Segment Routing for Cisco ASR 920 Series Aggregation Services Routers

March 31, 2017

Cisco Systems, Inc.
www.cisco.com

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

## CHAPTER 1 Segment Routing Overview 1-1
- How Does Segment Routing Work? 1-1
  - Examples for Segment Routing 1-2
  - Benefits of Segment Routing 1-4
  - Segment Routing Limitations 1-7
- General Limitations of Segment Routing 1-8
- Configuring Segment Routing 1-8
  - Configuring Segment Routing on an IGP Instance 1-9
  - Enabling Advertisement of Mapping Server Prefix Ranges 1-9
  - Disabling the Mapping Server 1-9

## CHAPTER 2 Segment Routing Global Block (SRGB) 2-1
- SRGB Limitations 2-1
- Configuring the SRGB 2-1
  - Reserving a New SRGB 2-1
  - Modifying an Existing SRGB 2-2
- Adjacency Segment Identifiers 2-2
- Prefix Segment Identifiers 2-2
  - Types of Prefix SID Mapping 2-2
  - Configuring Export Prefix SID Mapping 2-3
  - Configuring Connected Prefix SID Mapping 2-3
  - Configuring the Preferred Label 2-3
  - Configuring the Segment Routing Explicit Null 2-4

## CHAPTER 3 Using Segment Routing with IS-IS 3-1
- Restrictions for Using Segment Routing with IS-IS 3-1
- Enabling Segment Routing 3-1
- Enabling Segment Routing for IGPs 3-2
  - Configuring Segment Routing on IS-IS 3-2
  - Prefix-SID Received in LSPs from Remote routers 3-2
  - Limitations 3-3
Segment Routing Adjacency SID Advertisement 3-3
  Multiple Adjacency-SIDs 3-3

Segment Routing Mapping Server (SRMS) 3-4
  Connected Prefix SIDs 3-4
  Configuring IS-IS SRMS 3-4
  Configuring IS-IS SRMS Client 3-4
  Configuring ISIS SID Binding TLV Domain Flooding 3-4

SRGB Range Changes 3-5
  SRGB Deletion 3-5

MPLS Forwarding on an Interface 3-5

Segment Routing and LDP Preference 3-5

Segment Routing-TE 3-6
  Enabling and Disabling SR-TE Announcements 3-6

RLFA LDP and SR 3-6

Topology-Independent LFA 3-7
  Restrictions for the TI-LFA 3-7
  Tie-breaker 3-8
  Interface FRR Tiebreakers 3-9
  Limitations on Tie-Beakers 3-9
  Configuring T1 LFA 3-10
  Configuration Example 3-10
  Verifying the Tie-breaker 3-11
  Verifying the Primary and Repair Paths 3-13
  Verifying the IS-IS Segment Routing Configuration 3-14
  Verifying the IS-IS TI-LFA Tunnels 3-15

Using Segment Routing with OSPF 4-1

Using OSPF with Segment Routing 4-1

Restrictions for Using Segment Routing with OSPF 4-1

Enabling Segment Routing for OSPF 4-2
  Configuring SR on an OSPF Instance 4-2
  Enabling Advertisement of Mapping Server Prefix Ranges 4-2
  Disabling Mapping Server Functionality 4-2
  Interface Mode Prefix Attributes Command 4-3

Using OSPF Fast Reroute with Segment Routing 4-3
  Limitations of TI-LFA on OSPF 4-4
  Enabling and Disabling TI-FRR 4-4
Verifying TI-LFA on OSPF  4-5
Verifying the Configuration of SR on OSPF  4-6
Troubleshooting Segment Routing on OSPF  4-9
Additional References  4-10
  Standards  4-10
  MIBs  4-10
  RFCs  4-10
Segment Routing Overview

Segment routing is a method of forwarding packets on the network based on the source routing paradigm. The forward path is determined before the packet is even sent. The path is encoded in the packet, at the source as a list of segments bearing forwarding instructions. At each hop the top segment, which references the router information base (RIB), is used to identify the next hop. Segments are stacked in order, at the top of the packet header. When the top segment contains the identity of another node, the receiving node uses ECMP to move the packet to the next hop. When the identity is that of the receiving node, the node pops the top segment and performs the task required by the next segment.

Segment routing leverages other interior gateway protocols such as IS-IS, OSPF, and MPLS for efficient and flexible forwarding. Segment routing is a faster and more efficient way of forwarding traffic in the MPLS core network.

To understand the working of segment routing, let’s understand how MPLS traffic engineering works.

How Does Segment Routing Work?

A router in a Segment Routing network is capable of selecting any path to forward traffic, whether it is explicit or Interior Gateway Protocol (IGP) shortest path. Segments represent subpaths that a router can combine to form a complete route to a network destination. Each segment has an identifier (Segment Identifier) that is distributed throughout the network using new IGP extensions. The extensions are equally applicable to IPv4 and IPv6 control planes. Unlike the case for traditional MPLS networks, routers in a Segment Router network do not require Label Distribution Protocol (LDP) and Resource Reservation Protocol - Traffic Engineering (RSVP-TE) to allocate or signal their segment identifiers and program their forwarding information.

Each router (node) and each link (adjacency) has an associated segment identifier (SID). Node segment identifiers are globally unique and represent the shortest path to a router as determined by the IGP. The network administrator allocates a node ID to each router from a reserved block. On the other hand, an adjacency segment identifiers are locally significant and represent a specific adjacency, such as egress interface, to a neighboring router. Routers automatically generate adjacency identifiers outside of the reserved block of node IDs. In an MPLS network, a segment identifier is encoded as an MPLS label stack entry. Segment IDs direct the data along a specified path. There are two kinds of segment IDS:

- Prefix SID—A segment ID that contains an IP address prefix calculated by an IGP in the service provider core network. Prefix SIDs are globally unique. A node SID is a special form of prefix SID that contains the loop-back address of the node as the prefix. It is advertised as an index into the node specific SR Global Block or SRGB.
How Does Segment Routing Work?

- Adjacency SID—A segment ID that contains an advertising router’s adjacency to a neighbor. An adjacency SID is a link between two routers. Since the adjacency SID is relative to a specific router, it is locally unique.

Examples for Segment Routing

The following figure illustrates an MPLS network with five routers using Segment Routing, IS-IS, a label range of 100 to 199 for node IDs, and 200 and higher for adjacency IDs. IS-IS would distribute IP prefix reachability alongside segment ID (the MPLS label) across the network.

Figure 1-1  An MPLS Network with Five Routers Using Segment Routing

In the previous example, any router sending traffic to router E would push label 103 (router E node segment identifier) to forward traffic using the IS-IS shortest path. The MPLS label-swapping operation at each hop preserves label 103 until the packet arrives at E (Figure 2). On the other hand, adjacency segments behave differently. For example, if a packet arrives at Router D with a top-of-stack MPLS label of 203 (D-to-E adjacency segment identifier), Router D would pop the label and forward the traffic to Router E.
Segment identifiers can be combined as an ordered list to perform traffic engineering. A segment list can contain several adjacency segments, several node segments, or a combination of both depending on the forwarding requirements. In the previous example, Router A could alternatively push label stack (104, 203) to reach Router E using the shortest path and all applicable ECMPs to Router D and then through an explicit interface onto the destination (Figure 3). Router A does not need to signal the new path, and the state information remains constant in the network. Router A ultimately enforces a forwarding policy that determines which flows destined to router E are switched through a particular path.
How Does Segment Routing Work?

Figure 1-3  Destination Path of Router E

Benefits of Segment Routing

- Ready for SDN—Segment Routing is a compelling architecture conceived to embrace Software-Defined Network (SDN) and is the foundation for Application Engineered Routing (AER). It strikes a balance between network-based distributed intelligence, such as automatic link and node protection, and controller-based centralized intelligence, such as traffic optimization. It can provide strict network performance guarantees, efficient use of network resources, and very high scalability for application-based transactions. The network uses minimal state information to meet these requirements. Segment routing can be easily integrated with a controller-based SDN architecture. Below figure illustrates a sample SDN scenario where the controller performs centralized optimization, including bandwidth admission control. In this scenario, the controller has a complete picture of the network topology and flows. A router can request a path to a destination with certain characteristics, for example, delay, bandwidth, diversity. The controller computes an optimal path and returns the corresponding segment list, such as an MPLS label stack, to the requesting router. At that point, the router can inject traffic with the segment list without any additional signaling in the network.
In addition, segment lists allow complete network virtualization without adding any application state to the network. The state is encoded in the packet as a list of segments. Because the network only maintains segment state, it can support a large number - and a higher frequency - of transaction-based application requests without creating any burden on the network.

- **Simplified**—
  - When applied to the MPLS data plane, Segment Routing offers the ability to tunnel MPLS services (VPN, VPLS, and VPWS) from an ingress provider edge to an egress provider edge without any other protocol than an IGP (ISIS or OSPF).
  - Simpler operation without separate protocols for label distribution (for example, no LDP or RSVP).
  - No complex LDP or IGP synchronization to troubleshoot.
  - Better utilization of installed infrastructure, for lower capital expenditures (CapEx), with ECMP-aware shortest path forwarding (using node segment IDs).

- **Supports Fast Reroute (FRR)**—Deliver automated FRR for any topology. In case of link or node failures in a network, MPLS uses the FRR mechanism for convergence. With segment routing, the convergence time is sub-50-msec.

- **Large-scale Data Center**-
  - BGP distributes the node segment ID, equivalent to IGP node SID.
  - Any node within the topology allocates the same BGP segment for the same switch.
How Does Segment Routing Work?

- The same benefits are provided as for IGP node SID: ECMP and automated FRR (BGP PIC (Prefix Independent Convergence).
- This is a building block for traffic engineering - SR TE data center fabric optimization.

- Scalable—
  - Avoid thousands of labels in LDP database.
  - Avoid thousands of MPLS Traffic Engineering LSPs in the network.
  - Avoid thousands of tunnels to configure.

- Dual-plane Networks—
  - Segment Routing provides a simple solution for disjointness enforcement within a so-called “dual-plane” network, where the route to an edge destination from a given plane stays within the plane unless the plane is partitioned.
  - An additional SID “anycast” segment ID allows the expression of macro policies such as: "Flow 1 injected in node A toward node Z must go via plane 1” and "Flow 2 injected in node A towards node Z must go via plane 2.”

- Centralized Traffic Engineering—
  - Controllers and orchestration platforms can interact with Segment Routing traffic engineering for centralized optimization, such as WAN optimization.
  - Network changes such as congestion can trigger an application to optimize (recompute) the placement of segment routing traffic engineering tunnels.
  - Segment Routing tunnels are dynamically programmed onto the network from an orchestrator using southbound protocols like PCE.
  - Agile network programming is possible since Segment Routing tunnels do not require signaling and per-flow state at midpoints and tail end routers.

- Egress Peering Traffic Engineering (EPE)—
  - Segment Routing allows centralized EPE.
  - A controller instructs an ingress provider edge and content source to use a specific egress provider edge and specific external interface to reach a destination.
  - BGP “peering” segment IDs are used to express source-routed inter-domain paths.
  - Controllers learn BGP peering SIDs and the external topology of the egress border router through BGP Link Status (BGP-LS) EPE routes.
  - Controllers program ingress points with a desired path.

- Plug-and-Play deployment— Segment routing tunnels are inter-operable with existing MPLS control and data planes and can be implemented in an existing deployment.
Segment Routing Limitations

Figure 1-5  Segment Routing State Flow

Router Bootup
Router State: SR_NOT_CONFIGURED

Router state notified to IGPs

In global config mode, SR is configured
Router(config)# segment-routing

Router State: SR_DISABLED;
IGPs notified of router state
IGPs allow protocol-specific SR configuration, but cannot perform SID-level binding

Is SRGB configured?

No
Router uses default SRGB range

Yes

Is SRGB label range successfully reserved with MFI?

No

Yes

Are all labels in the range available for binding?

No

Yes

Router State: SR_ENABLED
IGPs can perform SID-level binding

Router State: SR_DISABLED;
IGPs notified of router state
IGPs allow protocol-specific SR configuration, but cannot perform SID-level binding.
User can modify SRGB range to avoid the range that is already used by LDP.
• Segment Routing must be globally enabled on the chassis before enabling it on the IGPs, like ISIS or OSPF.
• Segment routing must be configured on the ISIS instance before configuring a prefix SID value.
• The prefix SID value must be removed from all the interfaces under the same ISIS instance before disabling segment routing.

General Limitations of Segment Routing

• Segment routing is supported only on the Cisco ASR 920 and Cisco ASR903 routers with RSP2 module.
• In Cisco IOS XE Release 3.18S, the router supports four MPLS label stacks.
• The following types of services are supported:
  – VPLS
  – Layer 2 VPN
  – Layer 3 VPN
  – Global Prefixes
• To cater to scaled services, it is recommended to use the following values:
  – 1500 IGP
  – 4000 L3VPN
  – 2000 L2VPN virtual circuits
• It is recommended to have the micro-loop avoidance rib-update-delay under IGP configuration as 20000 msec.
• While configuring FRR, carrier-delay down msec 1 must be configured under interface configuration.

Configuring Segment Routing

To configure segment routing

1. Globally enable segment routing:
   ```
   enable
   configure terminal
   segment-routing
   ```
2. Specify the range of MPLS labels to be used to instantiate the segment routing SIDs into MPLS data plane.
   ```
   global block 16-200
   ```
3. Associate SID values with local prefix values.
   ```
   connected-prefix-sid-map
   address-family ipv4
   92.0.0.0/24 index 51 range 1
   2.2.2.2/32 index 2 range 1
   ```
Configuring Segment Routing on an IGP Instance

```
enable
configure terminal
segment-routing
  segment-routing [area N] {mpls | disable}
```

This command enables MPLS on all interfaces and programs the MPLS labels for forwarding.

**Note** If the `area` keyword is specified, segment routing is enabled only on that area.

**Note** The `disable` keyword can be used only if the `area` keyword is specified.

Enabling Advertisement of Mapping Server Prefix Ranges

Global segment routing configuration may contain prefix-to-SID mapping entries for prefixes that are not local to the router. Each of these entries specifies a range of prefixes. Remote mapping entries can be used to find SIDs for prefixes connected to routers that do not support SR and hence not capable of advertising SIDs themselves. This capability is part of SR-LDP inter-working functionality. OSPF learns the ranges configured in the global SR configuration and advertises them in the Extended Prefix Range TLVs.

To permit an OSPF instance to advertise mapping entries configured in the global SR mode, use the following command in router mode.

**Note** By default, this command is disabled. That is, no mapping ranges are advertised by OSPF even if they are configured in the global SR mode.

```
segment-routing prefix-sid-map advertise-local
```

Disabling the Mapping Server

When computing SIDs for prefixes, IGPs consider the prefix ranges received from mapping servers in the network by default. However, if this functionality needs to be disabled, use the following command in router mode. If the SR-LDP feature needs to be disabled, it is done in router-mode:

```
no segment-routing prefix-sid-map receive
```

**Note** This command does not affect processing of 'native' SIDs, that is, those SIDs that are advertised in the Extended Prefix TLVs by routers to whom the prefix is locally connected.
Segment Routing Global Block (SRGB)

The Segment Routing Global Block (SRGB) is the range of label values reserved for Segment Routing (SR) in the Label Switching Database (LSD). These values are assigned as segment identifiers (SIDs) to SR-enabled nodes and have global significance throughout the domain. On SR-capable routers, SRGB is enabled by default so that label values are automatically reserved when the router first boots whether SR is enabled or not. The default SRGB range is 16000 to 23999, and the SRGB can be disabled if SR is not used. You can also specify separate SRGBs for IS-IS and OSPF protocols so long as the ranges do not overlap.

SRGB Limitations

- LSD label values 0-15,999 are reserved.
- The SRGB size cannot be more than 2^16 or 65536.
- The SRGB upper bound value cannot exceed the platform capability.
- The SRGB cannot be configured to be the same value as the default SRGB. So SRGB cannot be configured for 16000 to 23999.

Note
Label values that are not previously reserved are available for dynamic assignment.

Configuring the SRGB

When SR is enabled, but the SRGB is not configured, the system reserves a default label range. After you configure the SRGB, the default label range is released.

When the SR is disabled, the corresponding label range is released and a default label range is reserved.

Reserving a New SRGB

If the SRGB is reserved successfully with the MPLS Forwarding Interface (MFI), then SR is enabled. Otherwise SR is disabled, but the segment routing MPLS global configuration is saved.

If the MFI reserves the SRGB, but there are some dynamically-allocated labels in use in that range, then SR is disabled, the SRGB is released, and the configuration is saved.
### Modifying an Existing SRGB

There can be two scenarios when modifying an SRGB:

1. Extending the upper bound of an existing SRGB. For example,
   - Current range—16000 to 20000
   - New range—16000 to 24000
   The new SRGB range is reserved based on the conditions mentioned in Reserving a New SRGB, page 2-1.

   **Note** In all cases, the new configuration is always saved.

2. The new range is either a disjoint range from the existing SRGB or overlaps with existing SRGB
   In this case, SR is disabled and the previous configuration is deleted. See Figure 1-5

To configure an SRGB:
```
enable
configure terminal
segment-routing mpls
global-block 16000 17000
```

### Adjacency Segment Identifiers

The Adjacency Segment Identifier (adj-SID) is a local label that points to a specific interface and a next hop out of that interface. The router in which the interface is installed automatically assigns an SR SID to the connection using values outside the range of those in its segment routing global block. This SID has local significance only and is not distributed for inclusion in the FIBs of other routers.

**Note** Only IPV4 address-family supports allocating adj-SIDs.

### Prefix Segment Identifiers

A prefix segment identifier (SID) identifies a segment routing tunnel leading to the destination represented by a prefix. The maximum prefix SID value is $2^{16} - 1$.

When a prefix SID value $x$ is configured, the prefix SID translates to a label value equivalent to $x$ + lower boundary of SRGB. For example, if the default SRGB is used, configuring a prefix-SID of 10 for interface Loopback 0 with IPv4 address 1.0.0.1/32 results in assigning the label 16010 to the prefix 1.0.0.1/32.

### Types of Prefix SID Mapping

- Export Prefix SID Mapping
- Connected Prefix SID Mapping
Export Prefix SID Mapping

These are the prefix-sid mappings that the IGPs export to the segment routing nodes through the SID or the Label Binding TLVs, and define the prefix-SID bindings for the network.

Connected Prefix SID Mappings

These are the prefix SID mappings that define the Prefix SID or Node-SID of the interface. Connected prefix SID mappings are created under the mapping-server that the IGPs query to obtain the prefix SID of the interface of an SR node.

Configuring Export Prefix SID Mapping

```
segment-routing mpls
    connected-prefix-sid-map
        address-family ipv4 cisco
        <prefix> / <masklen> [index | absolute] <label> [range <value>]
```

For example.

```
calendar
```

Note
The index and absolute keywords indicate whether the label value entered should be interpreted as an index in the SRGB or as an absolute value. By default, the value is interpreted as an index value. Regardless of the configuration mode, the value is advertised by the protocols as an index value.

Configuring Connected Prefix SID Mapping

```
segment-routing mpls
    mapping-server
        prefix-sid-map
            address-family ipv4 cisco
            <prefix> / <masklen> [index | absolute] <label> [range <value>]
```

Note
The index and absolute keywords indicate whether the label value entered should be interpreted as an index in the SRGB or as an absolute value. By default, the value is interpreted as an index value. Regardless of the configuration mode, the value is advertised by the protocols as an index value.

Configuring the Preferred Label

The Cisco Express Forwarding engine (CEF) can use either the prefix labels stored in the routing information base (RIB) or the labels provided by the label distribution protocol (LDP), for forwarding.

You can set the prefix label or the LDP label as the preferred label by using:

```
segment-routing mpls
    set-attributes
```
address-family ipv4 cisco
sr-label-preferred

The IGPs communicate the preference to the CEF, which in turn processes the forwarding for that prefix accordingly.

### Configuring the Segment Routing Explicit Null

To ensure that quality of service is maintained between the penultimate and last-hop routers, the penultimate router swaps the segment routing label with an explicit null label and forwards the packet to the last-hop router. This swapping preserves the MPLS header attributes for QoS purposes.

```
segment-routing mpls
set-attributes
  address-family ipv4 cisco
  explicit-null
```
Using Segment Routing with IS-IS

We know that segment routing enables a node to select any path (explicit or derived from the computations of the internal gateway protocol’s shortest path). This path is not dependent on a hop-by-hop signaling technique (through LDP or RSVP), but on a set of segments that are advertised by a routing protocol, such as IS-IS or OSPF. These segments act as topological sub-paths that can be combined to form the desired path.

Segment Routing must be enabled before any IGP, such as IS-IS or OSPF, can configure segment routing functionality. Similarly, when segment routing is disabled, all IGP-related configuration is also disabled.

Restrictions for Using Segment Routing with IS-IS

- Effective Cisco IOS XE Release 3.16S, ISIS supports segment routing for IPv4 only.
- Segment routing must be configured at the top level before any routing protocol configuration is allowed under its router configuration sub mode.
- IS-IS protocol SR command is based on per topology (IPv4 address family).
- Only network type = point-to-point is supported.

Enabling Segment Routing

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.
Enabling Segment Routing for IGPs

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.

**Note**

IS-IS protocol SR command is based on per topology (IPv4 address family).

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.

Configuring Segment Routing on IS-IS

This section describes configuring segment routing IPv4 for IS-IS protocol under the router configuration sub mode.

```plaintext
[no] segment-routing mpls
```

**Note**

This command is allowed only when segment routing is configured at the top level.

The following is an example of configuring IS-IS segment routing:

```plaintext
segment-routing mpls
router isis
    net 33.0001.0001.0001.00
    metric-style wide
    segment-routing mpls
    passive-interface Loopback2
```

Prefix-SID Received in LSPs from Remote routers

Prefix SIDs received in a label switched path (LSP) with a reachability TLV (TLV 135 and 235) are downloaded to the routing information base (RIB) if all of the following conditions are met:

- Segment routing is enabled for the topology and address-family
- Prefix-SID is valid
- The local label binding to MFI is successful.
For a prefix-SID received with reachability TLVs (TLV 135 and 235), the label is downloaded through RIB the same way as BGP downloads per prefix VPN labels.

If the path is a remote LFA path, ISIS downloads the path the same way it downloads it before adding the segment routing functionality but does not download any label with this path. This behavior ensures that remote LFA functionality is still supported using LDP.

**Limitations**

- For SIDs that do not fit in the specified SID range, labels are not used when updating the RIB. For cases, where SID does fit in the SID range, but does not fit the next-hop neighbor SID range, remote label associated with that path is not installed.
- Node SIDs received in an LSP with reachability TLVs (TLV 135 and 235) are downloaded to RIB only if segment routing is enabled under the corresponding address-family.
- In case of multiple best next hops, if not all next hops support segment routing, ISIS will treat this instance similar to when mismatched labels are assigned to the same prefix. That is, IS-IS ignores the labels and installs unlabeled paths for all ECMP paths into the global RIB.

**Segment Routing Adjacency SID Advertisement**

Effective with Cisco IOS XE Release 3.17S, IS-IS supports the advertisement of segment routing Adjacency SID. An Adjacency Segment Identifier (Adj-SID) represents a router adjacency in Segment Routing.

A segment routing-capable router may allocate an Adj-SID for each of its adjacencies and an Adj-SID sub-TLV is defined to carry this SID in the Adjacency TLVs. IS-IS adjacencies are advertised using one of the IS-Neighbor TLVs below:

- TLV-22 [RFC5305]
- TLV-23 [RFC5311]

IS-IS allocates the adjacency SID for each IS-IS neighbor only if the IS-IS adjacency state is up and IS-IS segment routing internal operational state is enabled. If an adjacency SID allocation failure is due to out-of-label resource, IS-IS retries to allocate the Adj-SID periodically in a default interval (30 seconds).

**Multiple Adjacency-SIDs**

Effective with Cisco IOS XE Release 3.18S, multiple adjacency-SIDs are supported. For each protected P2P/LAN adjacency, IS-IS allocates two Adj-SIDs. The backup Adj-SID is only allocated and advertised when FRR (local LFA) is enabled on the interface. If FRR is disabled, then the backup adjacency-SID is released. The persistence of protected adj-SID in forwarding plane is supported. When the primary link is down, IS-IS delays the release of its backup Adj-SID until the delay timer expires. This allows the forwarding plane to continue to forward the traffic through the backup path until the router is converged.

Cisco IOS XE Release 3.18S, IS-IS Adj-SID is changed to be per level based since the forwarding plane is unaware of protocol-specific levels. The allocated and advertised backup Adj-SIDs can be displayed in the output of `show isis neighbor detail` and `show isis data verbose` commands.
Segment Routing Mapping Server (SRMS)

Segment Routing Mapping Server (SRMS) allows configuration and maintenance of the Prefix-SID mapping policy entries. Effective with Cisco IOS XE Release 3.17S, the IGPs use the active policy of the SRMS to determine the SID values when programming the forwarding plane.

The SRMS provides prefixes to SID/Label mapping policy for the network. IGPs, on the other hand, are responsible for advertising prefixes to SID/Label mapping policy through the Prefix-SID/Label Binding TLV. Active policy information and changes are notified to the IGPs, which use active policy information to update forwarding information.

Connected Prefix SIDs

Sometimes, a router may install a prefix with a SID that is different than what it advertises to the LSP. For example, if more than one protocol or more than one IGP instance is announcing the same prefix with different SIDs to the SRMS, the SRMS resolves the conflict and announces the winning prefix and SID that may not be the same as the local instance. In that case, the IGP always advertises what it learns from its source LSP although it still tries to install the SID which may be different than what it learns in its LSP. This is done to prevent the IGP from redistributing the SIDs from another protocol or another protocol instance.

Configuring IS-IS SRMS

The following command enables the IS-IS SRMS and allows IS-IS to advertise local mapping entries. IS-IS does not send remote entries to the SRMS library. However, IS-IS uses the SRMS active policy, which is computed based only on the locally configured mapping entries.

```
[no] segment-routing prefix-sid-map advertise-local
```

Configuring IS-IS SRMS Client

By default, the IS-IS SRMS client mode is enabled. IS-IS always sends remote prefix-sid-mapping entries received through LSP, to SRMS. The SRMS active policy is calculated based on both, local and remote mapping entries.

The following command disables the prefix-sid-mapping client functionality.

```
segment-routing prefix-sid-map receive [disable]
```

This command is configured on the receiver side.

Configuring ISIS SID Binding TLV Domain Flooding

By default, the IS-IS SRMS server does not flood SID binding entries within the routing domain. In Cisco IOS XE Release 3.18S, the optional keyword `domain-wide` in the IS-IS SRMS server mode command to enable the SID and Label binding TLV flooding functionality.

```
segment-routing prefix-sid-map advertise-local [domain-wide]
```

The `domain-wide` keyword enables the IS-IS SRMS server to advertise SID binding TLV across the entire routing domain.
SRGB Range Changes

When IS-IS segment routing is configured, IS-IS must request an interaction with the SRGB before IS-IS SR operational state can be enabled. If no SRGB range is created, IS-IS will not be enabled.

When an SRGB change event occurs, IS-IS makes the corresponding changes in its sub-block entries. IS-IS also advertises the newly created or extended SRGB range in SR-capabilities sub-TLV and updates the prefix-sid sub TLV advertisement.

Note

In Cisco IOS XE Release 3.16S only one SRGB range and SRGB extension for the modification are supported.

SRGB Deletion

When IS-IS receives an SRGB deletion event, it looks for an SRGB entry in the IS-IS SRGB queue list. If an SRGB entry does not exist, IS-IS makes sure that there is no pending SRGB created event. If a pending SRGB creation event is found, then IS-IS removes the SRGB creation event, and completes the SRGB delete processing.

If an SRGB entry is found in the IS-IS SRGB queue, IS-IS locks the SRGB, redistributes the RIBs and un-advertises all prefixed-SIDs that have SID value within the pending delete SRGB range, and un-advertises the SRGB range from SR-capabilities sub TLV. Once IS-IS has completed the SRGB deletion processing, it unlocks the SRGB and deletes the SRGB from its SR sub-block entry.

If there is no valid SRGB after the deletion of the SRGB, IS-IS SR operational state becomes disabled.

MPLS Forwarding on an Interface

MPLS forwarding must be enabled before segment routing can use an interface. IS-IS is responsible for enabling MPLS forwarding on an interface.

When segment routing is enabled for a IS-IS topology, or IS-IS segment routing operational state is enabled, IS-IS enables MPLS for any interface on which the IS-IS topology is active. Similarly, when segment routing is disabled for a IS-IS topology, IS-IS disables the MPLS forwarding on all interfaces for that topology.

Segment Routing and LDP Preference

In Cisco IOS XE Release 3.16S, the command `sr-prefer` is used to tell the forwarding interface to prefer using segment routing labels over LDP labels for all prefixes in a topology.
Segment Routing-TE

Segment Routing Traffic Engineering requires the IGP to provide segment routing related information to TE. The information includes SRGB, Adjacency-SID, Prefix-SID, primary and repair paths for all nodes in the topology.

The maximum number of allowed SR-TE tunnels are 510.

Enabling and Disabling SR-TE Announcements

IS-IS announces the SR information to TE when it detects that both, IS-IS SR and TE are enabled for at least one level. IS-IS announce only the information that is obtained from the level for which TE is configured.

Similarly, IS-IS instructs TE to delete all announcements when it detects that SR is not enabled or TE is no longer configured on any level.

RLFA LDP and SR

Consider the following topology.

Figure 3-1 Sample Topology

The traffic flows from A to D. The primary path is A-E-D and the primary next hop interface is Ge0/1. The secondary path is A-B-F-C-D, and C is the PQ node. The repair tunnel ends at PQ node C. The existing RLFA uses LDP TE tunnel for the repair path. When both LDP and SR are enabled, the LDP tunnel is used for RLFA repair path by default unless the segment routing preferred is configured through the \texttt{sr-prefer} command.
Topology-Independent LFA

When the local LFA and remote LFA are enabled, there is a good coverage of the prefixes to be protected. However, for some rare topologies that do not have a PQ intersect node, both local and remote LFA will fail to find a release node to protect the failed link. Furthermore, there is no way to prefer a post-convergence path, as the two algorithms have no knowledge of the post-convergence characteristics of the LFA.

To overcome the above limitation, effective Cisco IOS XE Release 3.18S, topology-independent LFA (TI-LFA) is supported on an SR-enabled network.

In Cisco IOS XE Release 3.18S, TI-LFA supports the following:

- **Link Protection**—The LFA provides repair path for failure of the link.
- **Local LFA**—Whenever a local LFA on the post convergence path is available, it is preferred over TI-LFA because local LFA does not require additional SID for the repair path. That is, the label for the PQ node is not needed for the release node.
- **Local LFA for extended P space**—For nodes in the extended P space, local LFA is still the most economical method for the repair path. In this case, TI-LFA will not be chosen.
- **Tunnel to PQ intersect node**—This is similar to remote LFA except that the repair path is guaranteed on the post convergence path using TI-LFA.
- **Tunnel to PQ disjoint node**—This capability is unique to the TI-LFA in the case when local and remote LFA cannot find a repair path.
- **Tunnel to traverse multiple intersect or disjoint PQ nodes, up to the platform’s maximum supported labels**—TI-LFA provides complete coverage of all prefixes.
- **P2P interfaces for the protected link**—TI-LFA protects P2P interfaces.
- **Asymmetrical links**—The ISIS metrics between the neighbors are not the same.
- **Multi-homed (anycast) prefix protection**—The same prefix may be originated by multiple nodes.
- **Protected prefix filtering**—The route-map includes or excludes a list of prefixes to be protected and the option to limit the maximum repair distance to the release node.
- **Tiebreakers**—A subset of existing tiebreakers, applicable to TI-LFA, is supported.

Restrictions for the TI-LFA

- **IGP throttles timers** that are required for RLFA tunnel are also applicable to SR and SR-TILFA.
- **In Cisco IOS XE Release 3.18S, BFD is not supported with SR and TI-LFA.**
- **Scale values supported for TI-LFA**
  - Global prefixes: 1500
  - L3VPN: 4000 prefixes
  - L2VPN: 2000 virtual circuits
- **SR and TI-LFA are supported on BDI and routed ports.**
- **In Cisco IOS XE Release 3.18S, four MPLS label push is supported. TI-LFA tunnel carries a maximum of two labels and the other two labels are for services.**
**Tie-breaker**

Local and remote LFA use default or user-configured heuristics to break the tie when there is more than one path to protect the prefix. The attributes are used to trim down the number of repair paths at the end of the TI-LFA link protection computation before the load balancing.

Local LFA and remote-LFA support the following tiebreakers:

- **linecard-disjoint**—Prefers the line card disjoint repair path
- **lowest-backup-path-metric**—Prefers the repair path with lowest total metric
- **node-protecting**—Prefers node protecting repair path
- **srlg-disjoint**—Prefers SRLG disjoint repair path
- **load-sharing**—Distributes repair paths equally among links and prefixes

For TI-LFA link protection, the following tiebreakers are supported:

- **linecard-disjoint**—Prefers the line card disjoint repair path.

  **How it works:** When there are two repair paths for a particular prefix, the path that the output port on different line card than that of the primary port is chosen as the repair path.

  The following variant of the linecard-disjoint is supported:
  - **LC disjoint index**—If both the repair paths are on the same line card as that of the primary path, then, both paths are considered as candidates. If one of the path is on a different line card, then that path is chosen as the repair path.

- **srlg-disjoint**—Prefers the SRLG disjoint repair path

  The SRLG ID can be configured for each interface. When there are two repair paths for a prefix, the configured SRLG ID for the repair path is compared with that of the primary path SRLG ID. If the SRLG IDs for the secondary path is different than that of the primary, that path is chosen as the repair path.

  **Note** This policy comes into effect only when the primary path is configured with an SRLG ID.

  The following variant of the srlg-disjoint is supported:
  - **srlg index**—If both the repair paths have the same SRLG ID as that of the primary path, then, both the paths are considered as candidates. If one of the path has a different srlg id, then path is chosen as the repair path.

- **node-protecting**—For TI-LFA node protection, the protected node is removed when computing the post-convergence shortest path. The repair path must direct traffic around the protected node.

  It is possible to configure both node and SRLG protection modes for the same interface or the same protocol instance. In that case, an additional TI-LFA node-SRLG combination protection algorithm is run. The TI-LFA node-SRLG combination algorithm removes the protected node and all members of the interface with the same SRLG group when computing the post-convergence SPT.

  For TI-LFA node protection, SRLG protection, and node-SRLG combination protection, it is likely the coverage for the protected prefixes is small. TI-LFA link protection is also run to provide coverage for the prefixes that not yet covered. However, optimization can be achieved when SRLG protection is enabled with no SRLG group on the interface. In that case, SRLG protection produces the same result as link protection and link protection is skipped. Furthermore, if node-protection is also configured in this case, TI-LFA node-SRLG combination protection produces the same result as node-protection and node-protection is skipped.
Interface FRR Tiebreakers

For TI-LFA node and SRLG protection, interface FRR tiebreakers must also be provided. Existing FRR tiebreakers are configured on a per protocol instance. Because FRR tiebreakers are not specific to TI-LFA, interface FRR tiebreakers are available for all FRR types. When both interface and protocol instance FRR tiebreakers are configured, the interface FRR tiebreakers take precedence over the protocol instance. When interface FRR tiebreakers are not configured, the interface inherits the protocol instance FRR tiebreakers. As with the existing tiebreakers, the priority must be unique among the interface and protocol instance for the tiebreakers.

The following interface FRR tiebreaker commands apply only to the particular interface.

```
isis fast-reroute tie-break [level-1 | level-2] linecard-disjoint priority
isis fast-reroute tie-break [level-1 | level-2] lowest-backup-metric priority
isis fast-reroute tie-break [level-1 | level-2] node-protecting priority
isis fast-reroute tie-break [level-1 | level-2] srlg-disjoint priority
isis fast-reroute tie-break [level-1 | level-2] default
```

Tie-breaker default and explicit tie-breaker on the same interface are mutually exclusive.

The following tie-breakers are enabled by default on all LFAs:

- linecard-disjoint
- lowest-backup-metric
- srlg-disjoint

Effective with Cisco IOS XE Release 3.18S, node-protecting tie-breaker is disabled by default.

Limitations on Tie-Beakers

The following tie-breakers are not applicable for these LFA scheme.

**TILFA:**
- broadcast-interface-disjoint
- downstream
- primary-path
- secondary-path

**RLFA:**
- broadcast-interface-disjoint
- node-protecting
- downstream
- primary-path
- secondary-path
Configuring T1 LFA

TI-LFA is disabled by default. There are two methods to enable TI-LFA:

1. Using protocol enablement—Enable TI-LFA in router isis mode. This enables TI-LFA for all ISIS interfaces. Optionally, use the interface command to exclude the interfaces on which TI-LFA should be disabled.

   For example, to enable TI-LFA for all IS-IS interfaces:
   
   ```
   router isis 1
   fast-reroute per-prefix {level-1 | level-2}
   fast-reroute ti-lfa {level-1 | level-2} [maximum-metric value]
   ```

   The `maximum-metric` option specifies the maximum repair distance which a node is still considered eligible as a release node.

   To disable TI-LFA on a particular interface:
   
   ```
   interface interface-name
   isis fast-reroute ti-lfa protection level-1 disable
   ```

   **Note** The `isis fast-reroute protection level-x` command enables local LFA and is required to enable TI-LFA.

2. Using interface enablement—Enable TI-LFA selectively on each interface

   ```
   interface interface-name
   isis fast-reroute protection {level-1 | level-2}
   isis fast-reroute ti-lfa protection {level-1 | level-2} [maximum-metric value]
   ```

   When both interface and protocol are TI-LFA enabled, the interface configuration takes precedence over the protocol configuration.

Configuration Example

Example 1: In the following example, local LFA is configured with linecard-disjoint and srlg-disjoint tie-breakers. linecard-disjoint is given preference with a lower priority value (10) than the srlg-disjoint (11).

```
router isis access
net 49.0001.2037.0685.b002.00
metric-style wide
fast-flood 10
max-lsp-lifetime 65535
lsp-refresh-interval 65000
spf-interval 5 50 200
prc-interval 5 50 200
lsp-gen-interval 5 5 200
log-adjacency-changes
nsf ietf
segment-routing mpls
fast-reroute per-prefix level-1 all - configures the local LFA
fast-reroute per-prefix level-2 all
fast-reroute remote-lfa level-1 mpls-ldp - enables rLFA (optional)
fast-reroute remote-lfa level-2 mpls-ldp
fast-reroute ti-lfa level-1 - enables TI-LFA
```
microloop avoidance rib-update-delay 15000
bfd all-interfaces

Example 2—Enable TI-LFA node-protecting tie-breaker on all ISIS level-2 interfaces with priority 100. All other tie-breakers are disabled.

router isis
  fast-reroute per-prefix level-2 all
  fast-reroute ti-lfa level-2
  fast-reroute tie-break level-2 node-protecting 100

Example 3—Enable TI-LFA node-protecting tie-breaker with priority 100 and TI-LFA SRLG protection with priority 200 on all IS-IS level-2 interfaces. All other tiebreakers are disabled because the node-protecting tie-breaker is configured.

router isis
  fast-reroute per-prefix level-2 all
  fast-reroute ti-lfa level-2
  fast-reroute tie-break level-2 node-protecting 100
  fast-reroute tie-break level-2 srlg-disjoint 200

Example 3—Enable TI-LFA node-protecting tie-breaker with priority 100 and TI-LFA SRLG protection with priority 200 on all IS-IS level-2 interfaces. All other tiebreakers are disabled because the node-protecting tie-breaker is configured.

router isis
  fast-reroute per-prefix level-2 all
  fast-reroute ti-lfa level-2
  fast-reroute tie-break level-2 node-protecting 100
  fast-reroute tie-break level-2 linecard-disjoint 100

Example 5—Enable TI-LFA node-protecting tie-breaker with priority 200 and linecard-disjoint tie-breaker with priority 100 on all ISIS level-2 interfaces. All other tiebreakers are disabled.

router isis
  fast-reroute per-prefix level-2 all
  fast-reroute ti-lfa level-2
  fast-reroute tie-break level-2 linecard-disjoint 100
  fast-reroute tie-break level-2 node-protecting 200

Verifying the Tie-breaker

To view tiebreakers are enabled on the interface:

Router# show running-configuration | router isis access
Building configuration...

Current configuration : 702 bytes
!
Configuration of Partition - router isis access
!
router isis access
net 49.0001.2037.0685.b002.00
metric-style wide
fast-flood 10
max-lsp-lifetime 65535
lsp-refresh-interval 65000
spf-interval 5 50 200
prc-interval 5 50 200
lsp-gen-interval 5 50 200
no hello padding point-to-point
log-adjacency-changes
nsf cisco
nsf interval 0
segment-routing mpls
fast-reroute per-prefix level-1 all
fast-reroute per-prefix level-2 all
fast-reroute tie-break level-1 linecard-disjoint 12
fast-reroute remote-lfa level-1 mpls-ldp
fast-reroute remote-lfa level-2 mpls-ldp
fast-reroute ti-lfa level-1
bfd all-interfaces
mpls traffic-eng router-id Loopback0
mpls traffic-eng level-1
!
!
end

Similarly, to view the tiebreakers enabled for the router mode:

```
Router# show running-config | isis neighbour
```

<table>
<thead>
<tr>
<th>Tag access:</th>
<th>System Id</th>
<th>Type</th>
<th>Interface</th>
<th>IP Address</th>
<th>State</th>
<th>Holdtime</th>
<th>Circuit Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td></td>
<td>Type</td>
<td>Interface</td>
<td>IP Address</td>
<td>State</td>
<td>Holdtime</td>
<td>Circuit Id</td>
</tr>
<tr>
<td>920-CB1</td>
<td>L1</td>
<td>G10/2/0</td>
<td>1.1.1.1</td>
<td>UP</td>
<td>25</td>
<td>02</td>
<td></td>
</tr>
<tr>
<td>9k-1</td>
<td>L1</td>
<td>G10/2/3</td>
<td>14.0.0.2</td>
<td>UP</td>
<td>27</td>
<td>00</td>
<td></td>
</tr>
</tbody>
</table>

```
903-PE1(config-sr-mpls)#do sh run | sec interface GigabitEthernet0/2/0
interface GigabitEthernet0/2/0
srlg gid 5
srlg gid 10
ip unnumbered Loopback0
ip router isis access
ip ospf network point-to-point
carrier-delay down msec 1
negotiation auto
ipv6 address 10:1::2/64
mpls ip
mpls traffic-eng tunnels
bfd template BFD1
cdp enable
isis network point-to-point
903-PE1(config-sr-mpls)#do sh run | sec interface GigabitEthernet0/2/3
interface GigabitEthernet0/2/3
srlg gid 10
ip address 14.0.0.1 255.255.255.0
ip router isis access
```
Verifying the Primary and Repair Paths

In this example, 1.1.1.1 is the protecting neighbor and 4.4.4.4 is the neighbor on the protecting link.

**Router# show ip cef 1.1.1.1**
1.1.1.1/32
next-hop 1.1.1.1 GigabitEthernet0/2/0 label [explicit-null|explicit-null]() - slot 2 is primary interface
repair: attached-next-hop 24.0.0.2 TenGigabitEthernet0/3/0 - slot 3 is repair interface
next-hop 24.0.0.2 TenGigabitEthernet0/3/0 label [explicit-null|explicit-null]()
repair: attached-next-hop 1.1.1.1 GigabitEthernet0/2/0

**Router# show ip cef 4.4.4.4**
4.4.4.4/32
next-hop 4.4.4.4 GigabitEthernet0/2/3 label [explicit-null|16004]() - slot 2 is primary interface
repair: attached-next-hop 5.5.5.5 MPLS-SR-Tunnel2

**Router# show ip cef 4.4.4.4 int**
4.4.4.4/32, epoch 3, RIB[I], refcnt 6, per-destination sharing
sources: RIB, Adj, LTE
feature space:
IPRM: 0x00028000
Broker: linked, distributed at 4th priority
LFD: 4.4.4.4/32 2 local labels
dflt local label info: global/877 [0x3]
sr local label info: global/16004 [0x1B]
contains path extension list
dflt disposition chain 0x46654200
label implicit-null
FRR Primary
<primary: IP adj out of GigabitEthernet0/2/3, addr 4.4.4.4>
dflt label switch chain 0x46654268
label implicit-null
TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4
sr disposition chain 0x46654880
label explicit-null
FRR Primary
<primary: TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4>
sr label switch chain 0x46654880
label explicit-null
FRR Primary
<primary: TAG adj out of GigabitEthernet0/2/3, addr 4.4.4.4>
subblocks:
Adj source: IP adj out of GigabitEthernet0/2/3, addr 4.4.4.4 464C6620
Dependent covered prefix type adjfib, cover 0.0.0.0/0
ifnums:
GigabitEthernet0/2/3(11): 4.4.4.4
MPLS-SR-Tunnel2(1022)
path list 3B1FC930, 15 locks, per-destination, flags 0x4D [shble, hvsh, rif, hwcn]
path 3C04D5E0, share 1/1, type attached nexthop, for IPV4, flags [has-rpr]
MPLS short path extensions: [rib | lblmrg | srlbl] MOI flags = 0x21 label explicit-null
Verifying the IS-IS Segment Routing Configuration

```
 Router# show isis segment-routing

 ISIS protocol is registered with MFI
 ISIS MFI Client ID:0x63
 Tag Null - Segment-Routing:
  SR State:SR_ENABLED
  Number of SRGB:1
  SRGB Start:14000, Range:4001, srgb_handle:0xE0934788, srgb_state: created
  Address-family IPv4 unicast SR is configured
  Operational state: Enabled

 The command with keyword global-block displays the SRGB and the range for LSPs.

 Router# show isis segment-routing global-block

 IS-IS Level-1 Segment-routing Global Blocks:

 System ID       SRGB Base   SRGB Range
 nevada          20000       4001
 arizona         * 16000     1000
 utah            40000       8000

 The show isis segment-routing prefix-sid-map command with keyword advertise displays the
 prefix-sid maps that the router advertises.

 Router# show isis segment-routing prefix-sid-map adv

 IS-IS Level-1 advertise prefix-sid maps:
 Prefix      SID Index  Range  Flags
 16.16.16.16/32   101  1
 16.16.17.17/32   102  1

 The show isis segment-routing prefix-sid-map command with keyword receive displays the prefix-sid
 maps that the router receives.

 Router #sh isis segment-routing prefix-sid-map receive
 IS-IS Level-1 receive prefix-sid maps:
 Host  Prefix      SID Index  Range  Flags
 utah  16.16.16.16/32  101  1
       16.16.16.17/32  102  1
```
To display the connected-SIDs found in the LSPs and passed to the mapping server component, use the `show isis segment-routing connected-sid` command.

```
Router# show isis segment-routing connected-sid
```

IS-IS Level-1 connected-sids

<table>
<thead>
<tr>
<th>Host</th>
<th>Prefix</th>
<th>SID Index</th>
<th>Range</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>nevada</td>
<td>* 1.1.1.2/32</td>
<td>1002</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2.2.2/32</td>
<td>20</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>100.1.1.10/32</td>
<td>10</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>colorado</td>
<td>1.1.1.3/32</td>
<td>33</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1.1.6/32</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

IS-IS Level-2 connected-sids

<table>
<thead>
<tr>
<th>Host</th>
<th>Prefix</th>
<th>SID Index</th>
<th>Range</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>nevada</td>
<td>1.1.1.2</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1.1.5</td>
<td>70005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>colorado</td>
<td>1.1.1.6</td>
<td>60006</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1.1.2</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1.1.5</td>
<td>70005</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Verifying the IS-IS TI-LFA Tunnels**

```
Router# show isis fast-reroute ti-lfa tunnel
```

Fast-Reroute TI-LFA Tunnels:

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Interface</th>
<th>Next Hop</th>
<th>End Point</th>
<th>Label</th>
<th>End Point Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP1</td>
<td>Et1/0</td>
<td>30.1.1.4</td>
<td>1.1.1.2</td>
<td>41002</td>
<td>nevada</td>
</tr>
<tr>
<td>MP2</td>
<td>Et0/0</td>
<td>19.1.1.6</td>
<td>1.1.1.6</td>
<td>60006</td>
<td>colorado</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.1.2</td>
<td>16</td>
<td>nevada</td>
</tr>
<tr>
<td>MP3</td>
<td>Et0/0</td>
<td>19.1.1.6</td>
<td>1.1.1.6</td>
<td>60006</td>
<td>colorado</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.1.2</td>
<td>16</td>
<td>nevada</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.1.5</td>
<td>70005</td>
<td>wyoming</td>
</tr>
</tbody>
</table>
Using Segment Routing with OSPF

Segment Routing (SR) is a new paradigm of source routing driven by the IGPs and centered on inserting a list of instructions called segments into each packet. SR forwarding can be instantiated by MPLS or IPv6.

OSPF as an IGP propagates the segment information and may either use it internally (for example, to compute Fast Rerouting repair paths) or hand over the segment information to other clients within the router (for example, TE).

Using OSPF with Segment Routing

To provide a base SR functionality, OSPF interacts with several components:

- Segment Routing Application—It handles IGP and instance-independent global commands as well as manages global resources used by the SR such as, block of static MPLS labels available for SR Node SID MPLS instantiation).
- MPLS Forwarding Infrastructure (MFI)—Supports MPLS forwarding table.
- RIBv4—Supports the IPv4 routing table

Restrictions for Using Segment Routing with OSPF

- Segment routing must be configured at the router level before enabling it at the OSPF instance.
- OSPF instance must successfully register itself with both, Segment Routing Application and MFI and retrieve resources that are necessary for operation, such as SRGB range, dynamically-assigned MPLS labels for Adjacency SIDs, and so on.
- If more than one SR router in the network advertises SID for the same prefix, then the SID values and flags must match. If conflicting attributes are found when calculating the SID for the prefix, then all SIDs for the prefix are ignored.
- Network type point-to-point and broadcast are supported.
Enabling Segment Routing for OSPF

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.

SR functionality configurable globally, that is outside the context of any particular IGP instance, include:

- Global enabling SR on the router.
- Specifying the range of MPLS label values to be used to instantiate SR SIDs into MPLS dataplane (SRGB block)
- Associating SID index with local prefix

Configuring SR on an OSPF Instance

After SR is enabled globally on the router, it must be enabled in those OSPF instances that need to run SR.

`segment-routing [area N] {mpls | disable}`

This command is accepted only if SR is already enabled globally. If the `area` keyword is specified then SR is enabled in that area only, otherwise it is enabled in all areas attached to this OSPF instance. The keyword `disable` can be specified only when the `area` keyword is also present.

Enabling this command causes OSPF to originate RI LSA, Extended Prefix and Extended Link LSAs. It enables MPLS on all interfaces in area(s) enabled for SR and programs SR MPLS labels for forwarding.

Enabling Advertisement of Mapping Server Prefix Ranges

Global SR configuration may contain prefix-to-SID mapping entries for prefixes that are not local to the router. Each of these entries specify the range of prefixes. Remote mapping entries can be used to find SIDs for prefixes connected to routers that do not supporting SR and hence, are not capable of advertising SIDs themselves. This is part of SR-LDP inter-working functionality.

OSPF learns the ranges configured in the global SR configuration through the SR application and advertises them in the Extended Prefix Range TLVs.

The following command allows an OSPF instance to advertise mapping entries configured in the global SR mode:

`[no] segment-routing prefix-sid-map advertise-local`

This command is configurable in the router mode. Its default state is `disabled`, That is, no mapping ranges are advertised by OSPF even if they are configured in the global SR mode.

Disabling Mapping Server Functionality

By default, OSPF considers prefix ranges received from mapping servers in the network when computing SIDs for prefixes. This is the core of SR-LDP inter-working label computation. However, if the SR-LDP feature needs to be disabled, use the following command:

`[no] segment-routing prefix-sid-map receive`

Default state of this command is `enabled`. That is, OSPF processes mapping ranges received from mapping servers in the network.
When this command is configured in its non-default form, or the no form, it prohibits OSPF from considering prefix-SID mappings from mapping servers.

**Note**
This command does not affect processing of 'native' SIDs, that is, those SIDs that are advertised in the Extended Prefix TLVs by routers to whom the prefix is locally connected.

### Interface Mode Prefix Attributes Command

Extended Prefix TLV of the Extended Prefix LSA carries flags for the prefix and one of them is N-flag (Node). The N-flag indicates that any traffic sent along to the prefix is destined to the router originating the LSA. This flag typically marks the host routes of the router's loop-back.

By default, OSPF advertises the routes of its loopback with the N-flag. If the IP address of a loopback is not unique (for example, it is part of an anycast address), then OSPF must be configured to not advertise the N-flag with the prefix.

Use the following command to cause OSPF to clear N-flag on all prefixes configured on interface in the interface-mode:

```
ip ospf prefix-attributes n-flag-clear
```

### Using OSFP Fast Reroute with Segment Routing

IP Fast Reroute is a set of techniques that allow rerouting IP traffic around a failed link or a failed node in the network within a very short time (< 50ms). One of the techniques to do this is Loop Free Alternates (LFA). Effective with Cisco IOS XE Release 3.18S, OSPF supports per-prefix directly connected LFA and remote LFA (RLFA).

The per-prefix directly connected LFA provides loop-free alternate path for most triangular topologies, but does not provide good coverage for rectangular or circular topologies. However, the RLFA, which uses MPLS forwarding with LDP signaling for tunneling the rerouted traffic to an intermediate node, extends the IPFRR coverage in ring or rectangular topologies. For each link, RLFA defines the P-Space (the set of nodes reachable from the calculating node without crossing the protected link) and Q-Space (the set of nodes that can reach the neighbor on the protected link without crossing the protected link itself). The nodes that belong to both P- and Q-Spaces are called PQ nodes and can be used as the intermediate nodes for the protected traffic. However, for topologies where the P- and Q-Spaces are completely disjoint, there is still no coverage by RLFA.

Topology Independent Fast Reroute (TI-FRR) is a technique that uses Segment Routing to provide link protection in any topology, assuming the metric on the links in the topology is symmetrical. Even TI-LFA does not guarantee a backup in cases where the bandwidth on a single link is asymmetrical. TI-LFA only considers loop-free paths that are on the post-convergence path that helps you to better plan the capacity of the network.

Segment Routing allows creating a full explicit path through the network, but using such a fully specified path is not scalable in larger topologies due to the number of segments along the path. Specifying the whole path is, however, not necessary, and only a subset of the path is needed to carry the traffic to an intermediate node (release node) which does not loop the traffic back to the protecting node. When the release node is one of the neighbors of S (source or sender node), then we have a directly connected TI-LFA.
Effective with Cisco IOS XE Release 3.18S, an SR Tunnel is constructed to the release node (if remote) and used as the TI-LFA. The tunnel is constructed by explicitly forwarding through a set of one or more repair nodes. The tunnel is created using a SID stack consisting of one SID (Node SID or Adjacency SID) for every repair node and the corresponding label stack is pushed to the protected traffic.

Per Instance Enablement

- TI-LFA can be enabled on a per interface basis. One interface could be configured for LFA, another interface for LFA and RLFA, yet another interface for LFA and TI-LFA and another interface for LFA, RLFA, and TI-LFA.
- TI-LFA backup path is calculated only if TI-LFA protection is enabled on the output interface of the primary path.
- TI-LFA protection is not available for virtual links, sham links, and TE tunnels.
- Backup paths do not use virtual links, sham links, and TE tunnels.

Limitations of TI-LFA on OSPF

- TI-LFA is supported only on OSPFv2.
- TI-LFA only computes TI-LFA candidates that have been found based on a post-convergence path excluding the primary link. That is, TI-LFA only provides link protection. Node protection or SRLG protection is not supported.
- TI-LFA is calculated only if D and repair nodes (P, Q, PQ, or other) in the post-convergence path are segment routing capable. S does not need to be SR capable.
- TI-LFA is calculated only if Repair Nodes (P, Q, PQ, or other) in the post-convergence path have node SID. A node SID can be directly connected or one advertised by Mapping Server (SRMS).
- TI-LFA is restricted to a maximum of two or three segment tunnels, which may be lesser than the maximum labels that can be pushed by the router.
- When S is not SR capable, TI-LFA calculates a 0 or 1 segment LFA along the post-convergence path. The 1-segment LFA uses the LDP label to reach the PQ node in the post-convergence path.
- TI-LFA does not compute backup for virtual link, sham link, or TE tunnel path.
- TI-LFA does not use virtual link, sham link or TE tunnel as backup path.
- TI-LFA does not provide adjacency protection. It only protects prefixes. SR TE may provide protection for adjacency segments. Packets arriving with active adjacency segment do not have TI-LFA protection.
- TI-LFA is calculated only for prefixes having SR prefix SID or node SID.
- TI-LFA does not support Multi Topology Routing (MTR). LFA is calculated only for MTID zero.

Enabling and Disabling TI-FRR

TI-LFA can be enabled on interface, area, and process scopes. By default, TI-LFA is disabled globally. TI-LFA can be enabled using following commands.

```
faster-reroute per-prefix ti-lfa
```
However, when TI-LFA is enabled globally, you have the option to disable it per area level, using following command:

```plaintext
[no] fast-reroute per-prefix ti-lfa [area area disable]
```

This command is accepted even if Segment-Routing is not enabled on the OSPF instance or area. In this case, a TI-LFA backup path is created if the post-convergence path has a PQ node with an LDP label to reach it. That is, RLFA through a post-convergence path.

At the process level:

- `fast-reroute per-prefix ti-lfa [area area disable]`
- `fast-reroute per-prefix enable [area area] prefix-priority {high | low}`
- `fast-reroute per-prefix remote-lfa [area area] maximum-cost cost`
- `fast-reroute per-prefix remote-lfa [area area] tunnel mpls-ldp`
- `fast-reroute per-prefix remote-lfa [area area] tunnel mpls-ldp`
- `fast-reroute per-prefix tie-break attribute [required] index index`

At the interface level:

- `ip ospf fast-reroute per-prefix protection disabled`
- `ip ospf fast-reroute per-prefix candidate disable`
- `ip ospf fast-reroute per-prefix protection ti-lfa [disable]`

### Verifying TI-LFA on OSPF

The following `show command displays the details about TI-LFA configuration:

```plaintext
show ip ospf fast-reroute ti-lfa
```

OSPF Router with ID (13.13.13.13) (Process ID 100)

Microloop avoidance is enabled for protected prefixes, delay 5000 msec

Loop-free Fast Reroute protected prefixes:

<table>
<thead>
<tr>
<th>Area Topology name</th>
<th>Priority</th>
<th>Remote LFA Enabled</th>
<th>TI-LFA Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Base</td>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Repair path selection policy tiebreaks (built-in default policy):

- 0 post-convergence
- 10 primary-path
- 20 interface-disjoint
- 30 lowest-metric
- 40 linecard-disjoint
- 50 broadcast-interface-disjoint
- 256 load-sharing

OSPF/RIB notifications:

- Topology Base: Notification Enabled, Callback Registered

Last SPF calculation started 00:02:42 ago and was running for 8 ms.
Verifying the Configuration of SR on OSPF

- The following `show` command displays information about the new LSAs, such as router information, Extended Prefix and Extended Link LSAs:

  ```
  show ip ospf database opaque-area type ext-limit
  OSPF Router with ID (13.13.13.13) (Process ID 100)
  Type-10 Opaque Area Link States (Area 0)
  LS age: 1378
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 8.0.0.7
  Opaque Type: 8 (Extended Link)
  Opaque ID: 7
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000056
  Checksum: 0xFE8F
  Length: 76
  TLV Type: Extended Link
  Length: 52
  Link connected to : another Router (point-to-point)
  (Link ID) Neighboring Router ID: 12.12.12.12
  (Link Data) Interface IP address: 0.0.0.7
  Sub-TLV Type: Adj SID
  Length : 7
  Flags : L-Bit, V-bit
  MTID : 0
  Weight : 0
  Label : 27

  Sub-TLV Type: Adj SID
  Length : 7
  Flags : L-Bit, V-bit, B-bit
  MTID : 0
  Weight : 0
  Label : 34

  Sub-TLV Type: Local / Remote Intf ID
  Local Interface ID : 7
  Remote Interface ID : 0
  ```

  ```
  show ip ospf database opaque-area type ext-prefix
  OSPF Router with ID (13.13.13.13) (Process ID 100)
  Type-10 Opaque Area Link States (Area 0)
  LS age: 1392
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 7.0.0.0
  Opaque Type: 7 (Extended Prefix)
  Opaque ID: 0
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000055
  Checksum: 0xD156
  Length: 44
  ```
Verifying the Configuration of SR on OSPF

TLV Type: Extended Prefix
Length: 20
Prefix : 4.4.4.4/32
AF : 0
Route-type: Intra
Flags : N-bit

Sub-TLV Type: Prefix SID
Length: 8
Flags : None
MTID : 0
Algo : IGP metric based SPT
SID : 4

**show ip ospf database opaque-area type router-information**

OSPF Router with ID (13.13.13.13) (Process ID 100)

Type-10 Opaque Area Link States (Area 0)

| LS age: 1402 | Options: (No TOS-capability, DC) |
| Link State ID: 4.0.0.0 | LS Type: Opaque Area Link |
| Opaque Type: 4 (Router Information) | Opaque ID: 0 |
| Advertising Router: 4.4.4.4 | LS Seq Number: 80000055 |
| Checksum: 0x7B86 | Length: 52 |

TLV Type: Router Information
Length: 4
Capabilities:
Graceful Restart Helper
Stub Router Support
Traffic Engineering Support

TLV Type: Segment Routing Algorithm
Length: 1
Algorithm: IGP metric based SPT

TLV Type: Segment Routing Range
Length: 12
Range Size: 8000

Sub-TLV Type: SID/Label
Length: 3
Label: 16000

- The following show command displays the interface output, but only if segment routing auto-enabled MPLS forwarding on the interface and SIDs were allocated to that interface

**show ip ospf interface**

Loopback0 is up, line protocol is up
Internet Address 13.13.13.13/32, Interface ID 29, Area 0
Attached via Interface Enable
Process ID 100, Router ID 13.13.13.13, Network Type LOOPBACK, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Enabled by interface config, including secondary ip addresses
Verifying the Configuration of SR on OSPF

Loopback interface is treated as a stub Host
BDI2104 is up, line protocol is up
Interface is unnumbered, Interface ID 40, Area 0
Using address of Loopback0 (13.13.13.13)
Attached via Interface Enable
Process ID 100, Router ID 13.13.13.13, Network Type POINT_TO_POINT, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Can be protected by per-prefix Loop-Free FastReroute
Can be used for per-prefix Loop-Free FastReroute repair paths
Not Protected by per-prefix TI-LFA
Segment Routing enabled for MPLS forwarding
Index 1/3/3, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 8.8.8.8
Suppress hello for 0 neighbor(s)

- The following show command displays the information about segment routing
  - Per-instance state of the feature—whether enabled or disabled, whether operational or not
  - Registration status of OSPF with the SR application and MFI
  - Retrieved SRGB range

    show ip ospf [AS] segment-routing

OSPF Router with ID (13.13.13.13) (Process ID 100)

Global segment-routing state: Enabled

Segment Routing enabled:
Area Topology name Forwarding
0 Base MPLS

SR Attributes
Prefer SR Labels
Do not advertise Explicit Null

Local MPLS label block (SRGB):
  Range: 16000 - 23999
  State: Created

Registered with SR App, client handle: 10
Connected map notifications active (handle 0x18), bitmask 0x1
Active policy map notifications active (handle 0x19), bitmask 0xC
Registered with MPLS, client-id: 100

Bind Retry timer not running
Adj Label Bind Retry timer not running
Adj Protected Label Bind Retry timer not running
The following show command displays information about the SID database for one or for all SIDs. The output displays all prefixes that were advertised with a given SID and highlights which prefixes are local to the router.

```
show ip ospf [AS] segment-routing sid-database [SID]
```

OSPF Router with ID (13.13.13.13) (Process ID 100)

OSPF Segment Routing SIDs

Flags: L - local, N - label not programmed, M - mapping-server

<table>
<thead>
<tr>
<th>SID</th>
<th>Prefix/Mask</th>
<th>Adv-Rtr-Id</th>
<th>Area-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>8.8.8.8/32</td>
<td>8.8.8.8</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>10.10.10.10/32</td>
<td>10.10.10.10</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>(L) 13.13.13.13/32</td>
<td>13.13.13.13</td>
<td>0</td>
</tr>
</tbody>
</table>

This show command provides information only about locally-configured prefixes. Information about prefixes received from other routers is available either through LSDB (show ip ospf database opaque-area) or LRIB (show ip ospf rib local) show commands.

```
show ip ospf [AS] segment-routing local-prefix
```

OSPF Router with ID (13.13.13.13) (Process ID 100)

Area 0:

Prefix: Sid: Index: Interface:
13.13.13.13/32 13 0.0.0.0 Loopback0

**Troubleshooting Segment Routing on OSPF**

Use the following command to debug issues

- `debug ip ospf [AS] segment-routing`
- `debug ip ospf fast-reroute spf`
- `debug ip ospf fast-reroute spf detail`
- `debug ip ospf fast-reroute rib`
- `debug ip ospf fast-reroute rib [access-list]`
## Additional References

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>There are no new standards for this feature.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• —</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>There are no RFCs for this feature.</td>
</tr>
</tbody>
</table>