IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE 16 (Cisco ASR 920 Series)

First Published: 2017-06-09

Last Modified: 2020-07-01

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 1

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.

New and Changed Information

Table 1: New and Changed Features for Loop-Free Alternate Fast Reroute

Feature	Description	Changed in Release	Where Documented
Loop-Free Alternate Fast Reroute with L2VPN	This feature introduces loop-free alternate (LFA) fast reroute (FRR) support for Layer 2 VPN (L2VPN) and Virtual Private Wire Services (VPWS) to minimize packet loss due to link or node failure.	Cisco IOS XE Release 3.9S	Information About Loop-Free Alternate Fast Reroute, on page 3

Feature	Description	Changed in Release	Where Documented
BFD Triggered FRR	This feature introduces the support fot loop-free alternate fast reroute(LFAFRR) and Remote loop-free alternate fast reroute(RLFAFRR) triggered via Bi-Directional Forwarding Detection(BFD) Mechanisms. A BFD fall-over will trigger LFAFRR and RLFAFRR in this case	Cisco IOS XE Release 3.9S	Information About Loop-Free Alternate Fast Reroute, on page 3
LFA FRR and Remote Loop-Free Alternate Fast Reroute with TDM and ATM psuedowires	LFA FRR and remote LFA FRR is supported for TDM and ATM pseudowires	Cisco IOS XE Release 3.10S	Remote LFA FRR for TDM and ATM Psuedowires, on page 6
Remote LFA FRR with ECMP Support	This feature introduces LFAFRR and remote LFAFRR support when ECMP links are present in core.	Cisco IOS XE Release 3.10S	Supported Information, on page 4
LFA FRR and Remote Loop-Free Alternate Fast Reroute with Virtual Private LAN Service (VPLS)	LFA FRR and remote LFA FRR is supported with VPLS	Cisco IOS XE Release 3.10S	Remote LFA FRR with VPLS, on page 6
Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC) feature and the LFA FRR integration	Both BGP PIC and LFA FRR can be configured together on the router.	Cisco IOS XE Release 3.10S	Benefits of Loop-Free Alternate Fast Reroute, on page 4
LFA FRR and Remote LFA FRR over bridge domain interfaces (BDI).	LFA FRR and remote LFA FRR is suppported over BDI interfaces	Cisco IOS XE Release 3.11S	LFA FRR and Remote LFA FRR over Bridge Domains Interfaces, on page 4
BGP PIC support over FRR for BDI interfaces).	BGP PIC is supported for bridge domain interfaces (BDI) with FRR	Cisco IOS XE Release 3.11S	Border Gateway Protocol (BGP) Prefix-Independent Convergence (PIC) and LFA FRR Integration, on page 6

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.
- 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.
- 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 7.

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.

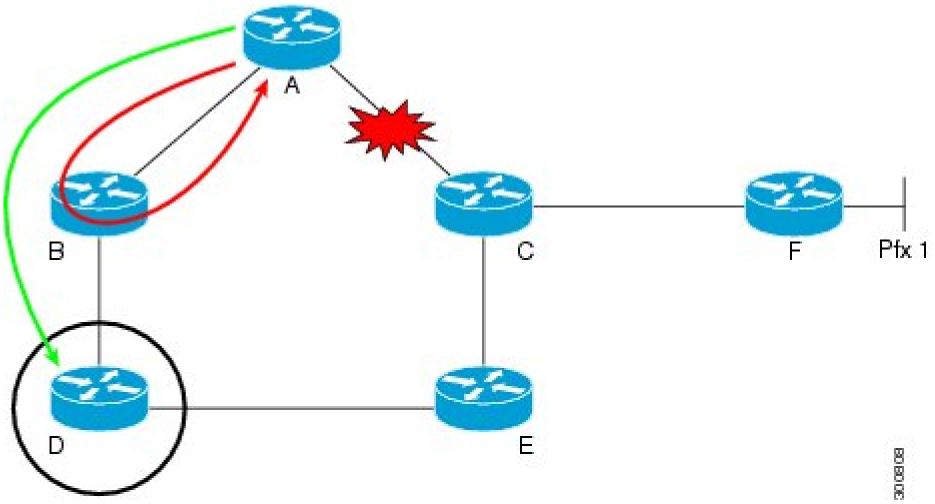
The IPv4 LFA FRR feature uses the following repair paths:

- 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 1: 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).

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 7.

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 7.

Configuring IS-IS Remote Loop-Free Alternate Fast Reroute

The following additional configurations are mandatory:

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

Procedure

	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.

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.

	Command or Action	Purpose
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.

Procedure

	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.

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**router 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

Procedure

	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.

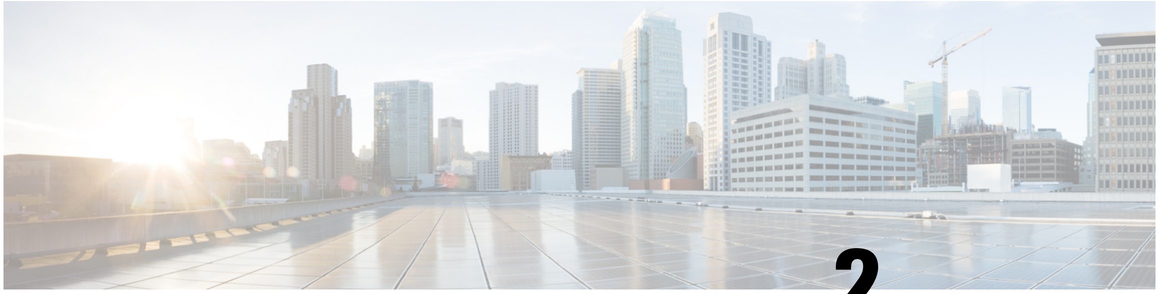
Additional References

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 2

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 ascertain if they will be policy-based routed, use the **match ip address** {*access-list-number* | *access-list-name*} [*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 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.

- The following ACL statement is not supported:

```
permit ip any any
```

  Note Use a specific prefix match for policy-based routing to work.

- The router does not support deny access control entries (ACE) in the access-lists when configured under route maps.
- If there is no match criteria in the route map, the traffic cannot be enabled for policy-based routing.

How to Configure Policy-Based Routing

Configuring Policy-Based Routing

Procedure

	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:**	Creates a Route-map statement named "pbr" for redistributing routes from one routing protocol into another routing protocol or

	Command or Action	Purpose
	`Router(config)#route-map pbr permit 10`	enables policy-based routing and enters route-map configuration mode.
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 3

Segment Routing—IS-IS v4 node SID

The Segment Routing—ISIS v4 node SID feature provides support for segment routing on Cisco Intermediate System-to-Intermediate System (IS-IS) networks.

Information About Segment Routing IS-IS v4 Node SID

Segment Routing IS-IS v4 Node SID

Segment Routing relies on a small number of extensions to Cisco Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. There are two levels of configuration required to enable segment routing for a routing protocol instance. The top level segment routing configuration which is managed by segment routing infrastructure component enables segment routing, whereas, segment routing configuration at the router level enables segment routing for a specific address-family of a routing protocol instance. There are three segment routing states:

- SR_NOT_CONFIGURED
- SR_DISABLED
- SR_ENABLED

Segment routing configuration under the IGPs is allowed only if the SR state is either SR_DISABLED or SR_ENABLED. The SR_ENABLED state indicates that there is at least a valid SRGB range reserved through the MFI successfully. You can enable segment routing for IGPs under the router configuration sub mode, through commands. However, IGP segment routing are enabled only after the global SR is configured.

The SR_ENABLED is a necessary state for any protocol to enable SR, however, it is not a sufficient for enabling SR for a protocol instance. The reason being that the IS-IS still does not have any information about segment routing global block (SRGB) information. When the request to receive information about the SRGB is processed successfully, the IS-IS SR operational state is enabled.

Segment Routing requires each router to advertise its segment routing data-plane capability and the range of MPLS label values that are used for segment routing in the case where global SIDs are allocated. Data-plane capabilities and label ranges are advertised using the SR-capabilities sub-TLV inserted into the IS-IS Router Capability TLV-242 that is defined in RFC4971.

ISIS SR-capabilities sub TLV includes all reserved SRGB ranges. However, the Cisco implementation supports only one SRGB range. The supported IPv4 prefix-SID sub TLV are TLV-135 and TLV-235.

How to Configure Segment Routing —IS-IS v4 Node SID

Configuring Segment Routing

Before you begin

Before configuring IS-IS to support segment routing you must first configure the segment routing feature in global configuration mode.

Procedure

	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	**segment-routing mpls** **Example:** `Device(config-sr)# segment-routing mpls`	Enables the segment feature using the MPLS data plane.
Step 4	**connected-prefix-sid-map** **Example:** `Device(config-srmpls)# connected-prefix-sid-map`	Enters a sub-mode where you can configure address-family specific mappings for local prefixes and SIDs.
Step 5	**address-family ipv4** **Example:** `Device(config-srmpls-conn)# address-family ipv4`	Specifies IPv4 address prefixes.
Step 6	**1.1.1.1/32 index 100 range 1** **Example:**	Associates SID 100 with the address 1.1.1.1/32.

	Command or Action	Purpose
	`Device(config-srmpls-conn-af)# 1.1.1.1/32 100 range 1`	
Step 7	**exit-address-family** **Example:** `Device(config-srmpls-conn-af)# exit-address-family`	Exits the address family.

Configuring Segment Routing on an IS-IS Network

Before you begin

Before you configure segment routing on IS-IS network, IS-IS must be enabled on your network.

Procedure

	Command or Action	Purpose
Step 1	**router isis** **Example:** `Device(config-router)# router isis`	Enables the IS-IS routing protocol and enters router configuration mode.
Step 2	**net network-entity-title** **Example:** `Device(config-router)# net 49.0000.0000.0003.00`	Configures network entity titles (NETs) for the routing instance.
Step 3	**metric-style wide** **Example:** `Device(config-router)# metric-style wide`	Configures the device to generate and accept only wide link metrics.
Step 4	**segment-routing** mpls **Example:** `Device(config-router)# segment-routing mpls`	Configures segment routing operation state.
Step 5	**exit** **Example:** `Device(config-router)# exit`	Exits segment routing mode and returns to the configuration terminal mode.

	Command or Action	Purpose
Step 6	**show isis segment-routing** **Example:** `Device# show is-is segment-routing`	Displays the current state of the IS-IS segment routing.

Example

The following example displays output from the **show isis segment-routing state** command for the segment routing under IS-IS:

```
Device# show isis segment-routing

ISIS protocol is registered with MFI
ISIS MFI Client ID:0x63
Tag 1 - Segment-Routing:
   SR State:SR_ENABLED
   Number of SRGB:1
   SRGB Start:16000, Range:8000, srgb_handle:0x4500AED0, srgb_state: created
   Address-family IPv4 unicast SR is configured
     Operational state:Enabled
```

Configuring Prefix-SID for IS-IS

This section explains how to configure prefix segment identifier (SID) index under each interface.

Before you begin

Segment routing must be enabled on the corresponding address family.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**segment-routing mpls** **Example:** `Device(config)# segment-routing mpls`	Configures segment routing mpls mode.

	Command or Action	Purpose
Step 4	**connected-prefix-sid-map** **Example:** `Device(config-srmpls)# connected-prefix-sid-map`	Enters a sub-mode where you can configure address-family specific mappings for local prefixes and SIDs.
Step 5	**address-family ipv4** **Example:** `Device(config-srmpls-conn)# address-family ipv4`	Specifies the IPv4 address family and enters router address family configuration mode.
Step 6	**1.1.1.1/32 index 100 range 1** **Example:** `Device(config-srmpls-conn-af)# 1.1.1.1/32 100 range 1`	Associates SID 100 with the address 1.1.1.1/32.
Step 7	**exit** **Example:** `Device(config-router)# exit`	Exits segment routing mode and returns to the configuration terminal mode.

Configuring Prefix Attribute N-Flag

By default, a flag called N-flag is set by IS-IS when advertising an SID that is associated with a loopback address. To clear this flag add explicit configuration.

Procedure

	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 loopback3** **Example:** `Device(config)# interface loopback3`	Specifies the interface loopback.

	Command or Action	Purpose
Step 4	**isis prefix n-flag-clear** **Example:** `Device(config-if)# isis prefix n-flag-clear`	Clears the prefix N-flag.

Configuring the Explicit Null Attribute

To disable penultimate-hop-popping (PHP) and add explicit-Null label, explicit-null option needs to be specified. Once the option is given, IS-IS sets the E flag in the prefix-SID sub TLV.

By default, a flag called E-flag (Explicit-Null flag) is set to 0 by ISIS when advertising a Prefix SID which is associated with a loopback address. If you wish to set this flag add explicit configuration.

Procedure

	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	**segment-routing mpls** **Example:** `Device(config)# segment-routing mpls`	Configures segment routing mpls mode.
Step 4	**set-attributes** **Example:** `Device(config-srmpls)# set-attributes`	Sets the attribute.
Step 5	**address-family ipv4** **Example:** `Device(config-srmpls-attr)# address-family ipv4`	Specifies the IPv4 address family and enters router address family configuration mode.
Step 6	**explicit-null** **Example:**	Enables the explicit-null label.

	Command or Action	Purpose

	`Device(config-srmpls-attr-af)#`
	`explicit-null`	

Step 7	**exit-address-family**
	Example:
	`Device(config-srmpls-attr-af)#`
	`exit-address-family`
		Exits the address family.

Configuration Examples for Segment Routing —IS-IS v4 Node SID

Example: Configuring Segment Routing on IS-IS Network

The following example shows how to configure prefix segment identifier (SID) index under each interface:

```
Device(config)#segment-routing mpls
 Device(config-srmpls)#connected-prefix-sid-map
  Device(config-srmpls-conn)#address-family ipv4
   Device(config-srmpls-conn-af)#10.1.2.2/32 index 2 range 1
  Device(config-srmpls-conn-af)#exit-address-family
 Device(config-srmpls-conn-af)#end
```

Example: Configuring an Explicit Null Attribute

The following is an example of configuring an explicit null attribute:

```
Device(config)# segment-routing mpls
Device(config-srmpls)# set-attributes
 Device(config-srmpls-attr)# address-family ipv4
  Device(config-srmpls-attr-af)# explicit-null
 Device (config-srmpls-attr-af)# exit-address-family
```

Additional References for Segment Routing-IS-IS v4 Node SID

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html
IP Routing ISIS commands	Cisco IOS IP Routing ISIS commands http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

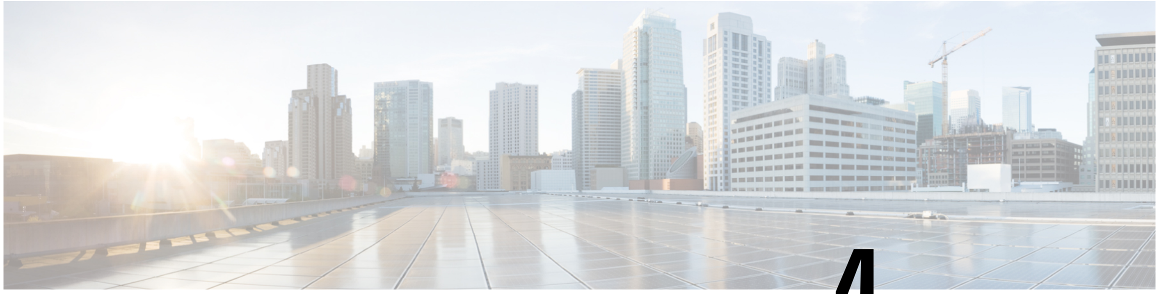
Technical Assistance

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 Segment Routing with IS-IS v4 Node SID

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.

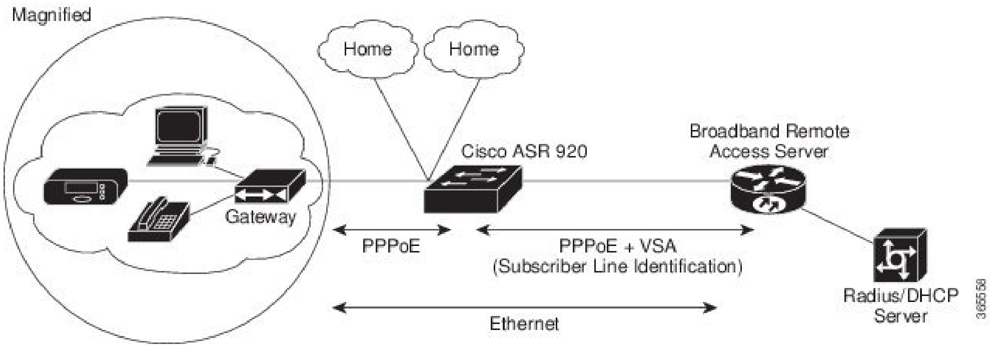


CHAPTER 4

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 2: PPP in an Ethernet Scenario


Magnified
Home
Home
Cisco ASR 920
Broadband Remote Access Server
Gateway
PPPoE
PPPoE + VSA (Subscriber Line Identification)
Radius/DHCP Server
Ethernet
365558

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.

- PPPoE is not supported with L2VPN.

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