminal
interface GigabitEthernet 0/1/1
pppoe intermediate-agent bridge-domain 40
end
```

Configuring PPPoE IA Circuit-ID on an Interface

You can configure Circuit-ID on interface level. The PADI, PADR and PADT packets (PPPoE Discovery packets) received on this physical interface gets IA-tagged using the configured circuit-id using the **pppoe intermediate-agent format-type circuit-id string word** command, irrespective of the Bridge Domain (BD). This command over-writes global level circuit-id configuration or automatic generation of circuit-id by the Switch.

This parameter is not set by default.

Note If BD is enabled with PPPoE IA, BD level circuit-id configuration overwrites all other circuit-id configuration, for the packets that are received on that particular BD.

To configure the circuit-ID on an interface, complete the following steps:

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent format-type circuit-id string root
end
```

Configuring PPPoE IA Circuit-ID on BD

This configuration overrides the circuit-id configuration specified at interface or global level. The packets received on the specified bridge-domain gets the PPPoE IA tag with configured circuit-id. By default the **pppoe intermediate-agent bridge-domain <bridge-domain_num> circuit-id {string {WORD}}** command is not configured.

Before You Begin

You must enable PPPoE IA globally and on particular BD.

To configure the circuit-ID on BD, complete the following steps:

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent bridge-domain 50 circuit-id ct1
end
```

Configuring PPPoE IA Remote-ID on an Interface

You can configure remote-id on interface level. The PADI, PADR and PADT packets (PPPoE Discovery packets) received on this physical interface gets IA-tagged using the configured remote-id using the **pppoe intermediate-agent format-type remote-id string word** command irrespective of the BD. This command over-writes global level remote-id configuration or automatic generation of remote-id by the device.

This parameter is not set by default.

Note If BD is enabled with PPPoE IA, BD level remote-id configuration overwrites all other remote-id configuration, for the packets that are received on that particular BD.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent format-type remote-id string granite
end
```

Configuring PPPoE IA Remote-ID on BD

This configuration overrides the remote-id configuration specified at interface/global level and the packets received on the specified bridge-domain, will get PPPoE IA tag with remote-id configured. By default the **pppoe intermediate-agent bridge-domain <bridge-domain_num> remote-id {string {WORD}}** command is not configured.

Note The default value of remote-id is the router MAC address (for all bridge-domains).

Before You Begin

You must enable PPPoE IA globally and on particular BD.

To configure the remote-ID on BD, complete the following steps:

```
enable
configure terminal
interface GigabitEthernet 0/1/1
pppoe intermediate-agent bridge-domain 50 remote-id RD1
end
```

Configuring PPPoE IA Rate Limiting Setting on an Interface

You can limit the rate (packets per second) at which PPPoE discovery packets (PADI, PADO, PADR, PADS, and PADT) are received on an interface. When the incoming packet rate achieves or exceeds the configured limit, a port enters an error-disabled state and shuts down.

Note This limit applies to the physical interface to counter misbehaving hosts. Even if a single EFP misbehaves on an interface in trunk mode, the entire interface is shut down (error-disabled), bringing down other EFP traffic on the interface.

If you set the limit on the interface that connect the access switch to BRAS, use a higher value since the BRAS aggregates all the PPPoE traffic to the access switch through this interface.

```
enable
configure terminal
interface GigabitEthernet 0/1/1
pppoe intermediate-agent limit rate 30
end
```

Configuring the PPPoE IA Trust Setting on an Interface

Interfaces that connect the device to the PPPoE server are configured as trusted. Interfaces that connect the device to users (PPPoE clients) are untrusted.

This setting is disabled by default.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent
pppoe intermediate-agent trust
end
```

Configuring PPPoE IA Vendor-tag Stripping on an Interface

Vendor-specific tags (VSAs) carry subscriber and line identification information in the packets.

Vendor-tag stripping involves removing the VSAs from PADO, PADS, and PADT packets that are received on an interface before forwarding them to the user.

You can configure vendor-tag stripping on interfaces connected to the PPPoE server.

This setting is disabled by default.

Note BRAS automatically strips the vendor-specific tag off of the PPPoE discovery packets before sending them downstream to the access switch. To operate with older BRAS which does not possess this capability, use the **pppoe intermediate-agent vendor-tag strip** command on the interface connecting the access switch to BRAS

To enable stripping on an interface , complete the following steps:

Before You Begin

1. Enable PPPoE on an interface.
2. Set the PPPoE interface to trust.

```
enable
configure terminal
interface GigabitEthernet 0/0/1
pppoe intermediate-agent vendor-tag strip
end
```

Verifying PPoE IA Configuration

Clearing Packet Counters

Use the following command to clear packet counters for all PPPoE discovery packets (PADI,PADO,PADR,PADS,PADT) on all interfaces (per-port and per-port-per-EFP):

```
Router# clear pppoe intermediate-agent statistics
```

Use the following command to clear packet counters on a selected interface:

```
Router# clear pppoe intermediate-agent statistics interface type typeslot /subslot /port
```

Example:

```
Router# clear pppoe intermediate-agent statistics interface gigabitEthernet 0/0/3
```

Verifying Interface Statistics

Use the following command to view the statistics of all the interfaces on which PPPoEIA is enabled:

```
Router# show pppoe intermediate-agent statistics
```

```
PPPOE IA Per-Port Statistics
---- -----------------

Interface : GigabitEthernet0/0/24
Packets received
 All = 53
 PADI = 17 PADO = 0
 PADR = 17 PADS = 0
 PADT = 19
Packets dropped:
 Rate-limit exceeded = 0
 Server responses from untrusted ports = 0
 Client requests towards untrusted ports = 0
 Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 8 PADO = 0 PADR = 8 PADS = 0 PADT = 9
BD 50: Packets received PADI = 9 PADO = 0 PADR = 9 PADS = 0 PADT = 10
Interface : GigabitEthernet0/0/24
Packets received
 All = 59
 PADI = 0 PADO = 19
 PADR = 0 PADS = 26
 PADT = 14
Packets dropped:
 Rate-limit exceeded = 0
 Server responses from untrusted ports = 0
 Client requests towards untrusted ports = 0
 Malformed PPPoE Discovery packets = 0
BD 40: Packets received PADI = 0 PADO = 12 PADR = 0 PADS = 15 PADT = 7
BD 50: Packets received PADI = 0 PADO = 7 PADR = 0 PADS = 11 PADT = 7
```

Use the following command to view the packet details on an interface:

```
Router# show pppoe intermediate-agent statistics interface type typeslot /subslot /port
```

Example:

```
Router# show pppoe intermediate-agent statistics interface gigabitEthernet 0/0/3
```

```
Interface : Gi 0/0/3
 Packets received
  All = 0
  PADI = 0 PADO = 0
  PADR = 0 PADS = 0
  PADT = 0
 Packets dropped:
  Rate-limit exceeded = 0
  Server responses from untrusted ports = 0
  Client requests towards untrusted ports = 0
  Malformed PPPoE Discovery packets = 0
```

```
BD 40: Packets received PADI = 0 PADO = 0 PADR = 0 PADS = 0 PADT = 0
BD 50: Packets received PADI = 0 PADO = 0 PADR = 0 PADS = 0 PADT = 0
```

Verifying PPPoE IA is Enabled

```
show pppoe intermediate-agent info

PPPoE Intermediate-Agent is enabled

Global access-node-id is default
Global generic error msg is not set
Global identifier-string and delimiter are not set

PPPoE Intermediate-Agent trust/rate is configured on the following Interfaces:

Interface               IA         Trusted    Vsa Strip   Rate limit (pps)
----------------------- --------   -------    ---------   ----------------
GigabitEthernet0/0/10        yes        no         no          unlimited
PPPoE Intermediate-Agent is configured on following bridge domains:
40,50
```

Verifying Configuration for PPPoE IA on an Interface

```
show pppoe intermediate-agent info interface GigabitEthernet 0/0/10

Interface               IA         Trusted    Vsa Strip   Rate limit (pps)
----------------------- --------   -------    ---------   ----------------
Gi 0/0/10         yes        no         no          unlimited
PPPoE Intermediate-Agent is configured on following bridge domains:
40,50
```

Troubleshooting Tips

The following debug commands can help you troubleshoot an improper PPPoE intermediate agent configuration and its related features:

- **debug pppoe intermediate-agent packet**—Displays the contents of a packet received in the software: source and destination MAC address of Ethernet frame, code, version and type of PPPoE Discovery packet and a list of TAGs present.
- **debug pppoe intermediate-agent event**—Provides debugging information about PPPoE events.
- **debug radius**—Generates a report that includes information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

Configuration Examples

Configuration Example for PPPoE IA on an Interface

```
enable
configure terminal
```

```
interface GigabitEthernet0/0/1
no ip address
media-type rj45
negotiation auto
pppoe intermediate-agent format-type circuit-id string cktid10
pppoe intermediate-agent format-type remote-id string rmtid10
pppoe intermediate-agent
service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 40
!
end
```

Configuration Example for PPPoE IA on a Bridge Domain Interface

```
enable
configure terminal
interface GigabitEthernet0/0/1
no ip address
media-type rj45
negotiation auto
pppoe intermediate-agent bridge-domain 40 circuit-id string cktid-20
pppoe intermediate-agent bridge-domain 40 remote-id string rmtid-20
pppoe intermediate-agent bridge-domain 40
service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 40
!
end
```

Configuration Example with Multiple Bridge Domains

```
enable
configure terminal
interface GigabitEthernet0/0/1
no ip address
media-type rj45
negotiation auto
pppoe intermediate-agent bridge-domain 40 circuit-id string cktid-20
pppoe intermediate-agent bridge-domain 40 remote-id string rmtid-20
pppoe intermediate-agent format-type circuit-id string cktid10
pppoe intermediate-agent format-type remote-id string rmtid10
pppoe intermediate-agent bridge-domain 40
pppoe intermediate-agent
service instance 1 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 40
!
service instance 2 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
!
end
```

In this example:

- the packet received on bd 40 will have circuit and remote id as cktid-20 and rmtid-20 respectively

- the packet received on bd 30 will have circuit & remote id as cktid-10 and rmtid-10 respectively

Additional References for PPPoE Intermediate Agent

The following sections provide references related to the PPPoE IA feature.

MIBs

MIB	MIBs link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

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 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/cisco/web/support/index.html