



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, on page 1](#)
- [Restrictions for Loop-Free Alternate Fast Reroute, on page 1](#)
- [Information About Loop-Free Alternate Fast Reroute, on page 2](#)
- [How to Configure Loop-Free Alternate Fast Reroute, on page 6](#)
- [Verifying Loop-Free Alternate Fast Reroute, on page 10](#)
- [Verifying Remote Loop-Free Alternate Fast Reroute with VPLS, on page 14](#)
- [Verifying Tunnel Interfaces Created by OSPF IPv4 Remote LFA IPFRR, on page 16](#)
- [Additional References, on page 17](#)

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 6](#).

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.

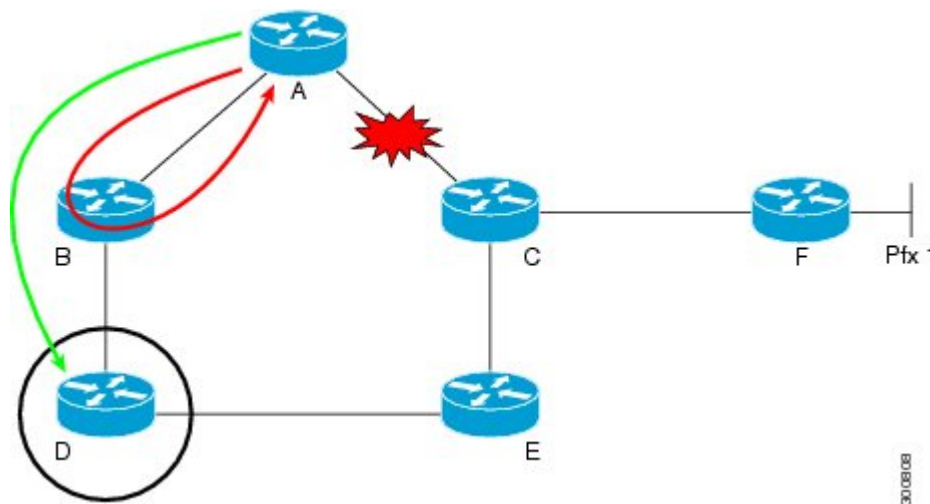
The IPv4 LFA FRR feature uses the following repair paths:

- 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 Pseudowires

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 6](#).

-
-
-

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 6](#).

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 OSPF 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, see [OSPF 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 6](#).

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router isis [area-tag] Example: Device(config)# router isis ipfrr	Enables the IS-IS routing protocol and specifies an IS-IS process. <ul style="list-style-type: none"> • 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: <pre>Device (config-router)# fast-reroute per-prefix level-1 all</pre>	Enables per-prefix FRR. <ul style="list-style-type: none"> • 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: <pre>Device (config-router)# fast-reroute remote-lfa level-1 mpls-ldp</pre>	Configures an FRR path that redirects traffic to a remote LFA tunnel for either level 1 or level 2 packets. <ul style="list-style-type: none"> • 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: <pre>Device (config-router)# end</pre>	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
 - pre-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)

Example: Configuring Remote LFA FRR with VPLS

```

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.

```

!
12 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 10	Enables OSPF routing and enters router configuration mode.
Step 4	fast-reroute per-prefix remote-lfa [area <i>area-id</i>] 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. <ul style="list-style-type: none"> • Use the area <i>area-id</i> 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Device(config)# router ospf 10	Enables OSPF routing and enters router configuration mode.
Step 4	fast-reroute per-prefix remote-lfa [area <i>area-id</i>] maximum-cost <i>distance</i> 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. <ul style="list-style-type: none"> • Use the area <i>area-id</i> 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
```

```
E12RW      : 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
!
```



```

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. <ul style="list-style-type: none"> • 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

