Segment Routing Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers

First Published: 2016-11-01

Last Modified: 2024-03-27

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

CONTENTS

Preface

The *Segment Routing Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 Series Routers* preface contains these sections:

Changes to This Document

The following table lists the technical changes made to this document since it was first published.

Date	Summary
January 2024	Republished for Cisco IOS XR Release 7.3.6.
March 2019	Republished for Cisco IOS XR Release 6.5.3.
March 2018	Republished for Cisco IOS XR Release 6.4.1.
March 2018	Republished for Cisco IOS XR Release 6.3.2.
September 2017	Republished for Cisco IOS XR Release 6.3.1.
May 2017	Republished for Cisco IOS XR Release 6.1.31.
November 2016	Initial release of this document.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Segment Routing Commands

This chapter describes the commands used to configure and use Segment Routing.

Note All commands applicable to the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

adjacency-sid

To manually allocate an adjacency segment ID (Adj-SID) on an interface, use the **adjacency-sid** command in IS-IS interface address family configuration mode.

adjacency-sid {**index** *adj-sid-index* | **absolute** *adj-sid-value*} [**protected**]

no adjacency-sid {**index** *adj-sid-index* | **absolute** *adj-sid-value*} [**protected**]

Syntax Description

index *adj-sid-index*	Specifies the Adj-SID for each link based on the lower boundary of the SRLB + the index.
absolute *adj-sid-value*	Specifies the specific Adj-SID for each link within the SRLB.
protected	Specify if the Adj-SID is protected. For each primary path, if the Adj-SID is protected on the primary interface and a backup path is available, a backup path is installed. By default, manual Adj-SIDs are not protected.

Command Default

Adjacency SID is not protected.

Command Modes

IS-IS interface address-family configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Segment routing must be configured on the ISIS instance before configuring adjacency SID value.

Manually allocated Adj-SIDs are supported on point-to-point (P2P) interfaces.

Task ID

Task ID	Operations
isis	read, write

Examples

This example shows how to configure an Adj-SID.

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# router isis 100
RP/0/RSP0/CPU0:router(config-isis)# interface GigabitEthernet0/0/0/7
RP/0/RSP0/CPU0:router(config-isis-if)# point-to-point
RP/0/RSP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-if-af)# adjacency-sid index 10
```

Related Commands

Command	Description
segment-routing local-block, on page 86	Configures the segment routing local block (SRLB).

affinity (flexible algorithm)

To configure flexible algorithm definition to include or exclude links with a particular affinity, use the **affinity** command in flexible algorithm configuration mode.

router isis *instance* **flex-algo** *algo* **affinity** [**reverse**] { **include-any** | **include-all** | **exclude-any** } *name1* **,** *name2* **,** . . .

router ospf *process* **flex-algo** *algo* **affinity** { **include-any** | **include-all** | **exclude-any** } *name1* **,** *name2* **,** . . .

Syntax Description

instance	Name of the IS-IS routing process. Maximum number of characters is 40.
process	Name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.
algo	Flex-algo value. An algorithm is a one octet value. Values from 128 to 255 are reserved for user defined values and are used for Flexible Algorithm representation.
reverse	Specifies the IS-IS Flexible Algorithm link admin group (affinity) constraint to include link colors on links in the reverse direction toward the calculating router.
name1	Name of affinity map.

Command Default

No default behavior or values

Command Modes

Flexible Algorithm configuration

Command History

Release	Modification
Releaes 7.9.1	The **reverse** keyword was added for IS-IS.
Release 7.1.1	The **include-any** and **include-all** keywords were added.
Release 6.6.1	This command was introduced.

Example

The following example shows how to configure IS-IS Flex-Algo:

```
Router#configure
Router(config)#router isis 1
Router(config-isis)#flex-algo 128
Router(config-isis-flex-algo)#affinity exclude-any red
Router(config-isis-flex-algo)#affinity include-any blue
Router(config-isis-flex-algo)#exit
Router(config-isis)#flex-algo 129
Router(config-isis-flex-algo)#affinity exclude-any green
```

```
Router(config-isis-flex-algo)#affinity reverse exclude-any green
```

affinity flex-algo

To advertise the affinity on an interface, use the **affinity flex-algo** command in the IS-IS interface configuration mode.

```
affinity  flex-algo { name | [anomaly name] }
```

Syntax Description

name	Name of affinity map.
anomaly	Advertises flex-algo affinity on performance measurement anomaly.

Command Default

No default behavior or values

Command Modes

IS-IS interface configuration

Command History

Release	Modification
Release 7.8.1	This command was modified
Release 6.6.1	This command was introduced.

Example

The following example shows how ISIS advertises affinity FOO for the adjacency over interface GigabitEthernet0/0/0/0.

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#router isis 1
RP/0/RSP0/CPU0:router(config-isis)#interface GigabitEthernet0/0/0/0
RP/0/RSP0/CPU0:router(config-isis-if)#affinity flex-algo FOO
```

With the IOS XR Release 7.8.1, the new optional keyword **anomaly** is introduced to the **interface** submode of **affinity flex-algo**. This keyword option helps to advertise flex-algo affinity on PM anomaly. The following command is used to associate the affinity with an interface:

router isis *instance* **interface** *type interface-path-id* **affinity flex-algo anomaly** *name 1, name 2, …*

router ospf *process* **area** *area* **interface** *type interface-path-id* **affinity flex-algo anomaly** *name 1, name 2, …*

name - name of the affinity-map

You can configure both normal and anomaly values. For the following example, the **blue** affinity is advertised. However, if a metric is received with the anomaly flag set, it will change to **red**:

```
Router# configure
Router(config)# router isis 1
Router(config-isis)#flex-algo 128
Router(config-isis-flex-algo)# interface GigabitEthernet0/0/0/2
```

```
Router(config-isis-flex-algo)# affinity flex-algo blue
Router(config-isis-flex-algo)# affinity flex-algo anomaly red
```

apply-weight ecmp-only bandwidth

To enable Unequal Cost Multipath (UCMP) functionality locally between Equal Cost Multipath (ECMP) paths based on the bandwidth of the local links, use the **apply-weight ecmp-only bandwidth** command in IS-IS interface address family configuration mode.

apply-weight ecmp-only bandwidth

Syntax Description

bandwidth	Enables UCMP functionality locally between ECMP paths based on the bandwidth of the local links.

Command Default

None.

Command Modes

IS-IS interface address-family configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Bandwidth-based local UCMP is performed for prefixes, segment routing Adjacency SIDs, and Segment Routing label cross-connects installed by IS-IS, and is supported on any physical or virtual interface that has a valid bandwidth.

Segment routing must be configured on the ISIS instance before configuring bandwidth-based local UCMP.

Task ID

Task ID	Operations
isis	read, write

Examples

This example shows how to configure bandwidth-based local UCMP.

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# router isis 100
RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-af)# apply-weight ecmp-only bandwidth
```

bgp auto-discovery segment-routing

To configure the BGP Auto-Discovery function for transporting IP VPN multicast traffic, use the **bgp auto-discovery segment-routing** command in multicast routing VRF address family configuration mode. To remove the configuration, use the **no** form of the command.

bgp auto-discovery segment-routing

Syntax Description

This command has no keywords or arguments.

Command Default

The BGP Auto-Discovery function is not enabled.

Command Modes

Multicast routing VRF address family configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

The **bgp auto-discovery segment-routing** command must be enabled on the PE routers, for *default* MDT, *partitioned* MDT and *data* MDT configuration

Example

The following example shows how to enable the BGP MVPN Auto-Discovery function:

```
Router(config)# multicast-routing vrf cust1
Router(config-mcast-cust1)# address-family ipv4
Router(config-mcast-cust1-ipv4)# bgp auto-discovery segment-routing
Router(config-mcast-cust1-ipv4-bgp-ad)# commit
```

bgp best-path sr-policy

To select the best path, backup, or multipath resolving over nexthop using SR policies, use the **bgp best-path sr-policy** command in BGP configuration mode. To remove the configuration, use the **no** form of the command.

bgp best-path sr-policy { **force** | **prefer** }

Syntax Description

force	When force mode is enabled, only SR policy paths are considered for best path calculation.
prefer	When prefer mode is enabled, SR policy paths and eBGP non-color paths are eligible for best path calculation.

Command Default

None.

Command Modes

BGP configuration mode

Command History

Release	Modification
Release 7.5.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to enable the force mode:

```
Router(config)#router bgp 100
Router(config-bgp)#bgp router-id 10.1.1.2
Router(config-bgp)#bgp best-path sr-policy force
```

clear segment-routing local-block discrepancy all

Clears segment routing local block (SRLB) label conflicts.

clear segment-routing local-block discrepancy all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you define a new SRLB range, there might be a label conflict (for example, if labels are already allocated, statically or dynamically, in the new SRLB range). In this case, the new SRLB range will be accepted, but not applied (pending). The previous SRLB range (active) will continue to be in use until one of the following occurs:

- Reload the router to release the currently allocated labels and allocate the new SRLB
- Use the **clear segment-routing local-block discrepancy all** command to clear the label conflicts

Task ID

Task ID	Operation

This example shows how to clear SRLB label conflicts.

```
RP/0/RSP0/CPU0:router(config)# clear segment-routing local-block discrepancy all
```

Related Commands

Command	Description
show segment-routing local-block inconsistencies, on page 123	Displays SRLB label conflicts
segment-routing local-block, on page 86	Configures the SRLB

data-plane

To enable participation of the Flexible Algorithm with segment routing (SR/SRv6) or IP data-planes, use the **data-plane** command in the IS-IS Flexible Algorithm configuration mode.

data-plane segment-routing | ip

Syntax Description

segment-routing	Participateswith the segment routing data-plane.
ip	Participates with the IP data-plane.

Command Default

Segment-routing data-plane is enabled.

Command Modes

IS-IS Flexible Algorithm configuration (config-isis-flex-algo)

Command History

Release	Modification
IOS XR Release 7.6.1	This command was introduced.

Usage Guidelines

To use this command, you must specify a data-plane.

Note If you are enabling participation of the IP Flexible Algorithm, data-plane ip must be enabled.

This example shows how to enable IP data-plane to participate with a Flexible Algorithm:

```
Router(config)#router isis 1
Router(config-isis)#flex-algo 128
Router(config-isis-flex-algo)#data-plane ip
```

explicit-path

Configures a fixed path through the network.

explicit-path name *path_name*

Syntax Description

path_name	Specifies a name for an explicit path.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to specify a path name and enter explicit-path configuration mode:

```
RP/0/RSP0/CPU0:router(config)# explicit-path name ABCD1_Nodes
RP/0/RSP0/CPU0:router(config-expl-path)#
```

Related Commands

Command	Description
index	Determines the order of path selection.

distribute link-state (IS-IS)

To configure filters for IS-IS advertisements to BGP-LS, use the **distribute link-state** command in the IS-IS configuration mode.

distribute link-state [**exclude-external exclude-interarea route-policy** *name*]

Table 1: Syntax Description:

Syntax	Description
exclude-external	Sets filter to exclude information for external prefixes and specify a route-policy name to filter based on a set of destination prefixes.
exclude-interarea	Sets filter to exclude information for interarea prefixes and specify a route-policy name to filter based on a set of destination prefixes.
route-policy*name*	Distributes prefixes based on the route policy name set.

Command Default

BGP-LS is disabled by default.

Command Modes

IS-IS Configuration

Command History

Release	Modification
Release 7.10.1	New keywords under the command **distribute link-state** was introduced.

Example

This example shows how to configure filters for IS-IS advertisements to BGP-LS:

```
Router#config
Router(config)#router isis 1
Router(config-isis)#distribute link-state exclude-external
Router(config-isis)#commit

Router#config
Router(config)#router isis 1
Router(config-isis)#ddistribute link-state exclude-interarea
Router(config-isis)#commit

Router# config
Router(config)# router isis 1
Router(config-isis)#distribute link-state route-policy isis-rp-1
Router(config-isis)#commit
```

encapsulation l2-traffic

To set the traffic-class on the IP header of the outgoing packet in an IPv6 network during L2VPN encapsulation, use the **encapsulation l2-traffic** command in XR Config mode. You must be in **hw-module profile segment-routing srv6 mode** to configure the **encapsulation l2-traffic**, for more information see the example.

encapsulation l2-traffic traffic-class [{ { *traffic-class value* | **propagate** } }]

Syntax Description

traffic-class	Control traffic-class field of SRv6 IPv6 header for inner l2 traffic.
traffic-class value	This specifies the traffic-class value. Range is from 0x0 to 0xff. Traffic-class value must be specified as 2 hexadecimals.
propagate	Propagate traffic-class from incoming packet or frame or use qos-group from input policy-map.

Command Default

The default traffic-class value is 0x0.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.7.1	This command was introduced.

Usage Guidelines

- Reload the line-cards for the following configuration changes.
- See the feature information table for the default mapping:

  VLAN Class of Service CoS Priority Code Point (PCP) to Traffic Class default mapping

CoS value	TC value
0	0
1	32
2	64
3	96
4	128
5	160
6	192
7	224

Task ID

Task ID	Operation
system	read and write

Example

The following example shows how to set the l2-traffic:

```
Router(config)# hw-module profile segment-routing srv6 mode micro-segment format f3216
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# l2-traffic
Router(config-srv6-encap-l2)# traffic-class propagate
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
```

encapsulation l3-traffic

To set the traffic-class on the IP header of the outgoing packet in an IPv6 network during L3VPN encapsulation, use the **encapsulation l3-traffic** command in XR Config mode. You must be in **hw-module profile segment-routing srv6 mode** to configure the **encapsulation l3-traffic**, for more information see the example.

encapsulation l3-traffic **traffic-class** [{ { *traffic-class value* | **propagate** | **policy-map** } }]

Syntax Description

traffic-class	Control traffic-class field of SRv6 IPv6 header for inner l3 traffic.
traffic-class value	This specifies the traffic-class value. Range is from 0x0 to 0xff. Traffic-class value must be specified as 2 hexadecimals.
propagate	Propagate traffic-class from incoming packet or frame or use qos-group from input policy-map.
policy map	Sets the traffic-class DSCP to qos-group that is selected by the input policy-map.

Command Default

The default traffic-class value is 0x0.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.7.1	This command was introduced.

Usage Guidelines

Reload the line-cards for the following configuration changes.

Task ID

Task ID	Operation
system	read and write

Example

The following example shows how to set the l3-traffic:

```
Router(config)# hw-module profile segment-routing srv6 mode micro-segment format f3216
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# l3-traffic
Router(config-srv6-encap-l3)# traffic-class policy-map
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
```

evi (bridge-domain)

To associate an EVI instance with an L2VPN bridge domain or enable ELAN bridged unicast traffic over an SRv6 network, use the **evi** command in the L2VPN bridge domain configuration mode. To disable this feature, use the **no** form of this command.

evi *instance* [**segment-routing srv6**]

Syntax Description

instance	EVI instance that is associated with an L2VPN bridge domain.
segment-routing srv6	(Optional) Specifies that SRv6 is associated with the EVI instance.

Command Default

The EVI instance is not associated with an L2VPN bridge domain.

Command Modes

L2VPN bridge domain configuration.

Command History

Release	Modification
Release 6.2.2	The **evi** command was introduced for MPLS bridging.
Release 7.5.2	The **segment-routing srv6** option was added to the command.

Examples

This example shows how to enable EVPN ELAN bridged unicast traffic over an SRv6 network:

```
Router # configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface Hu0/0/0/0.1
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# evi 1 segment-routing srv6
Router(config-l2vpn-bg-bd-evi-srv6)# commit
```

fast-reroute per-prefix ti-lfa

To enable Topology Independent Loop Free Alternate (TI-LFA) path for SR-TE policies using the IP Fast Reroute (FRR) mechanism, use the **fast-reroute per-prefix ti-lfa** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

fast-reroute per-prefix [**ti-lfa** | **tiebreaker** { **node-protecting** | **srlg-disjoint** } **index** *priority*]
no fast-reroute

Syntax Description

per-prefix	Specifies an alternate path for every prefix on the specified interface.
ti-lfa	Enables link-protecting TI-LFA.
tiebreaker	Enables fast reroute tie-breaker.
node-protecting	Enables node-protecting TI-LFA.
srlg-disjoint	Enables SRLG-protecting TI-LFA.
index *priority*	Specifies the priority of the configured tie-breaker. Priority range is from 1 to 255.

Command Default

FRR is disabled.

Link protection is disabled.

Node-protecting TI-LFA is disabled.

SRLG TI-LFA is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.1.3	This command was introduced.

Usage Guidelines

The goal of TI-LFA is to reduce the packet loss that results while routers converge after a topology change due to a link or node failure. Rapid failure repair (< 50 msec) is achieved through the use of pre-calculated backup paths that are loop-free and safe to use until the distributed network convergence process is completed. The optimal repair path is the path that the traffic will eventually follow after the IGP has converged.

TI-LFA supports the following protection:

- Link protection — The link is excluded during the post-convergence backup path calculation.
- Node protection — The neighbor node is excluded during the post convergence backup path calculation.
- Shared Risk Link Groups (SRLG) protection — SRLG refer to situations in which links in a network share a common fiber (or a common physical attribute). These links have a shared risk: when one link fails, other links in the group might also fail. TI-LFA SRLG protection attempts to find the post-convergence backup path that excludes the SRLG of the protected link. All local links that share any SRLG with the protecting link are excluded.

If the priority associated with the specified tiebreaker is higher than any other tiebreakers, then the specified post-convergence backup path will be selected, if it is available.

Task ID

Task ID	Operations
isis	read, write
ospf	

Examples

The following example shows how to enable FRR on an interface:

```
RP/0/RSP0/CPU0:R1(config)# router isis 1
RP/0/RSP0/CPU0:R1(config-isis)# interface TenGigE0/0/0/2/1
RP/0/RSP0/CPU0:R1(config-isis-if)# point-to-point
RP/0/RSP0/CPU0:R1(config-isis-if)# address-family ipv4 unicast
RP/0/RSP0/CPU0:R1(config-isis-if)# fast-reroute per-prefix
RP/0/RSP0/CPU0:R1(config-isis-if)# fast-reroute per-prefix ti-lfa
RP/0/RSP0/CPU0:R1(config-isis-if)# exit
```

The following example shows how to configure the SRLG-disjoint tiebreaker priority on an interface:

```
RP/0/RSP0/CPU0:R1(config)# router isis 1
RP/0/RSP0/CPU0:R1(config-isis)# interface TenGigE0/0/0/2/1
RP/0/RSP0/CPU0:R1(config-isis-if)# point-to-point
RP/0/RSP0/CPU0:R1(config-isis-if)# address-family ipv4 unicast
RP/0/RSP0/CPU0:R1(config-isis-if)# fast-reroute per-prefix
RP/0/RSP0/CPU0:R1(config-isis-if)# fast-reroute per-prefix ti-lfa
RP/0/RSP0/CPU0:R1(config-isis-if)# fast-reroute per-prefix tiebreaker srlg-disjoint index
100
RP/0/RSP0/CPU0:R1(config-isis-if)# exit
```

hw-module profile segment-routing srv6 mode

To enable Segment Routing over IPv6, use the **hw-module profile segment-routing srv6** command in XR Config mode.

hw-module profile segment-routing srv6 mode { **base** | **micro-segment format 3216** [**path-mtu**] }

Syntax Description

base	Base/F1 (full-length SIDs).
micro-segment format f3216	Micro-segment format F3216 (represents 32-bit block and 16-bit IDs).
base-and-micro-segment-f3216	Enables migration of existing SRv6 SID format1 to SRv6 Micro-SIDs (f3216) formats.
path-mtu	Enables Path MTU discovery for SRv6 profile.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.11.1	The **path-mtu** keyword is introduced.
Release 7.8.1	The option **base-and-micro-segment-f3216** is introduced.
Release 7.7.1	**Mode** keyword is mandatory from release 7.7.1 onwards.
Release 6.6.1	This command was introduced.

Usage Guidelines

You must reload the router for the **hw-module profile segment-routing srv6** to be functional.

Use the mandatory keyword **mode** from Cisco IOS XR Software Release 7.7.1 onwards.

Do not use the keyword **mode** prior to release 7.7.1.

Starting from Release 7.10.1, the SRv6 mode is automatically set to **base-and-micro-segment-f3216 mode** (dual mode) even if you configure the **base** mode. The running configuration would still continue to reflect the user configured mode only.

You can verify the change using the following console log:

```
fia_driver[238]: %FABRIC-FIA_DRVR-6-HW_MOD_PROFILE_AUTO_CONVERTED :
Auto-converting SRv6 hw-module base profile to base-and-micro-segment-f3216 profile
```

For the **path-mtu** keyword, use the following guidelines:

- The SRv6 uSID (F3216) format supports the feature.
- The SRv6 Full-length SID format does not support Path MTU discovery.
- You must configure this feature on the ingress Provider Edge (PE) router.
- SRv6 encapsulation supports the following scenarios:

- IPv4/IPv6 over SRv6
- SRv6-TE
- H insert
- TI-LFA for Single Carrier and Multi Carrier

- L2 services over SRv6 (L2VPN) do not support the feature.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable Segment Routing over IPv6 for base, from release 7.7.1 onwards:

```
Router(config)# hw-module profile segment-routing srv6 mode base
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# l2-traffic
Router(config-srv6-encap-l2)# traffic-class propagate
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
Router(config-srv6-encap-l2)#(config-srv6-encap-l2)# commit
```

The following example shows how to enable Segment Routing over IPv6 for micro-segment format, from release 7.7.1 onwards:

```
Router(config)# hw-module profile segment-routing srv6 mode micro-segment format f3216
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# l3-traffic
Router(config-srv6-encap-l3)# traffic-class policy-map
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
Router(config-srv6-encap-l2)#(config-srv6-encap-l2)# commit
```

The following example shows how to enable Segment Routing over IPv6, prior to release 7.7.1:

```
Router(config)# hw-module profile segment-routing srv6
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# l2-traffic
Router(config-srv6-encap-l2)# traffic-class propagate
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
Router(config-srv6-encap-l2)#(config-srv6-encap-l2)# commit
```

From IOS XR Release 7.8.1, the **hw-module profile segment-routing srv6 mode base-and-micro-segment-f3216** command is used for the in-migration state.

This example shows the in-migration state with SRv6 and configure locator:

```
Router(config)# segment-routing srv6
Router(config-srv6)# locators
Router(config-srv6-locators)# locator myLoc0
Router(config-srv6-locators)# prefix f1bb:bbbb:bb00:0001::/64
```

```
Router(config-srv6-locators)# delayed-delete
Router(config-srv6-locators)# locator myuLoc0
Router(config-srv6-locators)# micro-segment behavior unode psp-usd
Router(config-srv6-locators)# prefix fcbb:bb00:0001::/48
```

This example shows the in-migration state with SRv6 and IS-IS:

```
Router(config)# router isis 100
Router(config-isis)# address-family ipv6 unicast
Router(config-isis-af)# segment-routing srv6
Router(config-isis-srv6)# locator myLoc0
Router(config-isis-srv6)# locator myuLoc0
```

This example shows the in-migration state with SRv6 and BGP/EVPN:

```
Router(config)# router bgp 100
Router(config-bgp)# bgp router-id 10
Router(config-bgp)# segment-routing srv6
Router(config-bgp-srv6)# locator myuLoc0


Router(config)# evpn
Router(config-evpn)# segment-routing srv6
Router(config-evpn-srv6)# locator myuLoc0
```

This example shows how to enable Path MTU for Segment Routing over IPv6, from release 7.11.1 onwards:

```
Router(config)#hw-module profile segment-routing srv6 mode micro-segment format f3216
path-mtu
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
Router(config-srv6)#commit
```

hw-module profile segment-routing srv6 mode base

To enable the segment routing over IPv6 (SRv6) Full-length SID on the router, use the **hw-module profile segment-routing srv6 mode base** command in XR Config mode.

hw-module profile segment-routing srv6 mode base

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.7.1	This command was introduced.

Usage Guidelines

You must reload the router after enabling this feature.

Task ID

Task ID	Operation
system	read, write

The following example shows how to enable the segment routing over IPv6 (SRv6) Full-length SID on the router.

```
Router# configure
Router(config)# hw-module profile segment-routing srv6 mode base
```

hw-module profile segment routing srv6 mode base-and-micro-segment-f3216

To enable migration of existing SRv6 SID format1 to SRv6 Micro-SIDs (f3216) formats, use the **hw-module profile segment routing srv6 mode base-and-microsegment-f3216** command in XR Config mode.

hw-module profile segment-routing srv6 mode base-and-micro-segment-f3216

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

- You must reload the router after enabling the command.
- From IOS XR Release 7.8.1, the **hw-module profile segment-routing srv6 mode base-and-micro-segment-f3216** command is used for the in-migration state.
- Starting from Release 7.10.1, the SRv6 mode is automatically set to **base-and-micro-segment-f3216 mode** (dual mode) even if you configure the **base** mode. The running configuration would still continue to reflect the user configured mode only.

  You can verify the change using the following console log:

```
fia_driver[238]: %FABRIC-FIA_DRVR-6-HW_MOD_PROFILE_AUTO_CONVERTED :
Auto-converting SRv6 hw-module base profile to base-and-micro-segment-f3216 profile
```

Task ID

Task ID	Operation
system	read, write

Example

This example shows the in-migration state with SRv6 and configure locator:

```
Router(config)# segment-routing srv6
Router(config-srv6)# locators
Router(config-srv6-locators)# locator myLoc0
Router(config-srv6-locators)# prefix f1bb:bbbb:bb00:0001::/64
Router(config-srv6-locators)# delayed-delete
Router(config-srv6-locators)# locator myuLoc0
Router(config-srv6-locators)# micro-segment behavior unode psp-usd
Router(config-srv6-locators)# prefix fcbb:bb00:0001::/48
```

This example shows the in-migration state with SRv6 and IS-IS:

```
Router(config)# router isis 100
Router(config-isis)# address-family ipv6 unicast
Router(config-isis-af)# segment-routing srv6
Router(config-isis-srv6)# locator myLoc0
Router(config-isis-srv6)# locator myuLoc0
```

This example shows the in-migration state with SRv6 and BGP/EVPN:

```
Router(config)# router bgp 100
Router(config-bgp)# bgp router-id 10
Router(config-bgp)# segment-routing srv6
Router(config-bgp-srv6)# locator myuLoc0


Router(config)# evpn
Router(config-evpn)# segment-routing srv6
Router(config-evpn-srv6)# locator myuLoc0
```

hw-module profile segment routing srv6 mode micro-segment

To use SRv6 Micro-SID (uSID) before configuring SRv6 on the Cisco NCS 5500 Series Routers, enter the **hw-module profile segment-routing srv6 mode micro-segment** command in XR Config mode.

hw-module profile segment-routing srv6 mode micro-segment format f3216

Syntax Description

micro-segment format f3216	Enables the micro-segment format F3216 (represents 32-bit block and 16-bit IDs) for SRv6 profile.
path-mtu	Enables Path MTU discovery for SRv6 profile.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.11.1	The **path-mtu** keyword is introduced.
Release 7.7.1	This command was introduced.

Usage Guidelines

- You must reload the router after enabling the command.
- For the **path-mtu** keyword, use the following guidelines:
  - The SRv6 uSID (F3216) format supports the Path MTU discovery.
  - The SRv6 Full-length SID format does not support Path MTU discovery.
  - You must configure this feature on the ingress Provider Edge (PE) router.
  - SRv6 encapsulation supports the following scenarios:
    - IPv4/IPv6 over SRv6
    - SRv6-TE
    - H insert
    - TI-LFA for Single Carrier and Multi Carrier
  - L2 services over SRv6 (L2VPN) do not support the feature.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable Segment Routing over IPv6 for micro-segment format.

```
Router(config)# hw-module profile segment-routing srv6 mode micro-segment format f3216
Router(config-srv6)# encapsulation
Router(config-srv6-encap)# l3-traffic
Router(config-srv6-encap-l3)# traffic-class policy-map
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
Router(config-srv6-encap-l2)#(config-srv6-encap-l2)# commit
```

This example shows how to enable Path MTU for Segment Routing over IPv6.

```
Router(config)#hw-module profile segment-routing srv6 mode micro-segment format f3216
path-mtu
In order to activate/deactivate this srv6 profile, you must manually reload the chassis/all
 line cards
Router(config-srv6)#commit
```

hw-module profile segment-routing srv6 mode encapsulation traffic-class

To set the traffic-class on the IP header of the outgoing packet in an IPv6 network during L3VPN encapsulation, use the **hw-module profile segment-routing srv6 mode encapsulation traffic-class** command in XR Config mode.

hw-module profile segment-routing srv6 mode encapsulation traffic-class | [{ { **encapsulation l2 traffic-class** | | **encapsulation l3 traffic-class** } }]

Syntax Description

traffic-class	Controls traffic-class field of SRv6 IPv6 header for inner L2 and L3 traffic.
traffic-class value	Specifies the traffic-class value. This value, which is a hexidecimal number, ranges between *0x0* and *0xff*.
propagate	Propagates traffic-class from incoming packet or frame or use qos-group from input policy-map for L2 traffic.
policy-map	Sets the topmost 3-bit traffic-class DSCP to qos-group that is selected by the input policy-map for L3 traffic.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 6.6.1	This command was introduced.
Release 7.7.1	L2 and L3 EVPN QoS support was introduced.

Usage Guidelines

The default traffic-class value is 0.

The router must be reloaded for the **# hw-module profile segment-routing srv6 mode micro-segment format f3216 encapsulation** feature to be functional.

Task ID

Task ID	Operation
system	read, write

Example

This example shows how to set the **traffic-class propagate** option for L2 mode:

```
RP/0/RSP0/CPU0:ios# configure
RP/0/RSP0/CPU0:ios(config)# hw-module profile segment-routing srv6 mode micro-segment format
 f3216
RP/0/RSP0/CPU0:ios(config-srv6)# encapsulation
RP/0/RSP0/CPU0:ios(config-srv6-encap)# l2-traffic
RP/0/RSP0/CPU0:ios(config-srv6-encap-l2)# traffic-class propagate
```

This example shows how to set the **traffic-class policy-map** option for L3 mode.

```
RP/0/RSP0/CPU0:ios# configure
RP/0/RSP0/CPU0:ios(config)# hw-module profile segment-routing srv6 mode micro-segment format
 f3216
RP/0/RSP0/CPU0:ios(config-srv6)# encapsulation
RP/0/RSP0/CPU0:ios(config-srv6-encap)# l3-traffic
RP/0/RSP0/CPU0:ios(config-srv6-encap-l3)# traffic-class policy-map
```

hw-module profile segment-routing srv6 mode base encapsulation traffic-class propagate

To propagate traffic-class from incoming packet or frame or use qos-group from input policy-map, use the **hw-module profile segment-routing srv6 mode base encapsulation traffic-class propagate** command in XR Config mode.

hw-module profile segment-routing srv6 mode base encapsulation traffic-class propogate | [{ { **encapsulation l2 traffic-class** | | **encapsulation l3 traffic-class** } }]

Syntax Description

traffic-class	Control traffic-class field of SRv6 IPv6 header for inner L2 and L3 traffic
traffic-class value	This specifies the traffic-class value. Range is from 0x0 to 0xff. Traffic-class value must be specified as 2 hexadecimals.
propagate	Propagate traffic-class from incoming packet or frame or use qos-group from input policy-map.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

After enabling this feature, you must reload the router for the configuration to take effect.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable the feature that propagates traffic-class from incoming packet or frame or use qos-group from input policy-map.

```
Router# configure
Router(config)# hw-module profile segment-routing srv6 mode base encapsulation traffic-class
 propagate
```

hw-module profile sr-policy v6-null-label-autopush

To enable the V6 null label autopush over SR-policy, **hw-module profile sr-policy v6-null-label-autopush** command in XR Config mode.

hw-module profile sr-policy v6-null-label-autopush

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the **hw-module profile sr-policy v6-null-label-autopush** feature to be functional.

This profile enables the IPv6 null label autopush over SR policy.

This profile is not supported with 6VPE (the IPv6 null label is pushed rather than 6VPE label).

DSCP preserve is disabled.

With this feature, we can use up to 12 labels for IPv6 .

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable the IPv6 null label autopush over SR policy:

```
Router# configure
Router(config)# hw-module profile sr-policy v6-null-label-autopush
```

hw-module profile stats enh-sr-policy

To enable enhanced SR policy scale stats profile counter, use the **hw-module profile stats enh-sr-policy** command in XR Config mode.

hw-module profile stats enh-sr-policy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

Note This command is not supported on the NCS 540 series routers.

The router must be reloaded for the **hw-module profile stats enh-sr-policy** feature to be functional.

This command enables ingress SR counters and also increases the counters available in the egress pipeline.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable ingress SR counters:

```
Router# configure
Router(config)# hw-module profile stats enh-sr-policy
```

hw-module profile stats ingress-sr

To enable per-label statistics at “ingress” for Segment Routing labels, use the **hw-module profile stats enh-sr-policy** command in XR Config mode.

hw-module profile stats ingress-sr

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the **hw-module profile stats ingress-sr** feature to be functional.

This command enables per-label statistics at ingress for SR labels within the configured SRGB and SRLB.

When this profile is enabled, QoS Stats do not work for the same labeled packets.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable per-label statistics at ingress for Segment Routing labels:

```
Router# Configure
Router(config)# hw-module profile stats ingress-sr
```

hw-module profile stats tx-scale-enhanced ingress-sr

To enable the ingress segment routing statistics for increasing the Tx scale, use the **hw-module profile stats tx-scale-enhanced ingress-sr** command in XR Config mode.

hw-module profile stats tx-scaled-enhanced ingress-sr

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 6.6.1	This command was introduced.

Usage Guidelines

The router must be reloaded for the **hw-module profile stats tx-scale-enhanced ingress-sr** feature to be functional.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable the ingress segment routing statistics for increasing the Tx scale.

```
Router# configure
Router(config)# hw-module profile stats tx-scale-enhanced ingress-sr
```

index

Marks an explicit path. The index determines the order of path selection.

index *index_number* {{**exclude-address** | **exclude-srlg** | **next-address** [**loose** | **strict**]} **ipv4 unicast** *ip_address*} | {**next-label** *label*}

Syntax Description

index_number	Defines priority for the path to be selected. Ranges from 1 to 65535.
exclude-address	Specifies the IP address to be excluded from the path.
exclude-srlg	Specifies the IP address from which Shared Risk Link Groups (SRLGs) are derived for exclusion.
next-address	Specifies the next IP address in the path.
loose	Specifies the next hop in the path as a flexible hop.
strict	Specifies the next hop in the path as a fixed hop
ipv4 unicast *ip_address*	Specifies the the IPv4 unicast address.
next-label *label*	Specifies the next label in the path.

Command Default

None

Command Modes

Explicit path configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can include multiple addresses, labels, or both. However, once you start configuring labels, you need to continue with labels. You cannot use addresses after you use labels.

Task ID

Task ID	Operation
mpls-te	read, write

This example shows how to insert the next-address and next-label for explicit path ABCD1_Nodes:

```
RP/0/RSP0/CPU0:router(config)# explicit-path name ABCD1_Nodes
RP/0/RSP0/CPU0:router(config-expl-path)# index 10 next-address strict ipv4 unicast
  192.168.0.2
RP/0/RSP0/CPU0:router(config-expl-path)# index 20 next-label 24012
```

Related Commands

Command	Description
explicit-path	Configures a fixed path through the network.

mdt

To configure a default or partitioned MVPN profile for transporting IP VPN multicast traffic using SR-TE, use the **mdt** command in multicast routing VRF address family configuration mode. To remove the configuration, use the **no** form of the command.

mdt { **default** | **partitioned** } **segment-routing mpls** [**color** *value*] [**fast-reroute lfa**]

Syntax Description

default	Specifies that the MPVN profile is of the type *default*.
partitioned	Specifies that the MPVN profile is of the type *partitioned*.
segment-routing mpls	Specifies that the TE mechanism is Segment Routing, and data plane protocol is MPLS.
color *value*	(Optional) Specifies the on-demand color value that defines TE constraints and optimizations applied to the SR multicast policy.
fast-reroute lfa	(Optional) Enables the LFA FRR function for SR multicast policies that are created for the MDT.

Command Default

An MVPN default or partitioned profile is not configured.

Command Modes

Multicast routing VRF address family configuration.

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

The **mdt** configuration is enabled on all the VPN end-points, the PE routers used for MVPN peering.

Example

The following example shows how to configure a *default* MDT MVPN Profile for SR multicast:

```
Router(config)# multicast-routing vrf cust1
Router(config-mcast-cust1)# address-family ipv4
Router(config-mcast-cust1-ipv4)# mdt default segment-routing mpls color 10
Router(config-mcast-cust1-ipv4)# commit
```

Example

The following example shows how to configure a *partitioned* MDT MVPN Profile for SR multicast:

```
Router(config)# multicast-routing vrf cust1
Router(config-mcast-cust1)# address-family ipv4
Router(config-mcast-cust1-ipv4)# mdt partitioned segment-routing mpls color 10
Router(config-mcast-cust1-ipv4)# commit
```

mdt data

To configure an MVPN *data* profile for transporting IP VPN multicast traffic using SR-TE, use the **mdt data** command in multicast routing VRF address family configuration mode. To remove the configuration, use the **no** form of the command.

mdt data segment-routing mpls *max-mdt-nmr* [**color** *value*] [**fast-reroute lfa**] [**route-policy** *name*] [**threshold** *value*] [*ACL*] [**immediate-switch**]

Syntax Description

segment-routing mpls *max-mdt-nmr*	Specifies the maximum number of SR multicast polices to be used for *data* MDTs.
color *value*	(Optional) Specifies the on-demand SR policy color value. The TE constraints and optimizations are associated with the color value.
fast-reroute lfa	(Optional) Enables the LFA FRR function for SR multicast policies that are created for *data* MDTs.
route-policy *name*	(Optional) Specifies the route policy that dictates multicast flow-to-SR multicast policy mapping (with different colors). The route policy option is an alternative to enabling the **color** *value* option.
threshold *value*	(Optional) The traffic rate threshold value in Kbps. When the rate exceeds the specified value, multicast flow is switched to a *data* MDT.
ACL	(Optional) ACL that directs specific multicast flows to be switched to a *data* MDT.
immediate-switch	(Optional) Specifies that the multicast flow be switched to a *data* MDT, without waiting for the threshold limit to be crossed.

Command Default

An MVPN data profile is not configured.

Command Modes

Multicast routing VRF address family configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

The **mdt data** command has to be enabled on the ingress PEs where multicast flows need to be steered into the *data* MDT component for SR multicast processing. *Data* MDT can be configured for *default* and *partitioned* profiles.

Example

The following example shows how to configure an MVPN *data* profile.

```
Router(config)# multicast-routing vrf cust1
Router(config-mcast-cust1)# address-family ipv4
Router(config-mcast-cust1-ipv4)# mdt data segment-routing mpls 2 color 10
Router(config-mcast-cust1-ipv4)# commit
```

microloop avoidance rib-update-delay

To set the Routing Information Base (RIB) update delay value to avoid microloops in the network, use the **microloop avoidance rib-update-delay** command. To disable the RIB update delay, use the **no** form of this command.

microloop avoidance rib-update-delay *delay-time*

Syntax Description

delay-time	Specifies the amount of time the node uses the microloop avoidance policy before updating its forwarding table. The *delay-time* is in milliseconds. The range is from 1-60000.

Command Default

The default value is 5000 milliseconds.

Command Modes

IPv4 address family configuration

Router configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command with the **microloop avoidance segment-routing** command to specify how long the SR-TE policy path to the destination is used. After the RIB update delay timer expires, the SR-TE policy is replaced with regular forwarding paths.

Task ID

Task ID	Operation
ospf isis	read, write

Example

This example shows how to set the Routing Information Base (RIB) update delay value for OSPF:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router ospf 1
RP/0/RSP0/CPU0:router(config-ospf)# microloop avoidance segment-routing
RP/0/RSP0/CPU0:router(config-ospf)# microloop avoidance rib-update-delay 3000
```

This example shows how to set the Routing Information Base (RIB) update delay value for IS-IS:

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# router isis 1
RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-af)# microloop avoidance segment-routing
RP/0/RSP0/CPU0:router(config-isis-af)# microloop avoidance rib-update-delay 3000
```

microloop avoidance segment-routing

To enable the segment routing microloop avoidance and set the Routing Information Base (RIB) update delay value, use the **microloop avoidance** command. To disable segment routing microloop avoidance, use the **no** form of this command.

microloop avoidance segment-routing [**route-policy** *name*]

Syntax Description

route-policy *name*	Specifies the route policy for the destination prefixes for per-prefix filtering.

Command Default

Disabled.

Command Modes

IS-IS IPv4 address family configuration

IS-IS IPv6 address family configuration

OSPF configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.
Release 7.11.1	The **route-policy** *name* option is added for IS-IS.

Usage Guidelines

The Segment Routing Microloop Avoidance feature detects if microloops are possible following a topology change. If a node computes that a microloop could occur on the new topology, the node creates a loop-free SR-TE policy path to the destination using a list of segments. After the RIB update delay timer expires, the SR-TE policy is replaced with regular forwarding paths.

SR microloop avoidance per-prefix filtering uses route policies to identify the prefixes subjected to microloop avoidance. A route policy must be defined before it can be attached to the SR microloop avoidance configuration. Once a route policy is defined and attached to the SR microloop avoidance configuration, it cannot be modified or removed until the route policy is removed from the SR microloop avoidance configuration.

Task ID

Task ID	Operation
ospf	read, write
isis	

Example

This example shows how to enable Segment Routing Microloop Avoidance for OSPF:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router ospf 1
RP/0/RSP0/CPU0:router(config-ospf)# microloop avoidance segment-routing
```

```
RP/0/RSP0/CPU0:router(config-ospf)# microloop avoidance rib-update-delay 3000
```

This example shows how to enable Segment Routing Microloop Avoidance for IS-IS:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router isis 1
RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-af)# microloop avoidance segment-routing
RP/0/RSP0/CPU0:router(config-isis-af)# microloop avoidance rib-update-delay 3000
```

This example shows how to enable per-prefix filtering for a prefix set defined in "route policy FOO2":

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router isis 1
RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-af)# microloop avoidance segment-routing route-policy
FOO2
```

partition-detect

Use **partition-detect** command for an area or domain partition detection. It is a new command under IS-IS address-family sub-mode.

partition-detect { track *IPv4 address | IPv6 address [external-id IPv4 -address | IPv6 address]*

Syntax Description

Keyword	Details
track*IPv4 address | IPv6 address [external-id IPv4 -address | IPv6 address]*	Tracks the reachability of the specific ABR or ASBR. This command is under the partition-detect sub-mode. • Only IPv4 address is allowed under IPv4 address-family sub-mode and only IPv6 address is allowed under IPv6 address-family sub-mode. • external-id is only used for ASBR tracking. External-id is the address of the ASBR, in other domain.

Command Default

None.

Command Modes

IS-IS interface address-family configuration

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Task ID

Task ID	Operations
IS-IS	read, write

Examples

This example shows how to configure partition-detect.

```
Router(config)#router isis 1
Router(config-isis)#address-family ipv6 unicast
Router(config-isis-af)#router-id 2001:DB8:4::4
Router(config-isis-af)#partition-detect
Router(config-isis-af)#track 2001:DB8:1::1
Router(config-isis-af)#commit
```

path-option

To configure a path option for an SR-TE policy, use the **path-option** command in tunnel-te interface configuration mode. To return to the default behavior, use the **no** form of this command.

```
path-option path_preference_value {dynamic [attribute-set  | isis | lockdown |
ospf | pce | protected-by] | explicit {identifier path-number | name path-name}
[attribute-set  | isis | lockdown | ospf | protected-by | verbatim]}
segment-routing
```

Syntax Description

path_preference_value	Specifies the preference for an LSP. Range is from 1 to 1000.
dynamic [**attribute-set** | **isis** | **lockdown** | **ospf** | **pce** | **protected-by**]	Configures a dynamically allocated path based on the configured options. See the **attribute-set** statement for a description of all the attributes.
explicit {**identifier** *path-number* | **name** *path-name*} [**attribute-set** | **isis** | **lockdown** | **ospf** | **protected-by** | **verbatim**]	Configures a preset path, based on the configured options. The **verbatim** option is required for disabling loop detection on the path. When you configure this option, the topology database is not referred by the source router while configuring the preset path. See the **attribute-set** statement for a description of all the attributes.
segment-routing	Configures a segment routing path, based on the configured options.

Command Default

None

Command Modes

Tunnel-te interface configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to configure the tunnel to use an explicit path for segment routing:

```
RP/0/RSP0/CPU0:router(config)# interface tunnel-te22
RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered loopback0
RP/0/RSP0/CPU0:router(config-if)# destination 192.168.0.2
RP/0/RSP0/CPU0:router(config-if)# path-selection segment-routing adjacency protected
RP/0/RSP0/CPU0:router(config-if)# path-option 1 explicit name ABCD1_Nodes segment-routing
```

Related Commands

Command	Description
attribute-set	Configures the attribute set for an LSP.
index	Determines the order of path selection.

path-selection

Configures the LSP to be selected for the SR-TE tunnel.

path-selection [**cost-limit** *limit* | **hop-limit** *limit* | **invalidation** *timer* [**tear** | **drop**] | **metric** [**igp** | **te**] **segment-routing adjacency** [**protected** | **unprotected**] | **tiebreaker** [**max-fill** | **min-fill** | **random**]]

Syntax Description

cost-limit *limit*	Configures the cost limit for the LSP. Ranges from 1 to 4294967295.
hop-limit *limit*	Configures the hop limit for the LSP. Ranges from 1 to 255.
invalidation *timer* [**tear** | **drop**]	Configures the path invalidation timer. When the timer expires, the path is either torn down or just the segment labeled data is dropped. Ranges from 0 to 60000.
metric [**igp** | **te**]	Configures the type of metric to be used for the LSP.
segment-routing adjacency [**protected** | **unprotected**]	Configures the type of adjacency for segment routing.
tiebreaker [**max-fill** | **min-fill** | **random**]	Configures the tie breaker for path calculation of equal cost multiple paths. **Max-fill** selects the path with the most-utilized links. **Min-fill** selects the path with the least-utilized links. Random selects the path with randomly utilized links.

Command Default

None

Command Modes

Tunnel interface configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write

This example shows how to set the path-selection for segment routing adjacency protection.

```
RP/0/RSP0/CPU0:router(config)# interface tunnel-te22
RP/0/RSP0/CPU0:router(config-if)# path-selection segment-routing adjacency protected
```

pce segment-routing traffic-eng p2mp

To configure the SR-PCE server for managing multicast traffic flows, use the **pce segment-routing traffic-eng p2mp** command in global configuration mode. To remove the configuration, use the **no** form of the command.

pce segment-routing traffic-eng p2mp [**policy** *name* [**candidate-paths** [{ **constraints** [**affinity** { **include-any** | **include-all** | **exclude-any** } *name*] | [**sid-algorithm** *algo*] }]]] [{ **fast-reroute lfa** | **frr-node-set** { **from** | **to** } [**ipv4** *address*] }] | [**label-range min** *value* **max** *value*] | [**multipath-disable**]

Syntax Description

policy *name*	(Optional) Specifies the static or dynamic SR multicast policy for which LFA FRR is enabled.
constraints	Configures constraints.
affinity {**include-all** | **include-any** | **exclude-any**} *name*	Configures the affinity constraints and the affinity name.
sid-algorithm *algo*	Flex-algo value. An algorithm is a one octet value. Values from 128 to 255 are reserved for user defined values and are used for Flexible Algorithm representation.
fast-reroute lfa	Specifies that LFA FRR be enabled on all multicast routers of the SR multicast tree.
frr-node-set {**from**|**to**} [**ipv4** *address*]	Specifies the (*from* and *to*) paths on multicast routers that requires FRR protection. The PCE server applies the LFA FRR function for traffic *from* a specific IP address, sent *to* specific IP address(es).
label-range min *value* **max** *value*	Specifies the label range to be used for the multicast traffic LSPs.
multipath-disable	Disables load balancing of SR multicast traffic across ECMP paths.

Command Default

The SR-PCE server parameters are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 7.11.1	The **sid-algorithm** *algo* options are introduced.
Release 7.3.1	This command was introduced.

Example

The following example shows how to configure SR-PCE server parameters.

Label Range Configuration

The configuration specifies that labels between 30000 and 60000 be used for multicast traffic LSPs.

```
Router(config)# pce segment-routing traffic-eng p2mp label-range min 30000 max 60000
Router(config)# commit
```

FRR Configuration

The LFA FRR function is configured for all SR policies.

```
Router(config)# pce segment-routing traffic-eng p2mp fast-reroute lfa
```

The LFA FRR function is configured for the SR policy *tree1*.

```
Router(config)# pce segment-routing traffic-eng p2mp policy tree1 fast-reroute lfa
```

FRR protection is configured for traffic from the interface with IP address 192.168.0.3, and traffic being sent to the interface with IP address 192.168.0.4.

```
Router(config)# pce segment-routing traffic-eng p2mp frr-node-set from ipv4 192.168.0.3
Router(config)# pce segment-routing traffic-eng p2mp frr-node-set to ipv4 192.168.0.4
Router(config)# commit
```

Disable Load Balancing

To disable ECMP load splitting of different trees on the SR-PCE server, configure the **multipath-disable** command.

```
Router(config)# pce segment-routing traffic-eng p2mp multipath-disable
Router(config)# commit
```

Flexible Algorithm

The following example shows how to configure a P2MP policy with Flex-Algo constraint:

```
Router(config)# pce
Router(config-pce)# segment-routing traffic-eng
Router(config-pce-sr-te)# p2mp
Router(config-pce-sr-te-p2mp)# policy FOO
Router(config-pce-p2mp-policy)# candidate-paths
Router(config-pce-p2mp-policy-path)# constraints
Router(config-pce-p2mp-path-const)# sid-algorithm 128
Router(config-pce-p2mp-path-const)#
```

performance-measurement interface

This command helps you configure the target interface with probe packets that transit Interface ID within a network.

performance-measurement interface *GigE 0/1/0/1*
{ **path-tracing** { { **interface-id** *{1-4095}* } } }

Syntax Description

path-tracing	Enables path-tracing for the interface for tracing short timestamp, interface-id and interface load on source, midpoint and sink nodes in PT probes.
interface-id	Enter interface ID that is between 1-4095. Default value is none. Interface ID value 0 is used internally to indicate PT is disabled on the interface.

Command Default

Path tracing is disabled by default.

The default value for Interface ID is set to None.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

Enable path-tracing for the interface for tracing interface-id and interface load on source, midpoint and sink nodes in PT probes.

Examples

This example shows how to configure Path Tracing midpoint with InterfaceID:

```
Router(config)# performance-measurement
Router(config-pm)# interface FourHundredGigE0/0/0/1
Router(config-pm-interf)# path-tracing
Router(config-pm-interf-interf-id)# interface-id 200
Router(config-pm-interf-time)# exit
```

performance-measurement delay-measurement

To apply an SR performance measurement delay profile to an SR-TE policy, use the **performance-measurement delay-measurement** command in the SR-TE policy configuration mode. To disassociate the profile from the SR-TE policy, use the **no** form of the command.

performance-measurement delay-measurement [**delay-profile name** *profile*]
no performance-measurement delay-measurement [**delay-profile**]

Syntax Description

delay-profile name *profile*	(Optional) Specifies the delay profile that is to be associated with the SR-TE policy.

Command Default

The Default performance measurement delay profile is associated with an SR-TE policy.

Command Modes

SR-TE policy configuration (config-sr-te-policy)
On-Demand SR-TE policy configuration (config-sr-te-color)

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

The **performance-measurement** command is also available in global configuration mode. Amongst other configurations, you can use it for creating a Segment Routing performance measurement delay and liveness profiles.

Example

This example shows how to associate a delay profile to an SR-TE policy:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy TEST
Router(config-sr-te-policy)# color 4 end-point ipv4 10.10.10.10
Router(config-sr-te-policy)# performance-measurement delay-measurement delay-profile name
profile2
Router(config-sr-te-policy-perf-meas)# commit


Router(config-sr-te)# on-demand color 20
Router(config-sr-te-color)# performance-measurement delay-measurement delay-profile name
profile2
Router(config-sr-te-color)# commit
```

performance-measurement delay-profile endpoint

To detect the delay of an endpoint, use the **performance-measurement delay-profile endpoint** command in global configuration. To disable the delay-profile, use the **no** form of the command.

performance-measurement delay-profile endpoint { **default** | **name** *name* } { **advertisement accelerated** { **minimum-change** *value* | **threshold** *value* } | **logging delay-exceeded** | **periodic** { **disabled** | **interval** *value* | **minimum-change** *value* | **threshold** *value* } | **threshold-check** { **average-delay** | **maximum-delay** | **minimum-delay** } | **probe** { **burst-interval** *interval* | **computation-interval** *interval* | **measurement-mode one-way** | **tos dscp** *value* | **flow-label** { **explicit** *value* | **from** *value* **to** *value* **increment** *value* } } }

Syntax Description

advertisement	Enter interface delay profile advertisement submode
accelerated	Enter interface delay profile advertisement accelerated submode
minimum change *microseconds*	The range is from 0 to 100000 microseconds.
threshold *percent*	Checks the minimum-delay metric change for threshold crossing for accelerated advertisement. The range is from 0 to 100 percent.
logging delay-exceeded	Sends syslog when the delay exceeds the threshold.
periodic	Enter periodic advertisement configuration submode.
disabled	Disables periodic advertisement.
interval *seconds*	Periodic advertisement and metric aggregation interval. The interval range is from 30 to 3600 seconds.
minimum-change *microseconds*	The range is from 0 to 100000 microseconds.
threshold *percent*	Checks the minimum-delay metric change for threshold crossing for periodic advertisement. The range is from 0 to 100 percent.
threshold-check {**average-delay** | **maximum-delay** |**minimum-delay**}	max = default
probe	Enter probe configuration submode.
burst-interval *microseconds*	Specify the interval for sending probe packet. The range is from 30 to 15000 milliseconds.
computation-interval *seconds*	Specify the interval for metric computation. The range is from 1 to 3600 seconds.
measurement-mode {**one-way** | **two-way**}	Specify the interval measurement mode.
tos dscp *value*	Type of Service DSCP. The range is from 0 to 63.

Command Default

The default advertisement accelerated minimum change is 500 microseconds.

The default advertisement accelerated threshold is 20 percent.

The default advertisement periodic interval is 120 seconds.

The default advertisement periodic minimum-change is 500 microseconds.

The default advertisement periodic threshold is 10 percent.

The default advertisement threshold-check is **maximum-delay**.

The default burst-interval is 3000 microseconds.

The default computation-interval is 30 seconds.

The default measurement-mode is **one-way**.

The default ToS DSCP value is 48 for IP/UDP.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.4.1	This command was introduced.
Release 7.6.1	The **name** *name* keyword was deprecated. Use the **performance-measurement delay-profile name** command to create a named profile.

Usage Guidelines

Example

```
Router(config)# performance-measurement
Router(config-perf-meas)# delay-profile endpoint default
Router(config-pm-dm-ep)# probe
Router(config-pm-dm-ep-probe)# measurement-mode one-way
```

performance-measurement delay-profile interfaces

performance-measurement delay-profile interfaces { **default** | **name** *name* } { **advertisement** { **accelerated** { **minimum-change** *value* | **threshold** *value* } | **anomaly-check upper-bound** *upper_bound* **lower-bound** *lower_bound* | **logging delay-exceeded** | **periodic** { **disabled** | **interval** *value* | **minimum-change** *value* | **threshold** *value* } } | **probe** { **burst-interval** *value* | **computation-interval** *value* | **measurement-mode** { **one-way** | **two-way** } | **protocol** { **pm-mpls** | **twamp-light** } | **tos dscp** *value* } }

Syntax Description

advertisement	Enter interface delay profile advertisement submode.
accelerated	Enter interface delay profile advertisement accelerated submode.
minimum change *microseconds*	The range is from 0 to 100000 microseconds.
threshold *percent*	Checks the minimum-delay metric change for threshold crossing for accelerated advertisement. The range is from 0 to 100 percent.
anomaly-check upper-bound *upper_bound* **lower-bound** *lower_bound*	Specify the upper and lower bounds of the interface delay profile advertisement anomaly check. The range for *upper_bound* and *lower_bound* is from 1 to 200000 microseconds.
logging delay-exceeded	Sends syslog when the delay exceeds the threshold.
periodic	Enter periodic advertisement configuration submode.
disabled	Disables periodic advertisement.
interval *seconds*	Periodic advertisement and metric aggregation interval. The interval range is from 30 to 3600 seconds.
minimum-change *microseconds*	The range is from 0 to 100000 microseconds.
threshold *percent*	Checks the minimum-delay metric change for threshold crossing for periodic advertisement. The range is from 0 to 100 percent.
probe	Enter probe configuration submode.
burst-interval *microseconds*	Specify the interval for sending probe packet. The range is from 30 to 15000 milliseconds.
computation-interval *seconds*	Specify the interval for metric computation. The range is from 1 to 3600 seconds.
measurement-mode {**one-way** | **two-way**}	Specify the interval measurement mode.
protocol {**pm-mpls** | **twamp-light**}	Specify the protocol used. MPLS (using RFC6374 with MPLS encap) or Two-Way Active Measurement Protocol (TWAMP) Light (using RFC 5357 with IP/UDP encap).
tos dscp *value*	Type of Service DSCP. The range is from 0 to 63.

Command Default

The default advertisement accelerated minimum change is 500 microseconds.

The default advertisement accelerated threshold is 20 percent.

The default advertisement periodic interval is 120 seconds.

The default advertisement periodic minimum-change is 500 microseconds.

The default advertisement periodic threshold is 10 percent.

The default burst-interval is 3000 microseconds.

The default computation-interval is 30 seconds.

The default measurement-mode is **two-way**.

The default protocol is TWAMP-light.

The default ToS DSCP value is 48 for IP/UDP.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.3.1	This command was introduced.
Release 7.4.1	The **anomaly-check upper-bound** *upper_bound* **lower-bound** *lower_bound* command is introduced.
Release 7.6.1	The **name** *name* keyword was deprecated. Use the **performance-measurement delay-profile name** command to create a named profile.

Usage Guidelines

Example

This example shows how to configure performance-measurement functionalities for link delay as a global default profile.

```
RP/0/0/CPU0:router(config)# performance-measurement delay-profile interfaces default
RP/0/0/CPU0:router(config-pm-dm-intf)# probe
RP/0/0/CPU0:router(config-pm-dm-intf-probe)# measurement-mode one-way
RP/0/0/CPU0:router(config-pm-dm-intf-probe)# burst-interval 60
RP/0/0/CPU0:router(config-pm-dm-intf-probe)# computation-interval 60
RP/0/0/CPU0:router(config-pm-dm-intf-probe)# exit
RP/0/0/CPU0:router(config-pm-dm-intf)# advertisement periodic
RP/0/0/CPU0:router(config-pm-dm-intf-adv-per)# interval 120
RP/0/0/CPU0:router(config-pm-dm-intf-adv-per)# threshold 20
RP/0/0/CPU0:router(config-pm-dm-intf-adv-per)# minimum-change 1000
RP/0/0/CPU0:router(config-pm-dm-intf-adv-per)# exit
RP/0/0/CPU0:router(config-pm-dm-intf)# advertisement accelerated
RP/0/0/CPU0:router(config-pm-dm-intf-adv-acc)# threshold 30
RP/0/0/CPU0:router(config-pm-dm-intf-adv-acc)# minimum-change 1000
RP/0/0/CPU0:router(config-pm-dm-intf-adv-per)# exit
```

This example shows how to define thresholds above which delay and loss are considered “anomalous.”

```
RP/0/0/CPU0:router(config)# performance-measurement delay-profile interfaces default
RP/0/0/CPU0:router(config-pm-dm-intf)# advertisement
RP/0/0/CPU0:router(config-pm-dm-intf-adv)# anomaly-check upper-bound 5000 lower-bound 1000
RP/0/0/CPU0:router(config-pm-dm-intf-adv)# interval 120
```

```
RP/0/0/CPU0:router(config-pm-dm-intf-adv)# threshold 20
RP/0/0/CPU0:router(config-pm-dm-intf-adv)# minimum-change 1000
RP/0/0/CPU0:router(config-pm-dm-intf-adv)# exit
```

performance-measurement delay-profile name

To detect the delay of an name, use the **performance-measurement delay-profile name** command in global configuration. To disable the delay-profile, use the **no** form of the command.

performance-measurement delay-profile name value probe [{ **flow-label** { **explicit value** | **from value to value increment value** } | **measurement-mode** { **one-way** | **two-way** } | **sweep destination ipv4** *ip-address* **range** *range-value* | **tos** { **dscp value** | **traffic-class value** } | **tx-interval** *value* }]

Syntax Description

measurement-mode {**one-way** | **two-way**}	Specify the interval measurement mode. There are two options: one-way: Measures the one way delay with timestamp 1 and 2. two-way: Measures the one way delay with timestamp 1, 2, 3 and 4 without clock synchronization.
sweep destination ipv4*ip-address***range***value*	Specify the sweep IP destination addresses to perform ECMP hashing. The IPv4 adress range is 0 to 128.
tos {**dscp** *value* | **tos traffic-class** *value*}	Specify the delay probe type of service. The allowed range for DSCP is 0 to 63. specify the traffic class value to indicate the TOS level used by protocol PM MPLS. The range is from 0 to 7.
tX interval *value*	Specify the transmission interval. The allowed range is from 30000 to 15000000 micro seconds.
probe	Enter probe configuration submode.

Command Default

The default measurement-mode is **one-way**.

The default ToS DSCP value is 48 for IP/UDP.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.4.1	This command was introduced.
Release 7.6.1	The **name** *name* keyword was deprecated. Use the **performance-measurement delay-profile name** command to create a named profile.

Example

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

```
Router(config)# performance-measurement
Router(config-perf-meas)# delay-profile endpoint default
Router(config-pm-dm-ep)# probe
Router(config-pm-dm-ep-probe)# measurement-mode one-way
```

performance-measurement delay-profile

To create a unique Segment Routing performance measurement delay profile, use the **performance-measurement delay-profile** command in global configuration mode.

performance-measurement delay-profile { **sr-policy default** } { **endpoint default** } { **interface default** } { **name** *string name* } **advertisement** { **anomaly-loss** } { **anomaly-check** } **upper-bound** <*1-99*> **lower-bound** <*number lower than the upper bound (0-98)*>

Note Synthetic Loss Measurement is an inbuilt feature of delay measurement. To get the packet loss information for delay-measurement sessions, you only need to configure the delay sessions. No additional configuration is required for Synthetic Loss Measurement.

Syntax Description

name *string name*	(Optional) Specifies the Segment Routing performance measurement delay profile name.
sr-policy default	(Optional) Specifies the Segment Routing performance measurement default sr-policy name.
endpoint default	(Optional) Specifies the Segment Routing performance measurement default endpoint name.
interface default	(Optional) Specifies the Segment Routing performance measurement default interface.
advertisement	Specifies the Segment Routing performance measurement advertisement you want to configure.
anomaly-check	(optional) It checks the delay metrics, for example if the min delay changes exceed the configured threshold, it advertises ANOM-MIN-DYN; if you configured the anomaly-check and the static delay, and the configured static delay exceed the threshold, it advertises ANOM-MIN-STA. You can configure the anomaly loss with **upper-bound** and **lower-bound** values. • **upper-bound** specifies the upper limit for the anomaly check. It must be between 2-200000 • **lower-bound** specifies the lower limit for the anomaly check. It must be between 1-199999 and lower than the **upper-bound** value.

anomaly-loss	(optional) Once the packet loss exceed the configured threshold, it advertises ANOM-PKT-LOSS. You can configure the anomaly loss with **upper-bound** and **lower-bound** values. • **upper-bound** specifies the upper limit for the anomaly loss. It must be between 1-99 • **lower-bound** specifies the lower limit for the anomaly loss. It must be between 0-98 and lower than the **upper-bound** value. If both **anomaly-check** and **anomaly-loss** are triggered, then it advertises for anomaly-check, because it has a higher priority than anomaly-loss • min delay changes = current min delay - previous min delay • packet loss = (expected packet number - received packet number) / expect packet number * 100%

Command Default

No user created performance measurement delay profile exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 24.1.1	The **anomaly-loss** keyword was introduced.
Release 7.6.1	This command was deprecated and replaced with the **performance-measurement delay-profile** command.
Release 7.3.1	This command was introduced.

Task ID

Task ID	Operation
performance-measurement	write/read

Usage Guidelines

The **performance-measurement** command is also available in SR-TE specific configuration.

Example

This example shows how to create a unique Segment Routing performance measurement delay profile:

```
Router(config)# performance-measurement delay-profile sr-policy name profile1
Router(config)# commit
```

This example shows the example of anomaly-loss:

```
Router(config)#performance-measurement
Router(config-perf-meas)#delay-profile sr-policy default
Router(config-pm-dm-srpolicy)#advertisement
Router(config-pm-dm-srpolicy-adv)#anomaly-loss
```

```
Router(config-pm-dm-srpolicy-adv-anom-loss)#upper-bound 30 lower-bound 20
Router(config-pm-dm-srpolicy-adv-anom-loss)#commit
```

This example shows the example of anomaly-check:

```
Router(config)#performance-measurement
Router(config-perf-meas)#delay-profile sr-policy default
Router(config-pm-dm-srpolicy)#advertisement
Router(config-pm-dm-srpolicy-adv)#anomaly-check
Router(config-pm-dm-srpolicy-adv-anom-loss)#upper-bound 2000 lower-bound 20
Router(config-pm-dm-srpolicy-adv-anom-loss)#commit
```

performance-measurement endpoint

To enable endpoint for the performance measurement, use the **performance-measurement endpoint** command in global configuration mode. To disable the endpoint, use the **no** form of the command.

performance-measurement endpoint ipv4 *endpoint_ip_addr* [**vrf** *name*] [{ **delay-measurement** [**delay-profile name** *profile_name*] | **description** *description* | **liveness-detection** [**liveness-profile name** *profile_name*] | **segment-list name** *sidlist_name* | **source-address ipv4** *source_ip_addr* }]

Syntax Description

endpoint_ip_addr	IPv4 address of the endpoint.
vrf *name*	The name of the VRF instance.
delay-measurement	Enable delay-measurement on the endpoint.
delay-profile name *profile_name*	Specify an optional delay profile name.
description *description*	Specify a description for the endpoint.
liveness-detection	Enable liveness-detection on the endpoint.
liveness-profile name *profile_name*	Specify an optional liveness profile name.
segment-list name *sidlist_name*	Specify a segment list for the endpoint.
source-address ipv4 *source_ip_addr*	IPv4 address of the sender.

Command Default

None

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following example show how to enable IPv4 endpoint for the delay measurement.

```
Router(config)# performance-measurement
Router(config-perf-meas)# endpoint ipv4 10.10.1.5
Router(config-pm-ep)# source-address ipv4 10.10.1.1
Router(config-pm-ep)# delay-measurement
```

The following example show how to configure IPv6 endpoint for liveness.

```
Router(config)#performance-measurement
Router(config-perf-meas)#source-address ipv6 FCBB:0:1::
```

```
Router(config-perf-meas)#endpoint ipv6 FCBB:0:5::
Router(config-pm-ep)#exit
Router(config-perf-meas)#liveness-profile endpoint default
```

performance-measurement liveness-detection

To apply an SR performance measurement liveness profile to an SR-TE or an SRv6-TE policy, use the **performance-measurement liveness-detection** command in the SR-TE policy configuration mode. To disassociate the profile from the SR-TE policy, use the **no** form of the command.

performance-measurement liveness-detection [{ **liveness-profile** [**backup**] **name** *profile* | **validation-cp minimum-active segment-lists** [{ *1-128* | **all** }] }]

Syntax Description

liveness-profile [**backup**] **name** *profile*	(Optional) Specifies the liveness profile that is to be associated with the SR-TE policy. The **name** *profile* command form specifies the liveness profile, and the **backup name** *profile* command form specifies the backup liveness profile.
validation-cp minimum-active	(Optional) Validates the activeness of the candidate-path based on minimum number of active segment-lists.
segment-lists	Indicates the number of active segment-lists.
1-128 | **all**	• 1-128: Indicates the minimum number of segment-lists to have the PM liveness session up. • all: Indicates that all the segment-lists should be active to have the PM liveness session up.

Command Default

The Default performance measurement liveness profile is associated with an SR-TE policy.

Command Modes

SR-TE policy configuration (config-sr-te-policy)
On-Demand SR-TE policy configuration (config-sr-te-color)

Command History

Release	Modification
Release 7.11.1	The validation-cp minimum-active segment-lists option was introduced.
Release 7.4.2	The **backup** keyword was added to the command.
Release 7.3.1	This command was introduced.

Usage Guidelines

Path protection policies do not fully support PCE reporting of the standby LSP.

Example

This example shows how to associate a liveness profile to an SR-TE policy:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#policy TRST2
Router(config-sr-te-policy)#color 40 end-point ipv4 20.20.20.20
Router(config-sr-te-policy)#performance-measurement liveness-detection liveness-profile
name profile3
```

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#on-demand color 30
Router(config-sr-te-color)#performance-measurement liveness-detection liveness-profile name
 profile3
Router(config-sr-te-color)#commit
```

This example shows how to associate a backup liveness profile to an SR-TE policy:

```
RP/0/RSP0/CPU0:ios# configure
RP/0/RSP0/CPU0:ios(config)#segment-routing traffic-eng
RP/0/RSP0/CPU0:ios(config-sr-te)#policy foo
RP/0/RSP0/CPU0:ios(config-sr-te-policy)# color 10 end-point ipv4 192.168.0.3
RP/0/RSP0/CPU0:ios(config-sr-te-policy)# performance-measurement
RP/0/RSP0/CPU0:ios(config-sr-te-policy-perf-meas)# liveness-detection
RP/0/RSP0/CPU0:ios(config-sr-te-policy-live-detect)# liveness-profile name profile-WORKING

RP/0/RSP0/CPU0:ios(config-sr-te-policy-live-detect)# liveness-profile backup name
profile-PROTECT
RP/0/RSP0/CPU0:ios(config-sr-te-policy-live-detect)# commit
```

This example shows how to activate two segment-lists to have the PM liveness session up:

```
Router(config)#segment-routing
Router(config-sr)#traffic-eng
Router(config-sr-te)#policy po-103
Router(config-sr-te-policy)#performance-measurement
Router(config-sr-te-policy-perf-meas)#liveness-detection
Router(config-sr-te-policy-live-detect)#validation-cp minimum-active segment-lists 2
```

performance-measurement liveness-profile endpoint

performance-measurement liveness-profile endpoint { **default** | **name** *name* } { **liveness-detection** { **logging state-change detected** | **multiplier** *value* } | **probe** { **burst-interval** *value* | **measurement-mode loopback** | **tos dscp** *value* } }

Syntax Description

default	The default profile.
name *name*	The name of profile.
liveness-detection	Enter endpoint liveness detection submode.
logging state-change detected	Display a syslog when the liveness state change detected.
multiplier *value*	Specify the number of probe packets sent before the head-end node assumes the candidate path is down.
probe	Enter endpoint liveness detection probe submode.
burst-interval *interval*	Specify the interval for sending probe packet. The range is from 30 to 15000 milliseconds.
measurement-mode loopback	Specify the measurement mode. Liveness detection must use loopback mode.
tos dscp *value*	Type of Service DSCP. The range is from 0 to 63.

Command Default

Default burst interval is 3000 milliseconds (3 seconds).

Default ToC DSCP value is 48.

Command Modes

Global ConfigurationXR Config

Command History

Release	Modification
Release 7.4.1	This command was introduced.
Release 7.6.1	The **name** *name* keyword was deprecated. Use the **performance-measurement liveness-profile name** command to create a named profile.

Usage Guidelines

Liveness-detection and delay-measurement aren't supported together

Example

```
Router(config)# performance-measurement
Router(config-perf-meas)# liveness-profile endpoint default
Router(config-pm-ld-ep)# liveness-detection
Router(config-pm-ld-ep-ld)# multiplier 3
Router(config-pm-ld-ep-ld)# exit
```

```
Router(config-pm-ld-ep)# probe
Router(config-pm-ld-ep-probe)# measurement-mode loopback
```

performance-measurement liveness-profile

To create a unique Segment Routing performance measurement liveness profile, use the **performance-measurement liveness-profile** command in global configuration mode. To remove the profile, use the **no** form of the command.

performance-measurement liveness-profile [{ **name** [*name* **npu-offload enable**] | **probe flow-label** [{ **explicit** | **from** }] }]

Table 2: Syntax Description

Syntax	Description
name *name*	Specifies the Segment Routing performance measurement liveness profile name.
npu-offload	Enables performance measurement liveness hardware (NPU) offload feature in the SR
probe	Enter the liveness detection probe sub mode.
flow-label	Indicates the flow labels associated with SRv6 header.
explicit | **from**	Specify explicit flow label values or enter a range of flow labels that you want to configure. You can configure flow labels in the 0 to 1048575 range.

Command Default

No user created performance measurement liveness profile exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 7.11.1	The **flow-label** keyword was introduced.
Release 7.10.1	**npu-offload** was introduced. Use **performance-measurement liveness-profile name***liveness profile*. **Note** • **performance-measurement liveness-profile name***name* (named profile) and **performance-measurement liveness-profile sr-policy***default* (default profile) are supported. • **performance-measurement liveness-profile sr-policy***name* is deprecated.
Release 7.6.1	This **performance-measurement liveness-profile sr-policy** was introduced.

Usage Guidelines

The **performance-measurement** command is also available in SR-TE specific configuration.

Example

This example shows how to create a unique Segment Routing performance measurement liveness profile:

```
Router(config)# performance-measurement liveness-profile name profile1
Router(config)# commit
```

This example shows how to configure a range of flow labels in the SRv6 header:

```
Router#configure
Router(config)#performance-measurement
Router(config-perf-meas)#liveness-profile name name1
Router(config-pm-ld-profile)# probe flow-label from 0 to 1000000 increment 10
Routerconfig-pm-ld-profile)#commit
```

This example shows how to explicitly configure flow labels in the SRv6 header:

```
Router#configure
Router(config)#performance-measurement
Router(config-perf-meas)#liveness-profile name name1
Router(config-pm-ld-profile)# probe flow-label explicit 100 200 300 400 500
Routerconfig-pm-ld-profile)#commit
```

performance-measurement protocol twamp-light measurement delay

To configure the querier or responder nodes to accept packets from specific IP addresses on the network, use the **performance-measurement protocol twamp-light measurement delay** command in the global configuration mode. To remove the IP addresses, use the **no** form of the command.

performance-measurement protocol twamp-light measurement delay { **querier allow responder address** { **ipv4** | **ipv6** } | **responder allow querier address** { **ipv4** | **ipv6** } | **unauthenticated** { **ipv4** | **ipv6** | **querier-dst-port** | **querier-src-port** } }

Syntax Description

querier	Enter the querier submode to configure the IP addresses on a querier node.
responder	Enter the responder submode to configure the IP address on a responder node.
allow responder	Specifies the allowed responder address on the querier node. The configuration is applicable to delay measurement sessions.
allow querier	Specifies the allowed querier addresses on the responder node. The configuration is applicable to delay measurement sessions.
address	Specifies the querier or responder IP addresses that are configured.
{ ipv4 | ipv6 }	Configure the allowed querier or responder ipv4 or ipv6 addresses. You can specify the prefix for the IP addresses.
unauthenticated	Enter the unauthenticated submode to configure the IP address timestamp or the source and destination UDP ports.
ipv4 | ipv6	Configure the timestamp for ipv4 or ipv6 addresses.
querier-dst-port	Configure the UDP port to process queries. By default, the TWAMP reserved UDP destination port is 862.
querier-src-port	UDP port on Route Processor used as source port in queries.

Command Default

None.

Command Modes

Global Configuration

Command History

Release	Modification
Release 7.11.1	The **querier** and **responder** keywords were introduced.
Release 7.0.1	This command was introduced.

Usage Guidelines

None.

This example shows how to configure the IP address of a querier on a responder node for delay measurement.

```
Router#configure
Router(config)#performance-measurement
Router(config-perf-meas)#protocol twamp-light
Router(config-pm-protocol)#measurement delay
Router(config-pm-proto-meas)#responder
Router(config-pm-proto-responder)#allow-querier
Router(config-pm-allowed-querier)#address ipv4 10.10.10.1
Router(config-sr-te-color)#commit
```

ping sr-mpls

To check the connectivity of segment routing control plane, use the **ping sr-mpls** command in XR EXEC mode.

ping sr-mpls { *ipv4-address/mask* | *ipv6-address/mask* [**fec-type** { **bgp** | **generic** | **igp** { **ospf** | **isis** } }] | **nil-fec** | **dataplane-only** { **labels** { *label1* [**,** *label2...*] *ipv4-address/mask* | *ipv6-address/mask* | **policy** } } { **output** { **interface** *interface-path-id* } } | { **nexthop** *next-hop-ip-address* } }

Syntax Description

ipv4-address/mask or *ipv6-address/mask*	Address prefix of the target and number of bits in the target address network mask.
fec-type	(Optional) Specifies FEC type to be used. Default FEC type is generic. **bgp** Use FEC type as BGP. **generic** Use FEC type as generic **igp** Use FEC type as OSPF or IS-IS.
labels *label1, label2...*	Specifies the label stack. Use commas to separate each label.
output interface *interface-path-id*	Specifies the output interface where echo request packets are sent.
nexthop *next-hop-ip-address*	Causes packets to go through the specified IPv4 or IPv6 next-hop address.

Command Default

fec-type : generic

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Example

These examples show how to use segment routing ping to test the connectivity of segment routing control plane. In the first example, FEC type is not specified. You can also specify the FEC type as shown in the second example.

```
RP/0/RP0/CPU0:router# ping sr-mpls 10.1.1.2/32

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms
```

```
RP/0/RP0/CPU0:router# ping sr-mpls 10.1.1.2/32 fec-type igp ospf

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

prefix-sid

To specify or advertise prefix (node) segment ID (SID) on all routers, use the **prefix-sid** command in IS-IS interface address family or OSPF interface configuration mode. To stop advertising prefix SID, use the **no** form of this command.

prefix-sid [**strict-spf**] { **index** *sid-index* | **absolute** *sid-value* } [**n-flag-clear**] [**explicit-null**]

no prefix-sid [**strict-spf**] { **index** *sid-index* | **absolute** *sid-value* } [**n-flag-clear**] [**explicit-null**]

Syntax Description

strict-spf	Specifies that the prefix-SID should use the SPF path instead of the SR-TE policy.
index *sid-index*	Specifies the prefix SID based on the lower boundary of the SRGB + the index.
absolute *sid-value*	Specifies the specific prefix SID value within the SRGB.
n-flag-clear	Specifies that the prefix-SID is not a node-SID by setting the N flag in the prefix-SID sub Type Length Value (TLV) to 0.
explicit-null	Adds an explicit-Null label by setting the E flag in the prefix-SID sub TLV to 1. Automatically disables penultimate-hop-popping (PHP) by setting the P flag (IS-IS) or NP flag (OSPF) to 1.

Command Default

Prefix SID is a node SID (N-flag is set to 1).

Explicit-Null label is not set (E-flag is set to 0).

Command Modes

IS-IS interface address-family configuration

OSPF interface configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.
Release 6.2.1	The **strict-spf** keyword was added for IS-IS.

Usage Guidelines

Segment routing must be configured on the ISIS instance or on the OSPF process, area, or interface before configuring prefix SID value.

Strict-SPF SIDs are used to forward traffic strictly along the SPF path. Strict-SPF SIDs are not forwarded to SR-TE policies. IS-IS advertises the SR Algorithm sub Type Length Value (TLV) (in the SR Router Capability SubTLV) to include both algorithm 0 (SPF) and algorithm 1 (Strict-SPF). When the IS-IS area or level is Strict-SPF TE-capable, Strict-SPF SIDs are used to build the SR-TE Strict-SPF policies. Strict-SPF SIDs are also used to program the backup paths for prefixes, node SIDs, and adjacency SIDs.

Note The same SRGB is used for both regular SIDs and strict-SPF SIDs.

Task ID

Task ID	Operations
isis	read, write
ospf	

Examples

This example shows how to configure a prefix SID.

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# router isis 100
RP/0/RSP0/CPU0:router(config-isis)# interface loopback0
RP/0/RSP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-if-af)# prefix-sid index 1001
```

This example shows how to configure an absolute prefix SID on an OSPF interface.

```
RP/0/RSP0/CPU0:router # configure
RP/0/RSP0/CPU0:router(config)# router ospf 1
RP/0/RSP0/CPU0:router(config-ospf)# router area 0
RP/0/RSP0/CPU0:router(config-ospf-ar)# interface loopback0
RP/0/RSP0/CPU0:router(config-ospf-ar-if)# prefix-sid absolute 16041
```

Related Commands

Command	Description
segment-routing global-block	Configures the segment routing global block (SRGB).

prefix-unreachable

Use this command for UPA advertisements by enabling individual control parameters.

The new **prefix-unreachable** command under IS-IS address-family submode includes several command-options that control various parameters for UPAs originated by the router.

prefix-unreachable { adv-lifetime <*value*> | **adv-metric** <*value*> | **adv-maximum** <*value*> | **rx-process-enable }**

Syntax Description

Keyword	Details
prefix-unreachable	Lists the control options of UPA.
adv-lifetime	• This command is optional. • Amount of time the UPA will be advertised after the prefix becomes unreachable. Range of values is 30–65535 seconds. • Default value is 180 seconds.
adv-metric	• This command is optional. • Metric used when advertising UPA. Range of values is 4261412865–4294967294 (0xFE000001 to 0xFFFFFFFE). • Default value is 4261412865 (0xFE000001).
adv-maximum	• This command is optional. UPAs that are leaked or propagated are not counted against this limit. • Maximum number of UPAs that the router is allowed to generate to any of its attached areas or domains. UPAs that are leaked, propagate, or redistributed are not counted against this limit. Range of values is 1–65535. • Default value is 32.
rx-process-enable	• This command is optional. • If enabled, the UPA received by the router is sent to RIB and is used to trigger the BGP PIC. • It is disabled by default.

Command Default

None.

Command Modes

IS-IS interface address-family configuration

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Task ID

Task ID	Operations
IS-IS	read, write

Examples

This example shows how to configure UPA.

```
Router(config)#router isis 1
Router(config-isis)#address-family ipv6 un
Router(config-isis-af)#prefix-unreachable
Router(config-isis-prefix-unreachable)#adv-lifetime 500
Router(config-isis-prefix-unreachable)#adv-metric 4261412866
Router(config-isis-prefix-unreachable)#adv-maximum 77
Router(config-isis-prefix-unreachable)#rx-process-enable
Router(config-isis-prefix-unreachable)#commit
```

summary-prefix

Use the exiting **summary-prefix** command for UPA advertisement.

summary-prefix *prefix/mask* **level** *1or 2* [**tag** *value*] [**adv-unreachable** { **unreachable-component-tag** *value* **partition-repair** }]

Syntax Description

Keyword	Details
level*1or 2*	Enter the border router values 1 or 2. To set the border router level for UPA.
tag*value*	Enter the tag value for which you want to enable the UPA.
adv-unreachable	The new keyword **adv-unreachable** controls the UPA advertisement for the components of the summary. The new **adv-unreachable** keyword is optional and disabled by default.
unreachable-component-tag*value*	The **unreachable-component-tag** is used to limit UPAs to those components of the summary that are advertised with a specific tag value. The **unreachable-component-tag** keyword is disabled by default and UPA is generated for all components of the summary if enabled by the **adv-unreachable** keyword.
partition-repair	In case the area (domain) partition is detected, the summary is suppressed, and more specific prefixes are advertised.

Command Default

None.

Command Modes

IS-IS address-family configuration

Command History

Release	Modification
Release 7.10.1	The **partition-repair** keyword was introduced.
Release 7.8.1	This command was introduced.

Usage Guidelines

New commands are added under the exiting IS-IS address-family sub-mode **summary-prefix** command.

Task ID

Task ID	Operations
IS-IS	read, write

Examples

This example shows how to configure Summary-Prefix for UPA.

```
Router(config)#router isis 1
Router(config)#router isis 1
Router(config-isis)#address-family ipv6 unicast
Router(config-isis-af)#router-id 2001:DB8:4::4
Router(config-isis-af)#summary-prefix 2001:DB8::/32 level 2 partition-repair
Router(config-isis-af)#summary-prefix 2001:DB9::/32 level 2 algorithm 128 partition-repair
```

segment-routing global-block

To configure the segment routing global block (SRGB), use the **segment-routing global-block** command.

segment-routing global-block *starting_value ending_value*

Syntax Description

starting_value ending_value	Specifies the block of segment routing IDs that are allocated for the routers in the network. Ranges from 16000 to 1048574.

Command Default

Default SRGB range is 16000 to 23999.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To keep the segment routing configuration simple and to make it easier to troubleshoot segment routing issues, we recommend that you use the default SRGB range on each node in the domain. However, there are instances when you might need to define a different range:

- The nodes of another vendor support a label range that is different from the default SRGB, and you want to use the same SRGB on all nodes.
- The default range is too small.
- To specify separate SRGBs for IS-IS and OSPF protocols, as long as the ranges do not overlap.

Because the values assigned from the range have domain-wide significance, we recommend that all routers within the domain be configured with the same range of values.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to configure the SRGB range:

```
RP/0/RSP0/CPU0:router(config)# segment-routing global-block 17000 20000
```

Related Commands

Command	Description
prefix-sid	Configures the segment ID (SID).

segment-routing local-block

To configure the segment routing local block (SRLB), use the **segment-routing local-block** command.

segment-routing local-block *starting_value ending_value*

Syntax Description

starting_value ending_value	Specifies the block of labels that are reserved for manual allocation of adjacency segment IDs (Adj-SIDs). Ranges from 15000 to 1048574.

Command Default

Default SRLB range is 15000 to 15999.

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you define a new SRLB range, there might be a label conflict (for example, if labels are already allocated, statically or dynamically, in the new SRLB range). In this case, the new SRLB range will be accepted, but not applied (pending). The previous SRLB range (active) will continue to be in use until one of the following occurs:

- Reload the router to release the currently allocated labels and allocate the new SRLB
- Use the **clear segment-routing local-block discrepancy all** command to clear the label conflicts

The SRLB size cannot be more than 262,143.

To keep the segment routing configuration simple and to make it easier to troubleshoot segment routing issues, we recommend that you use the default SRLB range on each node in the domain. However, there are instances when you might need to define a different range:

- The nodes of another vendor support a label range that is different from the default SRLB, and you want to use the same SRLB on all nodes.
- The default range is too small.

Because the values assigned from the range have domain-wide significance, we recommend that all routers within the domain be configured with the same range of values.

Task ID

Task ID	Operation
mpls-te	read, write

This example shows how to configure the SRLB range:

```
RP/0/RSP0/CPU0:router(config)# segment-routing local-block 18000 19999
```

Related Commands

Command	Description
clear segment-routing local-block discrepancy all, on page 13	Clears SRLB label conflicts
show segment-routing local-block inconsistencies, on page 123	Displays SRLB label conflicts

segment-routing mapping-server

To configure the segment routing mapping server (SRMS), use the **segment-routing mapping-server** command.

segment-routing mapping-server prefix-sid-map address-family {**ipv4** | **ipv6**} *ip_address*/*subnet_mask* *SID_start_value* **range** *range*

Syntax Description

address-family {**ipv4** | **ipv6**}	Configures the address family for IS-IS.
ip_address/*subnet_mask*	Specifies the prefix and mask.
SID_start_value	Specifies the first prefix SID in the range.
range *range*	Specifies the size of the range.

Command Default

None

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The position of the mapping server in the network is not important. However, since the mapping advertisements are distributed in IGP using the regular IGP advertisement mechanism, the mapping server needs an IGP adjacency to the network.

The role of the mapping server is crucial. For redundancy purposes, you should configure multiple mapping servers in the networks.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to configure the mapping server and add prefix-SID mapping entries in the active local mapping policy:

```
RP/0/RSP0/CPU0:router(config)# segment-routing mapping-server prefix-sid-map address-family
```

```
ipv4 10.1.1.1/32 17000 range 100
```

Related Commands

Command	Description
segment-routing prefix-sid-map advertise-local	Enables the router to advertise the SRMS entries that are locally configured.
segment-routing prefix-sid-map receive disable	Disables mapping client functionality.
show isis segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for IS-IS.
show ospf segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for OSPF.
show segment-routing mapping-server prefix-sid-map	Displays the locally configured prefix-to-SID mappings.

segment-routing mpls

To enable segment routing for IPv4 addresses with MPLS data plane, use the **segment-routing mpls** command in IPv4 address family configuration mode. To disable segment routing, use the **no** form of this command.

segment-routing mpls

Syntax Description

mpls	Enables segment routing for IPv4 addresses with MPLS data plane.

Command Default

No default behavior or values.

Command Modes

IPv4 address family configuration

Router configuration

Area configuration

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write

Example

This example shows how to enable segment routing with MPLS data plane.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router isis 100
RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-af)# segment-routing mpls
```

segment-routing prefix-sid-map advertise-local

To enable the router to advertise the segment routing mapping server (SRMS) entries that are locally configured, use the **segment-routing prefix-sid-map advertise-local** command. In addition to advertising these local SRMS entries, these mapping entries are also used to calculate segment ID (SID).

segment-routing prefix-sid-map advertise-local

Syntax Description

advertise-local	Advertises the SRMS mapping entries that are locally configured.

Command Default

Disabled.

Command Modes

IPv4 address family configuration

Router configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ospf isis	read, write

Example

This example shows how to enable the router to advertise the locally configured SRMS entries:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router ospf 1
RP/0/RSP0/CPU0:router(config-ospf)# segment-routing prefix-sid-map advertise-local
```

Related Commands

Command	Description
segment-routing mapping-server, on page 88	Configures the segment routing mapping server (SRMS).
segment-routing prefix-sid-map receive disable	Disables mapping client functionality.

Command	Description
show isis segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for IS-IS.
show ospf segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for OSPF.
show segment-routing mapping-server prefix-sid-map	Displays the locally configured prefix-to-SID mappings.

segment-routing prefix-sid-map receive disable

To disable mapping client functionality, use the **segment-routing prefix-sid-map receive disable** command. To reenable client functionality, use the **segment-routing prefix-sid-map receive** command.

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

Syntax Description

receive	Only remote SRMS mapping entries are used for SID calculation.
disable	Disable remote SRMS mapping entries received by flooding.

Command Default

Enabled.

Command Modes

IPv4 address family configuration

Router configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The mapping client functionality is enabled by default. When you disable client functionality, the SRMS active policy is calculated without remote SRMS entries.

You can use this command with the **segment-routing prefix-sid-map advertise-local** command simultaneously.

Task ID

Task ID	Operation
ospf	read, write
isis	

Example

This example shows how to disable the mapping server client functionality:

```
RP/0/RSP0/CPU0:router(config)# router isis 1
RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-isis-af)# segment-routing prefix-sid-map receive disable
```

Related Commands

Command	Description
segment-routing mapping-server, on page 88	Configures the segment routing mapping server (SRMS).
segment-routing prefix-sid-map advertise-local	Enables the router to advertise the SRMS entries that are locally configured.
show isis segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for IS-IS.
show ospf segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for OSPF.
show segment-routing mapping-server prefix-sid-map	Displays the locally configured prefix-to-SID mappings.

show isis segment-routing prefix-sid-map

To verify the active and backup prefix-to-SID mappings for IS-IS, use the **show isis segment-routing prefix-sid-map** command.

show isis segment-routing prefix-sid-map [**active-policy** | **backup-policy**]

Syntax Description

active-policy	(Optional) Specifies the active mapping policy.
backup-policy	(Optional) Specifies the backup mapping policy.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
isis	read

Example

The example shows how to verify the active mapping policy on IS-IS:

```
RP/0/0/CPU0:router# show isis segment-routing prefix-sid-map active-policy

IS-IS 1 active policy
Prefix               SID Index    Range        Flags
1.1.1.100/32         100          20
1.1.1.150/32         150          10

Number of mapping entries: 2
```

The example shows how to verify the backup mapping policy on IS-IS:

```
RP/0/0/CPU0:router# show isis segment-routing prefix-sid-map backup-policy

IS-IS 1 backup policy
Prefix               SID Index    Range        Flags
1.1.1.100/32         100          20
1.1.1.150/32         150          10
```

```
Number of mapping entries: 2
```

Related Commands

Command	Description
segment-routing mapping-server, on page 88	Configures the segment routing mapping server (SRMS).
segment-routing prefix-sid-map advertise-local	Enables the router to advertise the SRMS entries that are locally configured.
segment-routing prefix-sid-map receive disable	Disables mapping client functionality.
show ospf segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for OSPF.
show segment-routing mapping-server prefix-sid-map	Displays the locally configured prefix-to-SID mappings.

show mvpn vrf

To view BGP MVPN configuration information for a VRF, use the **show mvpn vrf** command in EXEC mode.

show mvpn vrf *name* { **context** [**detail**] | **database segment-routing** | **pe** [*address*] }

Syntax Description

vrf *name*	Specifies the VRF for which BGP MVPN information is displayed.
context [**detail**]	Specifies that MVPN information including MDT, Route Distinguisher and Route Target details be displayed.
database segment-routing	Specifies that MDT database information be displayed.
pe [*address*]	Specifies the ingress or egress PE router for which MVPN information is to be displayed.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Example

View Default MDT Configuration Information

This command displays SR multicast tree information, including the MDT details (of *Default* type, etc), and customer VRF information (route target, route distinguisher, etc).

```
Router# show mvpn vrf vpn1 context

MVPN context information for VRF vpn1 (0x9541cf0)

RD: 1:10 (Valid, IID 0x1), VPN-ID: 0:0
Import Route-targets : 2
  RT:192.168.0.4:0, BGP-AD
  RT:192.168.0.4:17, BGP-AD
BGP Auto-Discovery Enabled (I-PMSI added)
SR P2MP Core-tree data:
  MDT Name: TRmdtvpn1, Handle: 0x4150, idb: 0x956fc30
  MTU: 1376, MaxAggr: 255, SW_Int: 30, AN_Int: 60
  RPF-ID: 3, C:0, O:1, D:0, CP:0
  Static Type : - / -
  Def MDT ID: 524289 (0x93993f0), added: 1, HLI: 0x80001, Cfg: 1/0
  Part MDT ID: 0 (0x0), added: 0, HLI: 0x00000, Cfg: 0/0
  Ctrl Trees : 0/0/0, Ctrl ID: 0 (0x0), Ctrl HLI: 0x00000
```

View Partitioned MDT Configuration Information

This command displays SR multicast tree information, including the MDT details (of *Partitioned* type, etc), and customer VRF information (route target, route distinguisher, etc).

```
Router# show mvpn vrf vpn1 context

MVPN context information for VRF vpn1 (0x9541cf0)

RD: 1:10 (Valid, IID 0x1), VPN-ID: 0:0
Import Route-targets : 2
  RT:192.168.0.4:0, BGP-AD
  RT:192.168.0.4:17, BGP-AD
BGP Auto-Discovery Enabled (I-PMSI added) , MS-PMSI sent
SR P2MP Core-tree data:
  MDT Name: TRmdtvpn1, Handle: 0x4210, idb: 0x956fc30
  MTU: 1376, MaxAggr: 255, SW_Int: 30, AN_Int: 60
  RPF-ID: 1, C:0, O:1, D:0, CP:0
  Static Type : - / -
  Def MDT ID: 0 (0x0), added: 0, HLI: 0x00000, Cfg: 0/0
  Part MDT ID: 524292 (0x9399318), added: 1, HLI: 0x80004, Cfg: 1/0
  Ctrl Trees : 0/0/0, Ctrl ID: 0 (0x0), Ctrl HLI: 0x00000
```

View MDT Configuration Information On The Ingress PE Router

This command displays SR multicast tree information on the PE router that receives the multicast traffic on the SP network. The information includes PE router details, MDT details, Tree-SID details, and the specified customer VRF information.

```
Router# show mvpn vrf vpn1 pe

MVPN Provider Edge Router information

VRF : vpn1

PE Address : 192.168.0.3 (0x9570240)
  RD: 0:0:0 (null), RIB_HLI 0, RPF-ID 13, Remote RPF-ID 0, State: 0, S-PMSI: 2
  PPMP_LABEL: 0, MS_PMSI_HLI: 0x00000, Bidir_PMSI_HLI: 0x00000, MLDP-added: [RD 0, ID 0,
Bidir ID 0, Remote Bidir ID 0], Counts(SHR/SRC/DM/DEF-MD): 0, 0, 0, 0, Bidir: GRE RP Count
 0, MPLS RP Count 0RSVP-TE added: [Leg 0, Ctrl Leg 0, Part tail 0 Def Tail 0, IR added:
[Def Leg 0, Ctrl Leg 0, Part Leg 0, Part tail 0, Part IR Tail Label 0
  Tree-SID Added: [Def/Part Leaf 1, Def Egress 0, Part Egress 0, Ctrl Leaf 0]
  bgp_i_pmsi: 1,0/0 , bgp_ms_pmsi/Leaf-ad: 1/1, bgp_bidir_pmsi: 0, remote_bgp_bidir_pmsi:
0, PMSIs: I 0x9570378, 0x0, MS 0x94e29d0, Bidir Local: 0x0, Remote: 0x0, BSR/Leaf-ad 0x0/0,
 Autorp-disc/Leaf-ad 0x0/0, Autorp-ann/Leaf-ad 0x0/0
 IIDs: I/6: 0x1/0x0, B/R: 0x0/0x0, MS: 0x1, B/A/A: 0x0/0x0/0x0

  Bidir RPF-ID: 14, Remote Bidir RPF-ID: 0
  I-PMSI:   Unknown/None (0x9570378)
  I-PMSI rem:  (0x0)
  MS-PMSI:   Tree-SID [524290, 192.168.0.3] (0x94e29d0)
  Bidir-PMSI:  (0x0)
  Remote Bidir-PMSI:  (0x0)
  BSR-PMSI:  (0x0)
  A-Disc-PMSI:  (0x0)
  A-Ann-PMSI:  (0x0)
  RIB Dependency List: 0x0
  Bidir RIB Dependency List: 0x0
    Sources: 0, RPs: 0, Bidir RPs: 0
```

View MDT Configuration Information On The Egress PE Router

This command displays SR multicast tree information on the MVPN egress PE router that sends multicast traffic from the SP network towards multicast receivers. The information includes PE router, Tree-SID, MDT, and the specified customer VRF details.

```
Router# show mvpn vrf vpn1 pe

MVPN Provider Edge Router information
```

```
PE Address : 192.168.0.4 (0x9fa38f8)
  RD: 1:10 (valid), RIB_HLI 0, RPF-ID 15, Remote RPF-ID 0, State: 1, S-PMSI: 2
  PPMP_LABEL: 0, MS_PMSI_HLI: 0x00000, Bidir_PMSI_HLI: 0x00000, MLDP-added: [RD 0, ID 0,
Bidir ID 0, Remote Bidir ID 0], Counts(SHR/SRC/DM/DEF-MD): 1, 1, 0, 0, Bidir: GRE RP Count
 0, MPLS RP Count 0RSVP-TE added: [Leg 0, Ctrl Leg 0, Part tail 0 Def Tail 0, IR added:
[Def Leg 0, Ctrl Leg 0, Part Leg 0, Part tail 0, Part IR Tail Label 0
  Tree-SID Added: [Def/Part Leaf 0, Def Egress 0, Part Egress 1, Ctrl Leaf 0]
  bgp_i_pmsi: 1,0/0 , bgp_ms_pmsi/Leaf-ad: 1/0, bgp_bidir_pmsi: 0, remote_bgp_bidir_pmsi:
0, PMSIs: I 0x9f77388, 0x0, MS 0x9fa2f98, Bidir Local: 0x0, Remote: 0x0, BSR/Leaf-ad 0x0/0,
 Autorp-disc/Leaf-ad 0x0/0, Autorp-ann/Leaf-ad 0x0/0
 IIDs: I/6: 0x1/0x0, B/R: 0x0/0x0, MS: 0x1, B/A/A: 0x0/0x0/0x0

  Bidir RPF-ID: 16, Remote Bidir RPF-ID: 0
  I-PMSI:   Unknown/None (0x9f77388)
  I-PMSI rem:  (0x0)
  MS-PMSI:   Tree-SID [524292, 192.168.0.4] (0x9fa2f98)
  Bidir-PMSI:  (0x0)
  Remote Bidir-PMSI:  (0x0)
  BSR-PMSI:  (0x0)
  A-Disc-PMSI:  (0x0)
  A-Ann-PMSI:  (0x0)
  RIB Dependency List: 0x9f81370
  Bidir RIB Dependency List: 0x0
    Sources: 1, RPs: 1, Bidir RPs: 0
```

View Default or Partitioned MDT Database

```
Router# show mvpn vrf vpn1 database segment-routing

Core Type    Core Source        Tree Core        State  On-demand Color
                                Information

Default           0.0.0.0            0 (0x00000)  Down   10
Part          192.168.0.4       524292 (0x80004)    Up   10
  Leaf AD Leg:  192.168.0.3
Control       192.168.0.4            0 (0x00000)  Down   10
```

show mrib nsf private

To display the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB), use the **show mrib nsf private**command in the appropriate mode.

show mrib nsf private

Syntax Description

show mrib nsf private	Displays the state of NSF operation in the MRIB.

Command Default

None

Command Modes

XR EXEC mode

Table 3: Release History

Release	Modification
Release 7.10.1	This command was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mrib nsf** command displays the current multicast NSF state for the MRIB. The state may be normal or activated for NSF. The activated state indicates that recovery is in progress due to a failure in MRIB or Protocol Independent Multicast (PIM). The total NSF timeout and time remaining are displayed until NSF expiration.

Table 4: Task ID

Release	Modification
multicast	read

Example

The example shows how to verify the Non Stop Forwarding:

```
Router#show mrib nsf private
Mon Jul 31 13:27:05.056 UTC
IP MRIB Non-Stop Forwarding Status:
Multicast routing state: Normal
   NSF Lifetime:       00:03:00
   Respawn Count: 6
   Last NSF On triggered: Tue Jul 25 13:20:49 2023, 6d00h
   Last NSF Off triggered: Tue Jul 25 13:22:49 2023, 6d00h
   Last NSF ICD Notification sent: Tue Jul 25 13:22:49 2023, 6d00h
   Last Remote NSF On triggered: Tue Jul 25 13:10:18 2023, 6d00h
   Last Remote NSF Off triggered: Tue Jul 25 13:10:27 2023, 6d00h
   Last Label TE NSF On triggered: Tue Jul 25 13:10:18 2023, 6d00h
   Last Label TE NSF Off triggered: Tue Jul 25 13:10:27 2023, 6d00h
```

```
   Last Label mLDP NSF On triggered: Tue Jul 25 13:10:18 2023, 6d00h
   Last Label mLDP NSF Off triggered: Tue Jul 25 13:10:27 2023, 6d00h
   Last Label PIM NSF On triggered: Tue Jul 25 13:20:49 2023, 6d00h
   Last Label PIM NSF Off triggered: Tue Jul 25 13:22:49 2023, 6d00h
   Last Label PIM6 NSF On triggered: Tue Jul 25 13:31:22 2023, 5d23h
   Last Label PIM6 NSF Off triggered: Tue Jul 25 13:33:22 2023, 5d23h
   Last Label XTC NSF On triggered: Tue Jul 25 13:41:51 2023, 5d23h
   Last Label XTC NSF Off triggered: Tue Jul 25 13:41:52 2023, 5d23h

IP NSF :- Active: N, Assume N
MRIB connect timer: Inactive
NSF statistics:
   Enabled Cnt - 4, Disabled Cnt - 4
   Last Enabled: 6d00h, Last Disabled: 6d00h
Multicast COFO routing state: Normal
Current LMRIB clients: LDP RSVP_TE PIM PIM6 XTC
LMRIB NSF clients: LDP RSVP_TE PIM PIM6 XTC
Converged LMRIB clients: LDP RSVP_TE PIM PIM6 XTC
RP/0/RSP0/CPU0:tb8-R2#
```

show ospf routes flex-algo

To display the OSPF routing table for flexible algorithm, use the **show ospf routes flex-algo** command in the EXEC mode.

show ospf routes flex-algo [**number**] [{ *IP prefix / prefix_len* | **route-type** { **external** | **inter** | **intra** } }] [**backup-path**] [**detail**]

Syntax Description

number	Specifies the flexible algorithm number. The range is from 128 to 255.
IP prefix/prefix_len	Specifies IP address along with the subnet mask.
backup-path	Displays the backup-path information of the OSPF routes.
detail	Displays the detailed information of the OSPF routes.
route-typeexternal	Displays OSPF external routes.
route-typeinter	Display OSPF inter area routes.
route-typeintra	Displays OSPF intra area routes.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.5.1	This command was introduced.

Usage Guidelines

Use the **show ospf routes flex-algo** command to display the OSPF private routing table for flexible algorithm (which contains only flexible algorithm routes calculated by OSPF). If there is something wrong with a route in the MPLS forwarding table and RIB, then it is useful to check the OSPF copy of the route to determine if it matches the RIB and MPLS forwarding entries. If it does not match, there is a synchronization problem between OSPF and the MPLS. If the routes match and the route is incorrect, OSPF has made an error in its routing calculation.

Example

This following show output displays the external route type configured:

```
Router#show ospf routes flex-algo 240 route-type external detail
Route Table of ospf-1 with router ID 192.168.0.2 (VRF default)

  Algorithm 240

  Route entry for 192.168.4.3/32, Metric 220, SID 536, Label 16536
   Priority : Medium

     Route type : Extern Type 1
```

```
Last updated : Apr 25 14:30:12.718
     Flags: Inuse

     Prefix Contrib Algo 240 SID 536
      From 192.168.0.4 Route-type 5
      Total Metric : 220 Base metric 20 FAPM 20
      Contrib Flags : Inuse, Reachable
      SID Flags : PHP off, Index, Global, Valid

      Path: 10.1.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2
       Out Label  : 16536
       Weight     : 0
       Area       : 0

      Path: 10.1.2.3, from 192.168.0.4, via GigabitEthernet0/2/0/3
       Out Label  : 16536
       Weight     : 0
       Area       : 0

      Path: 10.2.1.5, from 192.168.0.4, via GigabitEthernet0/2/0/4
       Out Label  : 16536
       Weight     : 0
       Area       : 0

  Route entry for 192.168.4.5/32, Metric 120, SID 556, Label 16556
   Priority : Medium

     Route type : Extern Type 1
     Last updated : Apr 25 14:30:12.724
     Flags: Inuse

     Prefix Contrib Algo 240 SID 556
      From 192.168.0.3 Route-type 5
      Total Metric : 120 Base metric 1 FAPM 20
      Contrib Flags : Inuse, Reachable
      SID Flags : PHP off, Index, Global, Valid

      Path: 10.1.1.3, from 192.168.0.3, via GigabitEthernet0/2/0/2
       Out Label  : 16556
       Weight     : 0
       Area       : 0

      Path: 10.1.2.3, from 192.168.0.3, via GigabitEthernet0/2/0/3
       Out Label  : 16556
       Weight     : 0
       Area       : 0
```

The following show output displays label information for flexible algorithm and its corresponding metric as added in RIB:

```
RP/0/RP0/CPU0:ios# show route 192.168.0.2/32 detail
Wed Apr  6 16:24:46.021 IST

Routing entry for 192.168.0.2/32
  Known via "ospf 1", distance 110, metric 2, labeled SR, type intra area
  Installed Apr  6 15:51:57.973 for 00:32:48
  Routing Descriptor Blocks
    10.10.10.2, from 192.168.0.2, via GigabitEthernet0/2/0/0, Protected
      Route metric is 2
      Label: 0x3 (3)
      Tunnel ID: None
      Binding Label: None
      Extended communities count: 0
      Path id:1       Path ref count:0
```

```
      NHID:0x1(Ref:1)
      Backup path id:65
      OSPF area: 1
    10.11.11.2, from 192.168.0.2, via GigabitEthernet0/2/0/1, Backup (Local-LFA)
      Route metric is 6
      Label: 0x3 (3)
      Tunnel ID: None
      Binding Label: None
      Extended communities count: 0
      Path id:65              Path ref count:1
      NHID:0x2(Ref:1)
      OSPF area:
  Route version is 0x12 (18)
  Local Label: 0x3ee6 (16102)
  Local Label Algo Set (ID, Label, Metric): (1, 16202, 0),(128, 17282, 2)
  IP Precedence: Not Set
  QoS Group ID: Not Set
  Flow-tag: Not Set
  Fwd-class: Not Set
  Route Priority: RIB_PRIORITY_NON_RECURSIVE_MEDIUM (7) SVD Type RIB_SVD_TYPE_LOCAL
  Download Priority 1, Download Version 38
  No advertising protos.
```

The following example shows the backup path for each path:

```
Router#show ospf routes flex-algo 240 route-type external backup-path


Route Table of ospf-1 with router ID 192.168.0.2 (VRF default)

  Algorithm 240

  192.168.4.3/32, Metric 220, SID 536, Label 16536
      10.1.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2
           Backup path:
              10.23.2.3, from 192.168.0.4, via GigabitEthernet0/2/0/3,
              Out Label: 16536
              Attributes: Metric: 220, Primary , Downstream, Interface Disjoint, SRLG
Disjoint
      10.1.2.3, from 192.168.0.4, via GigabitEthernet0/2/0/3
           Backup path:
              10.23.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2,
              Out Label: 16536
              Attributes: Metric: 220, Primary , Downstream, Interface Disjoint, SRLG
Disjoint
      10.1.1.5, from 192.168.0.4, via GigabitEthernet0/2/0/4
           Backup path:
              10.23.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2,
              Out Label: 16536
             Attributes: Metric: 220, Primary , Downstream, Node Protect, Interface Disjoint,
 SRLG Disjoint
  192.168.4.5/32, Metric 120, SID 556, Label 16556
      10.1.1.3, from 192.168.0.3, via GigabitEthernet0/2/0/2
           Backup path:
              10.23.2.3, from 192.168.0.3, via GigabitEthernet0/2/0/3,
              Out Label: 16556
              Attributes: Metric: 120, Primary , Downstream, Interface Disjoint, SRLG
Disjoint
      10.1.2.3, from 192.168.0.3, via GigabitEthernet0/2/0/3
           Backup path:
              10.1.1.3, from 192.168.0.3, via GigabitEthernet0/2/0/2,
              Out Label: 16556
              Attributes: Metric: 120, Primary , Downstream, Interface Disjoint, SRLG
Disjoint
```

The following example shows details of the route, but not the backup paths:

```
Router#show ospf routes flex-algo 240 route-type external detail

Route Table of ospf-1 with router ID 192.168.0.2 (VRF default)

  Algorithm 240

  Route entry for 192.168.4.3/32, Metric 220, SID 536, Label 16536
   Priority : Medium

     Route type : Extern Type 1
     Last updated : Apr 25 14:30:12.718
     Flags: Inuse

     Prefix Contrib Algo 240 SID 536
      From 192.168.0.4 Route-type 5
      Total Metric : 220 Base metric 20 FAPM 20
      Contrib Flags : Inuse, Reachable
      SID Flags : PHP off, Index, Global, Valid

      Path: 10.1.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2
       Out Label  : 16536
       Weight     : 0
       Area       : 0

      Path: 10.1.2.3, from 192.168.0.4, via GigabitEthernet0/2/0/3
       Out Label  : 16536
       Weight     : 0
       Area       : 0

      Path: 10.2.1.5, from 192.168.0.4, via GigabitEthernet0/2/0/4
       Out Label  : 16536
       Weight     : 0
       Area       : 0

  Route entry for 192.168.4.5/32, Metric 120, SID 556, Label 16556
   Priority : Medium

     Route type : Extern Type 1
     Last updated : Apr 25 14:30:12.724
     Flags: Inuse

     Prefix Contrib Algo 240 SID 556
      From 192.168.0.3 Route-type 5
      Total Metric : 120 Base metric 1 FAPM 20
      Contrib Flags : Inuse, Reachable
      SID Flags : PHP off, Index, Global, Valid

      Path: 10.1.1.3, from 192.168.0.3, via GigabitEthernet0/2/0/2
       Out Label  : 16556
       Weight     : 0
       Area       : 0

      Path: 10.1.2.3, from 192.168.0.3, via GigabitEthernet0/2/0/3
       Out Label  : 16556
       Weight     : 0
       Area       : 0
```

The following example shows details of the route and backup paths:

```
Router#show ospf routes flex-algo 240 route-type external backup-path detail
```

```
Route Table of ospf-1 with router ID 192.168.0.2 (VRF default)

  Algorithm 240

  Route entry for 192.168.4.3/32, Metric 220, SID 536, Label 16536
   Priority : Medium

     Route type : Extern Type 1
     Last updated : Apr 25 14:30:12.718
     Flags: Inuse

     Prefix Contrib Algo 240 SID 536
      From 192.168.0.4 Route-type 5
      Total Metric : 220 Base metric 20 FAPM 20
      Contrib Flags : Inuse, Reachable
      SID Flags : PHP off, Index, Global, Valid

      Path: 10.1.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2
       Out Label  : 16536
       Weight     : 0
       Area       : 0

           Backup path:
              10.1.2.3, from 192.168.0.4, via GigabitEthernet0/2/0/3,
              Out Label: 16536
              Attributes: Metric: 220, Primary , Downstream, Interface Disjoint, SRLG
Disjoint

      Path: 23.23.2.3, from 192.168.0.4, via GigabitEthernet0/2/0/3
       Out Label  : 16536
       Weight     : 0
       Area       : 0

           Backup path:
              10.1.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2,
              Out Label: 16536
              Attributes: Metric: 220, Primary , Downstream, Interface Disjoint, SRLG
Disjoint

      Path: 25.25.1.5, from 192.168.0.4, via GigabitEthernet0/2/0/4
       Out Label  : 16536
       Weight     : 0
       Area       : 0

           Backup path:
              10.1.1.3, from 192.168.0.4, via GigabitEthernet0/2/0/2,
              Out Label: 16536
             Attributes: Metric: 220, Primary , Downstream, Node Protect, Interface Disjoint,
 SRLG Disjoint

  Route entry for 192.168.4.5/32, Metric 120, SID 556, Label 16556
   Priority : Medium

     Route type : Extern Type 1
     Last updated : Apr 25 14:30:12.724
     Flags: Inuse

     Prefix Contrib Algo 240 SID 556
      From 192.168.0.3 Route-type 5
      Total Metric : 120 Base metric 1 FAPM 20
      Contrib Flags : Inuse, Reachable
      SID Flags : PHP off, Index, Global, Valid

      Path: 10.1.1.3, from 192.168.0.3, via GigabitEthernet0/2/0/2
```

```
        Out Label  : 16556
        Weight     : 0
        Area       : 0

            Backup path:
               10.1.2.3, from 192.168.0.3, via GigabitEthernet0/2/0/3,
               Out Label: 16556
               Attributes: Metric: 120, Primary , Downstream, Interface Disjoint, SRLG
Disjoint

      Path: 10.1.2.3, from 192.168.0.3, via GigabitEthernet0/2/0/3
        Out Label  : 16556
        Weight     : 0
        Area       : 0

            Backup path:
               10.1.1.3, from 192.168.0.3, via GigabitEthernet0/2/0/2,
               Out Label: 16556
               Attributes: Metric: 120, Primary , Downstream, Interface Disjoint, SRLG
Disjoint
```

show ospf segment-routing prefix-sid-map

To verify the active and backup prefix-to-SID mappings for OSPF, use the **show ospf segment-routing prefix-sid-map** command.

show ospf segment-routing prefix-sid-map [**active-policy** | **backup-policy**]

Syntax Description

active-policy	(Optional) Specifies the active mapping policy.
backup-policy	(Optional) Specifies the backup mapping policy.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ospf	read

Example

The example shows how to verify the active mapping policy on OSPF:

```
RP/0/0/CPU0:router# show ospf segment-routing prefix-sid-map active-policy

        SRMS active policy for Process ID 1

Prefix              SID Index    Range        Flags
1.1.1.100/32        100          20
1.1.1.150/32        150          10

Number of mapping entries: 2
```

The example shows how to verify the backup mapping policy on OSPF:

```
RP/0/0/CPU0:router# show ospf segment-routing prefix-sid-map backup-policy

        SRMS backup policy for Process ID 1

Prefix              SID Index    Range        Flags
```

```
1.1.1.100/32         100          20
1.1.1.150/32         150          10

Number of mapping entries: 2
```

Related Commands

Command	Description
segment-routing mapping-server, on page 88	Configures the segment routing mapping server (SRMS).
segment-routing prefix-sid-map advertise-local	Enables the router to advertise the SRMS entries that are locally configured.
segment-routing prefix-sid-map receive disable	Disables mapping client functionality.
show isis segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for IS-IS.
show segment-routing mapping-server prefix-sid-map	Displays the locally configured prefix-to-SID mappings.

show pce lsp p2mp

To view IP VPN multicast traffic details (such as LSP details) on the SR-PCE server, use the **show pce lsp p2mp** command in EXEC mode.

show pce lsp p2mp [**root ipv4** *address*] [*tree-ID*]

Syntax Description

root ipv4 *address*	(Optional) The multicast tree's root router IP address. Information will be displayed for the specified router.
tree-ID	(Optional) Multicast tree SID used (by multicast routers and the SR-PCE server) for transporting the IP VPN multicast traffic. Information will be displayed for the specified Tree-SID.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Example

The following example shows how to view IP VPN multicast traffic details on the SR-PCE server. The routes are created and managed by the SR-PCE server.

View SR-PCE Multicast Tree Configuration Information

```
Router# show pce lsp p2mp

Tree: sr_p2mp_root_192.168.0.1_tree_id_524290
 Label:    18000     Operational: up  Admin: up
 Metric Type: TE
 Transition count: 3
 Uptime: 00:00:03 (since Fri Jan 24 14:57:51 PST 2020)
 Source: 192.168.0.1
 Destinations: 192.168.0.4
 Nodes:
  Node[0]: 192.168.0.2 (rtrM)
   Role: Transit
   Hops:
    Incoming: 18000 CC-ID: 4
    Outgoing: 18000 CC-ID: 4 (17.17.17.4) [rtrR]
  Node[1]: 192.168.0.1 (rtrL1)
   Role: Ingress
   Hops:
    Incoming: 18000 CC-ID: 5
    Outgoing: 18000 CC-ID: 5 (12.12.12.2) [rtrM]
  Node[2]: 192.168.0.4 (rtrR)
   Role: Egress
   Hops:
    Incoming: 18000 CC-ID: 6
```

For dynamic SR multicast trees created for MVPN, the **show** command has filters to view root multicast router and Tree-ID information. When the root router is specified, all multicast trees from that root are displayed. When root and Tree-ID are specified, only the specified tree information is displayed.

```
Router# show pce lsp  p2mp root ipv4 1.1.1.1 524289

Tree: sr_p2mp_root_1.1.1.1_tree_id_524289, Root: 1.1.1.1 ID: 524289
 Label:    20000     Operational: up  Admin: up
 PCC: 1.1.1.1

 Local LFA FRR: Disabled
 Metric Type: TE
 Transition count: 11
 Uptime: 00:03:37 (since Mon May 11 12:53:33 PDT 2020)
 Destinations: 1.1.1.3, 1.1.1.4, 1.1.1.5
 Nodes:
  Node[0]: 1.1.1.1 (root1)
   Role: Ingress
   Hops:
    Incoming: 20000 CC-ID: 26
    Outgoing: 20000 CC-ID: 26 (192.168.114.4) [mid-4]
    Outgoing: 20000 CC-ID: 26 (192.168.112.2) [mid-2]
  Node[1]: 1.1.1.4 (mid-4)
   Role: Egress
   Hops:
    Incoming: 20000 CC-ID: 27
  Node[2]: 1.1.1.2 (mid-2)
   Role: Transit
   Hops:
    Incoming: 20000 CC-ID: 28
    Outgoing: 20000 CC-ID: 28 (192.168.123.3) [leaf-3]
    Outgoing: 20000 CC-ID: 28 (192.168.125.5) [leaf-5]
  Node[3]: 1.1.1.3 (leaf-3)
   Role: Egress
   Hops:
    Incoming: 20000 CC-ID: 29
  Node[4]: 1.1.1.5 (leaf-5)
   Role: Egress
   Hops:
    Incoming: 20000 CC-ID: 30
```

The following output shows that LFA FRR is enabled on the hop from rtrR to rtrM. Unlike typical multicast replication where the address displayed is the remote address on the link to a downstream router, the IP address 192.168.0.3 (displayed with an exclamation mark) is the router-ID of the downstream router rtrM. The output also displays the LFA FRR state for the multicast tree.

```
Router# show pce lsp p2mp

Tree: sr_p2mp_root_192.168.0.4_tree_id_524290
 Label:    18000     Operational: up  Admin: up
 LFA FRR: Enabled
 Metric Type: TE
 Transition count: 1
 Uptime: 3d19h (since Thu Feb 13 13:43:40 PST 2020)
 Source: 192.168.0.4
 Destinations: 192.168.0.1, 192.168.0.2
 Nodes:
  Node[0]: 192.168.0.3 (rtrM)
   Role: Transit
   Hops:
    Incoming: 18000 CC-ID: 1
    Outgoing: 18000 CC-ID: 1 (12.12.12.1) [rtrL1]
```

```
  Outgoing: 18000 CC-ID: 1 (15.15.15.2) [rtrL2]
Node[1]: 192.168.0.4 (rtrR)
 Role: Ingress
 Hops:
  Incoming: 18000 CC-ID: 2
  Outgoing: 18000 CC-ID: 2 (192.168.0.3!) [rtrM]
Node[2]: 192.168.0.1 (rtrL1)
 Role: Egress
 Hops:
  Incoming: 18000 CC-ID: 3
Node[3]: 192.168.0.2 (rtrL2)
 Role: Egress
 Hops:
  Incoming: 18000 CC-ID: 4
```

show performance-measurement history

To display the history for delay-measurement, use the **performance-measurement history** show command in XR EXEC mode.

show performance-measurement history { **probe-computation** | **advertisement** | **aggregation** } { **interfaces** | **endpoint** | **rsvp-te** | **sr-policy** }

Syntax Description

probe-computation	(Optional) Displays information for the delay metric computation result within each probe interval.
advertisement	(Optional) Displays information for the delay metric computation result within each advertisement interval.
aggregation	(Optional) Displays information for the delay metric computation result within each aggregation interval.
interface	(Optional) Displays information on the specified interface.
endpoint	(Optional) Displays information on the specified endpoint.
rsvp-te	(Optional) Displays information on the specified Resource Reservation Protocol - Traffic Engineering (RSVP-TE).
sr-policy	(Optional) Displays information on the specified sr-policy.

Command Default

No default

Command Modes

XR EXEC

Command History

Release	Modification
Release 24.1.1	This command was updated with synthetic and anomaly loss information.
Release 7.3.1	This command was introduced.

Task ID

Task ID	Operation
performance-measurement	write/read

```
Router# show performance-measurement history probe-computation interfaces
Interface Name: GigabitEthernet0/2/0/0 (ifh: 0x1000020)
Delay-Measurement history (uSec):
  Probe Start Timestamp     Pkt(TX/RX)   Average       Min       Max
  Aug 01 2023 08:04:15.230       10/10       704       651       779
```

```
Router# show performance-measurement history probe-computation endpoint
Endpoint name: IPv4-192.168.0.4-vrf-default
  …
```

```
  Segment-List              : None
    Delay-Measurement history (uSec):
      Probe Start Timestamp     Pkt(TX/RX)   Average       Min       Max
      Aug 01 2023 08:26:48.823       10/10      3399      2962      3808
```

```
Router# show performance-measurement history aggregation rsvp-te
...
Delay-Measurement history (uSec):
      Aggregation Timestamp     Pkt(TX/RX)   Average       Min       Max
      Aug 01 2023 08:37:23.702       40/40      3372      3172      4109
```

```
Router# show performance-measurement history advertisement sr-policy
...
Delay-Measurement history (uSec):
          Advertisement Timestamp   Pkt(TX/RX)   Average       Min       Max        Reason
          Aug 01 2023 10:05:14.072       24/24      3408      3408      3408     ACCEL-MAX
```

Table 5: This table gives show performance-measurement history field descriptions:

Field	Description
TX	Number of packets sent.
RX	Number of packets received.
Average	Average delay of all the delay measures within one probe.
Max	Maximum delay of all the delay measures within one probe.
Min	Minimum delay of all the delay measures within one probe.

Reason	Provides the reason for the delay in packets:" • NONE : No advertisements occurred • PER-AVG : Periodic timer, average delay threshold crossed • PER-MIN : Periodic timer, min delay threshold crossed • PER-MAX : Periodic timer, max delay threshold crossed • ACCEL-AVG : Accelerated threshold crossed, average delay threshold crossed • ACCEL-MIN : Accelerated threshold crossed, min delay threshold crossed • ACCEL-MAX : Accelerated threshold crossed, max delay threshold crossed • ACCEL-UP-AVG : Accelerated threshold crossed, average delay upper-bound crossed • ACCEL-UP-MIN : Accelerated threshold crossed, min delay upper-bound crossed • ACCEL-UP-MAX : Accelerated threshold crossed, max delay upper-bound crossed • ANOM-MIN-DYN : Min delay A flag toggled and dynamic delay is in effect • ANOM-MIN-STA : Min delay A flag toggled and static delay is in effect • FIRST : First advertisement • NEW-SESSION : New child session • ENABLE : Advertisement enabled • DISABLE : Advertisement disabled • DELETE : Session deleted • EXEC-CLEAR : Cleared through exec command • ADV-CFG : Advertise delay config • ADV-UNCFG : Advertise delay unconfig • ERROR : Control code error • LINK-DOWN : Link state changed to down • SESSION-ERROR : Performance measurement session error • DYN-DM : Dynamic delay advertisement is in effect • PT-CFG : Path tracing config • PT-UNCFG : Path tracing unconfig • PT-INTF_READY : Path tracing interface ready • PKT-LOSS : Packet loss detected • ANOM-PKT-LOSS : PM session anomaly due to packet loss • N/A : Invalid advertisement reason

show pim vrf

To view SR multicast tree information for *data* MDTs, including cache, router-local, and remote MDT information, use the **show pim vrf** command in EXEC mode.

show pim vrf *name* **mdt sr-p2mp** { **local tree-id** *value* | **remote** | **cache** [*core-src-ip-add* [*cust-src-ip-add cust-grp-ip-add*]] }

Syntax Description

vrf *name*	VRF for which information is to be displayed.
mdt sr-p2mp	Specifies that the multicast traffic is transported using SR multicast. The MDT-specific information that is to be displayed, has to be provided from the subsequent choices. Based on the chosen option, information is displayed.
local tree-id *value*	Specifies a locally assigned Tree-SID of the *data* MDT core tree.
remote	Specifies a Tree-SID of the *data* MDT tree that is learnt from remote PE routers.
cache [*core-src-ip-add* [*cust-src-ip-add cust-grp-ip-add*]]	Specifies data MDT cache information.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Example

You can view SR multicast tree information for *data* MDTs, including cache, router-local, and remote MDT information, with these commands.

View Data MDT Cache Information

```
Router# show pim vrf vpn1 mdt cache

Core Source      Cust (Source, Group)               Core Data        Expires
192.168.0.3      (26.3.233.1, 232.0.0.1)            [tree-id 524292]  never
192.168.0.4      (27.3.233.6, 232.0.0.1)            [tree-id 524290]  never
   Leaf AD:  192.168.0.3
```

View Local MDT information

```
Router# show pim vrf vpn1 mdt sr-p2mp local

Tree                          MDT            Cache DIP Local VRF Routes  Ondemand
Identifier                    Source         Count     Entry Using Cache Color
[tree-id 524290 (0x80002)]    192.168.0.4    1     N   Y     1           10
   Tree-SID Leaf:  192.168.0.3
```

Remote MDT information

```
Router # show pim vrf vpn1 mdt sr-p2mp remote

Tree                            MDT             Cache DIP Local VRF Routes  On-demand
Identifier                      Source          Count     Entry Using Cache Color
[tree-id 524290 (0x80002)]      192.168.0.4     1     N   N     1           0
```

show segment-routing mapping-server prefix-sid-map

To verify the locally configured prefix-to-SID mappings, use the **show segment-routing mapping-server prefix-sid-map** command.

show segment-routing mapping-server prefix-sid-map [**ipv4** | **ipv6**] [*prefix*] [**detail**]

Syntax Description

ipv4	(Optional) Specifies an IPv4 address family.
ipv6	(Optional) Specifies an IPv6 address family.
prefix	(Optional) Specifies a prefix.
detail	(Optional) Displays detailed information on the prefix-to-SID mappings.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
	read

Example

The example shows how to verify the IPv4 prefix-to-SID mappings:

```
RP/0/0/CPU0:router# show segment-routing mapping-server prefix-sid-map ipv4
Prefix               SID Index    Range        Flags
20.1.1.0/24          400          300
10.1.1.1/32          10           200
Number of mapping entries: 2
```

The example shows how to display detailed information on the IPv4 prefix-to-SID mappings:

```
RP/0/0/CPU0:router# show segment-routing mapping-server prefix-sid-map ipv4 detail
Prefix
20.1.1.0/24
    SID Index:      400
```

```
    Range:          300
    Last Prefix:    20.2.44.0/24
    Last SID Index: 699
    Flags:
10.1.1.1/32
    SID Index:      10
    Range:          200
    Last Prefix:    10.1.1.200/32
    Last SID Index: 209
    Flags:
Number of mapping entries: 2
```

Related Commands

Command	Description
segment-routing mapping-server, on page 88	Configures the segment routing mapping server (SRMS).
segment-routing prefix-sid-map advertise-local	Enables the router to advertise the SRMS entries that are locally configured.
segment-routing prefix-sid-map receive disable	Disables mapping client functionality.
show isis segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for IS-IS.
show ospf segment-routing prefix-sid-map	Displays the active and backup prefix-to-SID mappings for OSPF.

show segment-routing srv6 sid

You can use the **show segment-routing srv6 sid** command to verify the SRv6 global and locator configuration.

show segment-routing srv6 sid

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.8.1	This command output was modified.
Release 7.0.12	This command was introduced.

Usage Guidelines

The command displays SID information across locators. By default, only “active” (i.e. non-stale) SIDs are displayed.

From IOS XR Release 7.8.1, IOS XR nodes with SRv6 Micro-SID F3216 format will accept and allow service SIDs received from non-IOS XR node peers with SRv6 base F128. Non-IOS XR node peers can be without SID Struct TLV (SSTLV), or with an incompatible SSTLV having an SID that is F3216 compatible. This allows for interoperability without any IETF extension or configuration changes on the Non-IOS XR peer node.

The following example shows how to display detailed information on the remote side, with the allocation type:

```
Router# show segment-routing srv6 locator usid sid fccc:ccc1:1:e00f::
 Mon Dec 13 15:58:53.640 EST
 SID                         Behavior          Context                           Owner
           State  RW
 --------------------------  ----------------  ------------------------------
------------------  -----  --
 fccc:ccc1:1:e00f::          uDT46             '**iid'
rib_lib_test_xtf    InUse  Y
   SID Function: 0xe00f
   SID context: { '**iid' }
     App data: [0000000000000000]
   Locator: 'usid'
   Allocation type: Dynamic | Explicit
```

show segment-routing traffic-eng p2mp policy

To view SR-TE multicast policy information that is used for transporting IP VPN multicast traffic, use the **show segment-routing traffic-eng p2mp policy** command in EXEC mode.

show segment-routing traffic-eng p2mp policy [{ **name** *policy* | **root ipv4** *address* [*tree-ID*] }]

Syntax Description

name *policy*	Policy for which information is to be displayed.
root ipv4 *address* [*tree-ID*]	Specifies that information be displayed for the specified multicast tree root router and the Tree-SID.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Example

The following example shows how to view SR-TE multicast policy information.

Multicast Tree Information on Routers

```
Router# show segment-routing traffic-eng p2mp policy

SR-TE P2MP policy database:
---------------------
! - Replications with Fast Re-route

Policy: sr_p2mp_root_192.168.0.1_tree_id_524290  LSM-ID: 0x2
 Role: Leaf
 Replication:
  Incoming label: 18001 CC-ID: 6

Policy: sr_p2mp_root_192.168.0.4_tree_id_524290  LSM-ID: 0x80002 (PCC-initiated)
 Color: 0
 LFA FRR: Disabled
 Role: Root
 Replication:
  Incoming label: 18000 CC-ID: 2
  Interface: None [192.168.0.3!]  Outgoing label: 18000 CC-ID: 2
 Endpoints:
  192.168.0.1, 192.168.0.2
```

For SR multicast policies originated locally on the router (root router of a dynamic MVPN multicast policy) additional policy information is displayed. The information includes color, end points, and whether LFA FRR is requested by the local application. When the SR-PCE server enables LFA FRR on a specific hop, the outgoing information shows the address of the next router with an exclamation mark and None is displayed for the outgoing interface.

For dynamic SR multicast trees created for MVPN, the **show** command has filters for displaying root multicast router and Tree-ID information. When the root router is specified, all multicast trees for that root are displayed. When root and Tree-ID are specified, only the specified tree information is displayed.

```
Router# show segment-routing traffic-eng p2mp policy root ipv4 1.1$

SR-TE P2MP policy database:
---------------------
! - Replications with Fast Re-route, * - Stale dynamic policies/endpoints

Policy: sr_p2mp_root_1.1.1.1_tree_id_524289  LSM-ID: 0x691
 Root: 1.1.1.1, ID: 524289
 Role: Transit
 Replication:
  Incoming label: 20000 CC-ID: 28
  Interface: Bundle-Ether23 [192.168.123.3]  Outgoing label: 20000 CC-ID: 28
  Interface: Bundle-Ether25 [192.168.125.5]  Outgoing label: 20000 CC-ID: 28

Policy: sr_p2mp_root_1.1.1.1_tree_id_524290  LSM-ID: 0x692
 Root: 1.1.1.1, ID: 524290
 Role: Transit
 Replication:
  Incoming label: 19999 CC-ID: 28
  Interface: Bundle-Ether23 [192.168.123.3]  Outgoing label: 19999 CC-ID: 28
  Interface: Bundle-Ether25 [192.168.125.5]  Outgoing label: 19999 CC-ID: 28
```

show segment-routing local-block inconsistencies

Displays any segment routing local block (SRLB) label inconsistencies.

show segment-routing local-block inconsistencies

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When a new SRLB range is defined, there might be a label conflict (for example, if labels are already allocated, statically or dynamically, in the new SRLB range). In this case, the new SRLB range will be accepted, but not applied (pending). The previous SRLB range (active) will continue to be in use until one of the following occurs:

- Reload the router to release the currently allocated labels and allocate the new SRLB
- Use the **clear segment-routing local-block discrepancy all** command to clear the label conflicts

Task ID

Task ID	Operation

Example

This example shows how to display the SRGB inconsistencies:

```
RP/0/RSP0/CPU0:router(config)# show segment-routing local-block inconsistencies
Tue Aug 15 13:53:30.555 EDT
SRLB inconsistencies range: Start/End: 30000/30009
```

Related Commands

Command	Description
clear segment-routing local-block discrepancy all, on page 13	Clears SRLB label conflicts
segment-routing local-block, on page 86	Configures the SRLB

srv6 mode base encapsulation

To enter the SRv6 encapsulation submode, use the **encapsulation** command in the SRv6 base configuration mode.

hw-module profile segment-routing srv6 mode base encapsulation

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Segment routing base mode configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

You must reload the router after enabling this feature.

Task ID

Task ID	Operation
system	read, write

The following example shows how to enter the SRv6 encapsulation submode.

```
Router# configure
Router(config)# hw-module profile segment-routing srv6 mode base encapsulation
```

traceroute sr-mpls

To trace the routes to a destination in a segment routing network, use the **traceroute sr-mpls** command in XR EXEC mode.

traceroute sr-mpls { *ipv4-address/mask* | *ipv6-address/mask* [**fec-type** { **bgp** | **generic** | **igp** { **ospf** | **isis** } }] | **multipath** { *ipv4-address/mask* | *ipv6-address/mask* [**fec-type** { **bgp** | **generic** | **igp** { **ospf** | **isis** } } } | **nil-fec** | **dataplane-only** { **labels** { *label1* [**,** *label2...*] *ipv4-address/mask* | *ipv6-address/mask* | **policy** } } { **output** { **interface** *interface-path-id* } } { **nexthop** *next-hop-ip-address* } }

Syntax Description

ipv4 address/mask or *ipv6 address/mask*	Address prefix of the target and number of bits in the target address network mask.
fec-type	(Optional) Specifies FEC type to be used. Default FEC type is generic. **bgp** Use FEC type as BGP. **generic** Use FEC type as generic. **igp** Use FEC type as OSPF or ISIS.
labels *label,label...*	Specifies the label stack. Use commas to separate each label.
output interface *interface-path-id*	Specifies the output interface where echo request packets are sent.
nexthop *next-hop-ip-address*	Causes packets to go through the specified IPv4 or IPv6 next-hop address.

Command Default

fec-type : generic

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For SR-TE policies, provide a valid LSP endpoint for non-Nil-FEC traceroute operation.

Task ID

Task ID	Operations
mpls-te	read, write

Example

These examples show how to use segment routing traceroute to trace the LSP for a specified IPv4 prefix segment routing id (SID). In the first example, FEC type is not specified. You can also specify the FEC type as shown in the second example. The third example uses multipath traceroute to discover all the possible paths for a IPv4 prefix SID.

```
RP/0/RP0/CPU0:router# traceroute sr-mpls 10.1.1.2/32

Tracing MPLS Label Switched Path to 10.1.1.2/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 3 ms


RP/0/RP0/CPU0:router# traceroute sr-mpls 10.1.1.2/32  fec-type  igp ospf

Tracing MPLS Label Switched Path to 10.1.1.2/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 2 ms


RP/0/RP0/CPU0:router# traceroute sr-mpls multipath 10.1.1.2/32

Starting LSP Path Discovery for 10.1.1.2/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
```

```
!
Path 0 found,
 output interface GigabitEthernet0/0/0/2 nexthop 10.13.13.2
source 10.13.13.1 destination 127.0.0.0
!
Path 1 found,
 output interface Bundle-Ether1 nexthop 10.12.12.2
source 10.12.12.1 destination 127.0.0.0

Paths (found/broken/unexplored) (2/0/0)
Echo Request (sent/fail) (2/0)
Echo Reply (received/timeout) (2/0)
Total Time Elapsed 14 ms
```

UCMP Disable

To disable Unequal-Cost Multiple Path (UCMP) for specific Flexible Algorithm use this command in ISIS Address Family submode.

UCMP Disable

Syntax Description

UCMP Disable	Disables UCMP functionality.

Command Default

None.

Command Modes

IS-IS interface address-family configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

UCMP must be configured at the ISIS Address Family instance.

Task ID

Task ID	Operations
isis	read, write

Examples

Example configuration to disable UCMP of specific Flexible Algorithm. Here, it is Flex-algo 128

```
Router(config)# router isis 1
Router(config-isis-flex-algo)# flex-algo 128
Router(config-isis-flex-algo)# ucmp disable
```

Segment Routing Traffic Engineering Commands

This chapter describes the commands used to configure and use Segment Routing Traffic Enginering.

Note All commands applicable to the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

accounting prefixes ipv6 mode

To enable SRv6 traffic accounting, use the **accounting prefixes ipv6 mode** command in XR Config mode.

accounting prefixes ipv6 mode per-prefix per-nexthop srv6-locator

Syntax Description

per-prefix	Enables accounting for every prefix.
per-nexthop	Enables accounting for every prefix and nexthop.
srv6-locator	Enables accounting only for Segment-routing SRv6 locator.

Command Default

None

Command Modes

XR Config

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

The following example shows how to enable SRv6 traffic accounting:

```
Router(config)#accounting prefixes ipv6 mode per-prefix per-nexthop srv6-locators
```

affinity (SR-TE)

To configure a named interface link admin group by assigning affinity to an interface, use the **affinity name** *NAME* command in SR-TE interface submode.

affinity name *name*

Syntax Description

name	Affinity color name

Command Default

None

Command Modes

SR-TE interface

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Named Interface Link Admin Groups let you assign, or map, up to 32 color names for affinity and attribute-flag attributes instead of 32-bit hexadecimal numbers. After mappings are defined, the attributes can be referred to by the corresponding color name in the CLI.

Example

The following example shows how to assign affinity to interfaces:

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# interface TenGigE0/0/1/2
Router(config-sr-if)# affinity
Router(config-sr-if-affinity)# name RED
```

affinity-map (SR-TE)

To define an affinity map, use the **affinity-map name** *name* **bit-position** *bit-position* command in SR-TE sub-mode.

affinity-map name *name* **bit-position** *bit-position*

Syntax Description

name *name*	Specify the name of the affinity-map.
bit-position *bit-position*	Specify the bit position in the Extended Admin Group bitmask. The *bit-position* range is from 0 to 255.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Configure affinity maps on the following routers:

- Routers with interfaces that have an associated admin group attribute.
- Routers that act as SR-TE head-ends for SR policies that include affinity constraints.

Example

The following example shows how to define affinity maps.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# affinity-map
Router(config-sr-te-affinity-map)# name RED bit-position 23
```

autoroute include ipv6 all

To enable IPv6 autoroute support for SR-TE policies with IPv4 endpoints, use the **autoroute include ipv6 all** command in the SR-TE policy and PCC profile modes. To disable this feature, use the **no** form of this command.

autoroute include ipv6 all
no autoroute include ipv6 all

Syntax Description

This command has no keywords or arguments.

Command Default

IPv6 autoroute support is disabled.

Command Modes

SR-TE policy

PCC profile

Command History

Release	Modification
Release 7.3.4	This command was introduced.

Usage Guidelines

The **include ipv6 all** command form enables autoroute support for IPv6 prefixes, for a specified SR-TE policy. This command can be used in the SR-TE policy and PCC profile modes.

Example

The following example shows how to configure the IPv6 autoroute function for an SR-TE policy with an IPv4 endpoint:

```
Router# configure
Router(config)# segment-routing traffic-eng policy pol12
Router(config-sr-te-policy)# autoroute include ipv6 all
Router(config-sr-te-policy)# commit
```

The following example shows how to configure the IPv6 autoroute function for a PCE-instantiated SR-TE policy with an IPv4 endpoint:

```
Router# configure
Router(config)# segment-routing traffic-eng pcc profile 10
Router(config-pcc-prof)# autoroute include ipv6 all
Router(config-pcc-prof)# commit
```

bfd timers

To specify how long to wait for new BFD session to come up, use the **bfd timers** command in SR-TE sub-mode.

bfd timers session-bringup *seconds*

Syntax Description

seconds	Specify how long to wait for new BFD session to come up, in seconds. The range is from 10 to 3600.

Command Default

The default BFD session bring-up timer is 60 seconds.

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to configure the BFD session timer.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# bfd timers session-bringup 90
```

bgp bestpath igp-metric sr-policy

To configure BGP best path selection based on SR policy metrics in an SR-TE domain, use the **bgp bestpath igp-metric sr-policy** command in BGP configuration mode on the headend router. To remove the configuration, use the **no** form of the command.

bgp bestpath igp-metric sr-policy

Syntax Description

This command has no keywords or arguments.

Command Default

BGP best path selection based on SR policy metrics is disabled.

Command Modes

BGP configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Example

The following example shows how to configure BGP best path selection based on SR policy metrics (over IGP metric) in an SR-TE domain:

```
RR # configure
RR (config) # router bgp 100
RR (config-bgp)# bgp bestpath igp-metric sr-policy
RR (config-bgp)# commit
RR (config-bgp)# end
```

bgp prefix-path-label ignore

To indicate BGP to ignore the programming of the service route's prefix label when recursing onto the BSID of an SR-TE policy, use the **bgp prefix-path-label ignore** command in SR-TE policy steering config mode.

bgp prefix-path-label ignore

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

SR-TE policy steering

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

This command can be configured for manual SR policies.

Example

The following example shows how to configure BGP to ignore the programming of the service route's prefix label when recursing onto the BSID of an SR-TE policy:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# steering
Router(config-sr-te-policy-steering)# bgp prefix-path-label ignore
```

binding-sid (SR-TE)

To specify the binding SID (BSID) allocation behavior, use the **binding-sid** command in SR-TE sub-mode.

binding-sid { **dynamic disable** | **explicit** { **enforce-srlb** | **fallback-dynamic** } }

Syntax Description

dynamic disable	Disables dynamic binding SID allocation. Candidate paths without an explicit BSID will be considered invalid.
explicit enforce-srlb	Specifies strict SRLB enforcement. If the BSID is not within the SRLB, the policy stays down.
explicitfallback-dynamic	Specifies that, if the BSID is not available, the BSID is allocated dynamically and the policy comes up.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

Explicit BSIDs are allocated from the segment routing local block (SRLB) or the dynamic range of labels. A best-effort is made to request and obtain this BSID for the SR-TE policy. If requested BSID is not available (if it does not fall within the available SRLB or is already used by another application or SR-TE policy), the policy stays down.

Use this command to specify how the BSID allocation behaves if the BSID value is not available.

Example

The following example shows how to specify how the BSID allocation behaves if the BSID value is not available.

Fallback to dynamic allocation:

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# binding-sid explicit fallback-dynamic
```

Strict SRLB enforcement:

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# binding-sid explicit enforce-srlb
```

distribute link-state

To enable reporting of SRTE policies, use the **distribute link-state** command in the SR-TE configuration mode.

distribute link-state [**report-candidate-path-inactive**]

Table 6: Syntax Description:

Syntax	Description
report-candidate-path-inactive	Enables reporting of SRTE policies using BGP-LS.

Command Default

The reporting of policies to BGP-LS is disabled by default.

Command Modes

SR-TE configuration (config-sr-te)

Command History

Release	Modification
Release 24.1.1	Supports reporting of SR-TE policies using BGP- Link State for SRv6.
Release 7.10.1	This command was introduced and supports reporting of SR-TE policies using BGP- Link State for SR-MPLS.

Task ID

Task ID	Operation
distribute link-state	write/read

Example

This example shows how to enable BGP-LS reporting and syncing of SRTE Policies:

```
Router# config
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# distribute link-state
Router(config-sr-te-distribute-ls)# report-candidate-path-inactive
Router(config-sr-te-distribute-ls)# exit
```

effective-metric

effective-metric admin-distance metric-type { **igp** | **te** | **latency** | **hopcount** | **unknown** } **admin-distance** *distance*

Syntax Description

admin-distance metric-type	Specify the metric type.
admin-distance *distance*	Specify the admin distance for the specified metric type.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# effective-metric admin-distance metric-type te admin-distance 15
```

interface

To to assign affinity and configure the TE metric for an interface, use the **interface** command in SR-TE submode.

interface *type interface-path-id* { **affinity name** *name* | **metric** *value* }

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
affinity name *name*	Specifies the affinity color name. Configure this on routers with interfaces that have an associated admin group attribute.
metric *value*	Specifies the traffic engineering (TE) metric. The range is from 0 to 2,147,483,647.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Configure this on routers with interfaces that have an associated admin group attribute.

Example

The following example show how to assign affinity to an interface.

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# interface TenGigE0/0/1/2
Router(config-sr-if)# affinity
Router(config-sr-if-affinity)# name RED
```

The following example show how to configure the TE metric for an interface.

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# interface TenGigE0/0/1/2
Router(config-sr-te-if)# metric 50
```

kshortest-paths

To set the maximum number of attempts for SR-TE to compute paths that satisfy cumulative metric bounds criteria, use the **kshortest-paths** command in SR-TE configuration mode. To revert to the default number of attempts (100), use the **no** form of the command.

kshortest-paths *max-attempts*

no kshortest-paths

Syntax Description

max-attempts	Maximum number of attempts. Choose a value between 1 and 200.

Command Default

100 attempts are made to compute paths that satisfy the cumulative metric bounds criteria.

Command Modes

SR-TE configuration (config-sr-te)

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

By default, a maximum of 100 attempts are made. To update the value, you can use this command.

You can use the **show segment-routing traffic-eng policy color** command (**Number of K-shortest-paths** field) to see the K-shortest path algorithm computation result. For example, if the **Number of K-shortest-paths** field displays 4, it means that the K-shortest path algorithm took 4 computations to find the right path. The 4 shortest paths that are computed using K-shortest path algorithm did not respect the cumulative bounds, and the fifth shortest path was valid against the bounds.

Example

This example shows how to set the maximum number of attempts for computing paths that satisfy the cumulative metric bounds criteria:

```
Router# configure terminal
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# kshortest-paths 120
Router(config-sr-te)# commit
```

logging

To enable SYSLOG alarms related to PCEP peer-status and SR-TE policies, use the **logging** command in SR-TE submode.

logging { **pcep peer-status** | **policy status** }

Syntax Description

pcep peer-status	Enables PCEP peer status SYSLOG alarms.
policy status	Enables SR-TE related SYSLOG alarms.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to enable logging for SR-TE policies.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# logging policy status
```

maximum-sid-depth

To customize the maximum number of SIDs advertised by the router or signaled by the PCC during PCEP session establishment, use the **maximum-sid-depth** command in SR-TE sub-mode or SR-TE ODN sub-mode.

maximum-sid-depth *value*

Syntax Description

value	Specifies the maximum number of SIDs advertised by the router or signaled by the PCC during PCEP session establishment. The range is from 1 to 255.

Command Default

The default MSD *value* is equal to the maximum MSD supported by the platform (555).

Command Modes

SR-TE configuration

SR-TE On-Demand Next-Hop (SR-ODN) configuration

Command History

Release	Modification
Release 6.3.2	This command was introduced.

Usage Guidelines

The default MSD *value* is equal to the maximum MSD supported by the platform (555).

Note The platform's SR-TE label imposition capabilities are as follows:

- Up to 5 transport labels when no service labels are imposed
- Up to 3 transport labels when service labels are imposed
- Up to 5 transport labels when no service labels are imposed
- Up to 3 transport labels when service labels are imposed
- Up to 5 transport labels when no service labels are imposed
- Up to 3 transport labels when service labels are imposed

For cases with path computation at PCE, a PCC can signal its MSD to the PCE in the following ways:

- During PCEP session establishment – The signaled MSD is treated as a node-wide property.
  - MSD is configured under **segment-routing traffic-eng maximum-sid-depth** *value* command.
- During PCEP LSP path request – The signaled MSD is treated as an LSP property.
  - On-demand (ODN) SR Policy: MSD is configured using the **segment-routing traffic-eng on-demand color** *color* **maximum-sid-depth** *value* command.

Note If the configured MSD values are different, the per-LSP MSD takes precedence over the per-node MSD.

After path computation, the resulting label stack size is verified against the MSD requirement.

- If the label stack size is larger than the MSD and path computation is performed by PCE, then the PCE returns a "no path" response to the PCC.
- If the label stack size is larger than the MSD and path computation is performed by PCC, then the PCC will not install the path.

Note A sub-optimal path (if one exists) that satisfies the MSD constraint could be computed in the following cases:

- For a dynamic path with TE metric, when the PCE is configured with the **pce segment-routing te-latency** command or the PCC is configured with the **segment-routing traffic-eng te-latency** command.
- For a dynamic path with LATENCY metric
- For a dynamic path with affinity constraints

For example, if the PCC MSD is 4 and the optimal path (with an accumulated metric of 100) requires 5 labels, but a sub-optimal path exists (with accumulated metric of 110) requiring 4 labels, then the sub-optimal path is installed.

Example

The following example shows how to configure the MSD during PCEP session establishment. The signaled MSD is treated as a node-wide property:

```
RP/0/RSP0/CPU0:ios(config)# segment-routing
RP/0/RSP0/CPU0:ios(config-sr)# traffic-eng
RP/0/RSP0/CPU0:ios(config-sr-te)# maximum-sid-depth 4
```

The following example shows how to configure the MSD during PCEP LSP path request for the On-demand (ODN) SR Policy. The signaled MSD is treated as an LSP property:

```
RP/0/RSP0/CPU0:ios(config)# segment-routing
RP/0/RSP0/CPU0:ios(config-sr)# traffic-eng
RP/0/RSP0/CPU0:ios(config-sr-te)# on-demand color 250
RP/0/RSP0/CPU0:ios(config-sr-te-color)# maximum-sid-depth 4
```

max-install-standby-cpaths

To configure standby candidate paths for all SR policies, for a specific policy, or for an ODN template, use the **max-install-standby-cpaths** command.

To disable the configuration for global SR policies, use the **no** form of this command.

max-install-standby-cpaths *value*

Syntax Description

value	Specifies the number of non-active CPs to program in forwarding. The range for *value* is from 1 to 3 for global SR policies, and from 0 (disable) to 3 for local and ODN policies.

Command Default

None

Command Modes

SR-TE configuration

SR-TE Policy configuration

SR-TE On-Demand Next-Hop (SR-ODN) configuration

Command History

Release	Modification
Release 7.6.1	This command was introduced.

Usage Guidelines

- Up to three non-active CPs can be programmed in the forwarding plane.
- Manually configured CPs are supported. This includes CPs with explicit paths or dynamic (head-end computed or PCE-delegated) paths.
- On-Demand instantiated CPs (ODN) are supported.
- BGP-initiated CPs are supported.
- PCE-initiated CPs via PCEP are not supported.
- Programming of non-active CPs is not supported with SRv6-TE policies, Per-Flow Policies (PFP), or point-to-multipoint SR policies (Tree-SID)
- PCEP reporting of additional CPs is supported, but the PCEP reporting does not distinguish between active and non-active CPs.
- Programming of non-active CPs can be enabled for all SR policies (global), for a specific policy (local), or ODN template.

  If enabled globally and locally or on ODN template, the local or ODN configuration takes precedence over the global configuration.

  - Programming of non-active CPs under global SR-TE and configuring policy path protection of an SR policy is supported. In this case, policy path protection takes precedence.
  - Programming of non-active CPs for a specific SR policy and configuring policy path protection of an SR policy is not supported.

- The number of policies supported could be impacted by the number of non-active CPs per policy. Programming non-active CPs in the forwarding plane consumes hardware resources (such as local label and ECMP FEC) when more candidate paths are pre-programmed in forwarding than are actually carrying traffic.
- The active CP will be in programmed state. The remaining CPs will be in standby programmed state.
- We recommend that you create separate PM sessions for active and standby candidate paths to monitor the health of the paths end-to-end.
- The protected paths for each CP is programmed in the respective LSPs. The protected paths of active CPs are programmed in the active LSP, and the protected paths of standby CPs are programmed in the standby LSP.
- If a candidate path with higher preference becomes available, the traffic will switch to it in Make-Before-Break (MBB) behavior.

Example

The following example shows how to configure standby candidate paths globally:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# max-install-standby-cpaths 2
Router(config-sr-te)#
```

The following example shows how to configure standby candidate paths for a specific SR policy:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy MyBackupPolicy
Router(config-sr-te-policy)# max-install-standby-cpaths 2
Router(config-sr-te-policy)#
```

The following example shows how to configure standby candidate paths for an SR ODN template:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# on-demand color 10
Router(config-sr-te-color)# max-install-standby-cpaths 1
Router(config-sr-te-color)#
```

The following example shows how to enable three standby CPs globally and disable standby CPs on SR policy and ODN template:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# max-install-standby-cpaths 3
Router(config-sr-te)# policy MyBackupPolicy
Router(config-sr-te-policy)# max-install-standby-cpaths 0
Router(config-sr-te-policy)# exit
Router(config-sr-te)# on-demand color 10
Router(config-sr-te-color)# max-install-standby-cpaths 0
Router(config-sr-te-color)#
```

max-metric

Use the **max-metric** command in the SR-TE sub-mode to set the protocol advertising maximum metric. This will render the router as a less preferable intermediate hop for other routers.

maximum-metric *default-route delay external interlevel level on-startup srv6-locator te*

Syntax Description

default-route	Override the default route metric with maximum metric.
delay	Apply max metric to delay metric.
external	Override metric of prefixes learned from another protocol with maximum metric.
interlevel	Override metric of prefixes learned from another ISIS level with maximum metric.
level	Set maximum metric for one level only.
on-startup	Set maximum metric temporarily after reboot.
srv6-locator	Override segment routing ipv6 locator metric with maximum metric.
te	Apply max-metric to TE metric.

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 7.6.1	This command was introduced.
Release 7.8.1	This command was modified.

Example

The following example shows how to set the maximum metric for the SR-TE:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# max-metric delay te
Router(config-sr-te)# commit

Router(config-sr-te)# #sh isis da de r100

IS-IS 1 (Level-2) Link State Database
LSPID    LSP Seq Num    LSP Checksum    LSP Holdtime/Rcvd    ATT/P/OL
F100.00.00  * 0x000000a    0x79ab        1190 /*              0/0/0
    Area Address:    49.0001
    LSP MTU:         1350
    NLPID:           0xcc
    NLPID:           0x8e
    MT:              Standard (IPv4 Unicast)
    MT:              IPv6 Unicast
```

```
IP Address:      2020:1000::100
Hostname:        100
Router Cap:      20.1.0.100 D:0 S:0
Metric: 16777214        IS-Extended r101.00
Metric: 16777214        IS-Extended r101.00
Metric: 16777214        MT (IPv6 Unicast) IS-Extended r101.00
Metric: 16777214        MT (IPv6 Unicast) IS-Extended r103.00
Metric: 16777214        IP-Extended 6.6.6.100/32
Metric: 16777214        IP-Extended 10.1.1.0/24
Metric: 16777214        IP-Extended 10.4.1.0/24
Metric: 16777214        IP-Extended 20.1.0.100/32
Metric: 16777214        MT (IPv6 Unicast) IPv6 2001:1000::/64
Metric: 16777214        MT (IPv6 Unicast) IPv6 2004:1000::/64
Metric: 16777214        MT (IPv6 Unicast) IPv6 2020:1000::100/128
Metric: 16777214        MT (IPv6 Unicast) IPv6 6060:1000::100/128
```

nexthop validation color-extcomm disable

To disable BGP Next-Hop validation on the route reflector in an SR-TE domain, use the **nexthop validation color-extcomm disable** command in BGP configuration mode. To remove the configuration, use the **no** form of the command.

nexthop validation color-extcomm disable

Syntax Description

This command has no keywords or arguments.

Command Default

BGP NH validation is not disabled in an SR-TE domain.

Command Modes

BGP configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

To fully enable Next-Hop soft validation for SR policy-installed routes, do the following:

- On the headend router, enable **nexthop validation color-extcomm sr-policy**
- On the route reflector, enable **nexthop validation color-extcomm disable**

Note BGP NH soft validation is enabled on the headend router while the usual BGP NH validation is disabled on the RR.

Example

The following example shows how to disable BGP Next-Hop validation on a RR in an SR-TE domain:

```
Headend # configure
Headend (config) # router bgp 100
Headend (config-bgp)# nexthop validation color-extcomm disable
Headend (config-bgp)# commit
Headend (config-bgp)# end
```

nexthop validation color-extcomm sr-policy

To enable BGP Next-Hop soft validation in an SR-TE domain, use the **nexthop validation color- extcomm sr-policy** command in BGP configuration mode.

nexthop validation color-extcomm sr-policy

Syntax Description

This command has no keywords or arguments.

Command Default

BGP NH validation is disabled.

Command Modes

BGP configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

To fully enable Next-Hop soft validation for SR policy-installed routes, do the following:

- On the headend router, enable nexthop validation color-extcomm sr-policy
- On the route reflector, enable nexthop validation color-extcomm disable

Note BGP NH soft validation is enabled on the headend router while the usual BGP NH validation is disabled on the RR.

Example

The following example shows how to configure BGP Next-Hop soft validation on the headend router in an SR-TE domain:

```
Headend # configure
Headend (config) # router bgp 100
Headend (config-bgp)# nexthop validation color-extcomm sr-policy
Headend (config-bgp)# commit
Headend (config-bgp)# end
```

Use this command to view BGP Soft Next-Hop Validation details.

```
Headend # show bgp process detail | i Nexthop

Use SR-Policy admin/metric of color-extcomm Nexthop during path comparison: enabled
ExtComm Color Nexthop validation: SR-Policy then RIB.
```

on-demand constraints

To configure the SR Flexible Algorithm constraints, use the **constraints segments sid-algorithm** command in SR-TE sub-mode.

To specify resource constraints for path computation for ODN SR-TE policies, use the **constraints resources** command in SR-TE configuration mode.

on-demand color *color* **constraints** { **segments sid-algorithm** *algo* | **resources** { **exclude resource-list** *name* | **exclude-group** *group_name* | **apply-group** *group_name* } }

Syntax Description

segments	Specify constraints for segments of a path in a network.
sid-algorithm *algo*	Specify the SR Flexible Algorithm value. The *algo* range is from 128 to 255.
resources	Specify resource constraints for path computation.
exclude	Exclude resources from path computation.
resource-list *name*	Specify the name of the resource-list to exclude from the path computation.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 24.1.1	The resources option was introduced.
Release 7.9.1	For Cisco IOS XR Release 7.9.1, you must reconfigure all SR-ODN configurations with Flexible Algorithm constraints that use the on-demand dynamic sid-algorithm with the on-demand constraints command.
Release 7.4.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to add an SR Flexible Algorithm constraint:

```
Router(config-sr-te-color)#constraints segments sid-algorithm 128
```

The following example shows how to associate the excluded IPv4 addresses for ODN SR-TE policies:

```
Router(config)#segment-routing
Router(config-sr)#traffic-eng
Router(config-sr-te)#on-demand color 7001
Routerconfig-sr-te-color)#constraints resources exclude resource-list node_resc_list
```

on-demand dynamic affinity

To configure the affinity constraints for dynamic ODN paths, use the **on-demand dynamic affinity** command in SR-TE sub-mode.

on-demand color *color* **dynamic affinity** { **include-all** | **include-any** | **exclude-any** } [**name** *name*]

Syntax Description

affinity {**include-all** | **include-any** | **exclude-any**}	Specify the affinity type.
name *name*	Name of the affinity.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to configure the affinity contraints .

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 10 dynamic
Router(config-sr-te-color-dyn)# affinity include-all name CROSS
Router(config-sr-te-color-dyn)#
```

on-demand dynamic bounds

To configure SR-TE ODN to calculate a shortest path with cumulative metric bounds, use the **on-demand dynamic bounds** command in SR-TE sub-mode.

on-demand color *color* **bounds cumulative type** { **hopcount** | **igp** | **latency** | **te** } *metric*

Syntax Description

type {**hopcount** | **igp** | **latency** | **te**}	Specify the metric type.
metric	Specify the bound metric value. Valid values are from 1 to 4294967295.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

When an SR policy is configured on a head-end node with these metric bounds, a path is finalized towards the specified destination only if it meets each of these criteria.

PCE-based cumulative metric bounds computations are not supported. You must use non-PCE (SR-TE topology) based configuration for path calculation, for cumulative bounds.

If you use PCE dynamic computation configuration with cumulative bounds, the PCE computes a path and validates against cumulative bounds. If it is valid, then the policy is created with this path on PCC. If the initial path doesn't respect the bounds, then the path is not considered, and no further K-shortest path algorithm is executed to find the path.

Example

The following example shows how to configure IGP, TE, hop count, and latency metric bounds for the SR-ODN color template:

```
Router(config-sr-te)# on-demand color 1000 dynamic
Router(config-sr-te-color-dyn) bounds cumulative
Router(config-sr-te-odc-bounds-type)# type igp 100
Router(config-sr-te-odc-bounds-type)# type te 60
Router(config-sr-te-odc-bounds-type)# type hopcount 6
Router(config-sr-te-odc-bounds-type)# type latency 1000
```

on-demand dynamic disjoint-path

To configure the disjoint-path constraints, use the **on-demand dynamic disjoint-path** command in SR-TE sub-mode.

on-demand color *color* **dynamic disjoint-path group-id** *id* **type** { **link** | **node** | **srlg** | **srlg-node** } [{ **sub-id** *sub_id* | **fallback disable** }]

Syntax Description

group-id *id*	Specify the group ID of the disjoint path. Valid values are from 1 to 65535.
type {**link** | **node** | **srlg** | **srlg-node** }	Specify the type of disjointness.
sub-id *id*	Specify the sub-group ID of the disjoint path. Valid values are from 1 to 65535.
fallback disable	Disable all fallback behavior in case the requested disjointness cannot be achieved.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 24.1.1	The **fallback disable** keyword was introduced.
Release 6.3.1	This command was introduced.

Usage Guidelines

Configures the disjoint group ID and defines the preferred level of disjointness (the type of resources that should not be shared by the two paths):

- link—Specifies that links are not shared on the computed paths.
- node—Specifies that nodes are not shared on the computed paths.
- srlg—Specifies that links with the same SRLG value are not shared on the computed paths
- srlg-node—Specifies that SRLG and nodes are not shared on the computed paths.

If a pair of paths that meet the requested disjointness level cannot be found, then the paths will automatically fallback to a lower level:

- If the requested disjointness level is SRLG or node, then link-disjoint paths will be computed.
- If the requested disjointness level was link, or if the first fallback from SRLG or node disjointness failed, then the lists of segments encoding two shortest paths, without any disjointness constraint, will be computed.

Example

```
Router(config-sr-te-color-dyn)# disjoint-path group-id 775 type link
```

The following example indicates how to configure strict disjointness for an ODN SR-TE policy:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#on-demand color 4
Router(config-sr-te-color)#dynamic
Router(config-sr-te-color-dyn)#disjoint-path group-id 1 type node fallback disable
Router(config-sr-te-color-dyn)#commit
```

on-demand dynamic metric

To configure the On-Demand dynamic path metric, use the **on-demand dynamic metric** command in SR-TE sub-mode.

on-demand color *color* **dynamic metric** { **margin** { **absolute** *value* | **relative** *percent* } *margin* | **type** { **hopcount** | **igp** | **latency** | **te** } }

Syntax Description

metric {**absolute** *value* | **relative** *percent*}	Specify the On-Demand dynamic path metric margin. The range for *margin* and *percent* is from 0 to 2147483647.
type { **hopcount** | **igp** | **latency** | **te** }	Specify the metric type for use in path computation.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
Router(config-sr-te-color-dyn)# metric type te
Router(config-sr-te-color-dyn)# metric margin absolute 5
```

on-demand dynamic pcep

To indicate that only the path computed by SR-PCE should be associated with the on-demand SR policy, use the **on-demand dynamic pcep** command in SR-TE sub-mode.

on-demand color *color* **dynamic pcep**

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

With this configuration, local path computation is not attempted; instead the head-end router will only instantiate the path computed by the SR-PCE.

Example

```
Router(config-sr-te)# on-demand color 10 dynamic pcep
```

on-demand dynamic sid-algorithm

Note For Cisco IOS XR Release 7.9.1, you must reconfigure all SR-ODN configurations with Flexible Algorithm constraints that use the on-demand dynamic sid-algorithm with the on-demand constraints command.

To configure the SR Flexible Algorithm constraints, use the **on-demand dynamic sid-algorithm** command in SR-TE sub-mode.

on-demand **color** *color* **dynamic** **sid-algorithm** *algo*

Syntax Description

sid-algorithm *algo*	Specify the SR Flexible Algorithm value . The *algo* range is from 128 to 255.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.
Release 7.4.1	This command was replaced by the **on-demand constraints** command.
Release 7.9.1	For Cisco IOS XR Release 7.9.1, you must reconfigure all SR-ODN configurations with Flexible Algorithm constraints that use the **on-demand dynamic sid-algorithm** with the **on-demand constraints** command.

Usage Guidelines

This command was replaced by the on-demand constraints command.

Example

```
Router(config-sr-te-color-dyn)# sid-algorithm 128
```

on-demand maximum-sid-depth

To customize the maximum SID depth (MSD) constraints advertised by the router, use the **on-demand maximum-sid-depth** command in SR-TE sub-mode.

on-demand color *color* **maximum-sid-depth** *value*

Syntax Description

maximum-sid-depth *value*	Specify the maximum SID depth. The range of *value* is 1 to 255.

Command Default

The default MSD *value* is equal to the maximum MSD supported by the platform (555).

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
Router(config-sr-te-color)# maximum-sid-depth 5
```

on-demand steering

on-demand color *color* **steering** { **labeled-services disable** | **path-invalidation drop** }

Syntax Description

labeled-services disable	Disable steering of labeled-services for on-demand color policies. This configuration applies for a specific ODN color.
path-invalidation drop	Drop traffic but keep the SR policy up in the control plane.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 7.0.1	This command was introduced.
Release 7.4.1	The **path-invalidation drop** keywords are introduced.

Usage Guidelines

- **labeled-services disable**: The SR-TE MPLS Label Imposition Enhancement feature increases the maximum label imposition capabilities of the platform.

  In previous releases, the platform supported:

  - Up to 5 MPLS transport labels when no MPLS service labels are imposed
  - Up to 3 MPLS transport labels when MPLS service labels are imposed

  With the SR-TE MPLS Label Imposition Enhancement feature, the platform supports the following:

  - Up to 12 MPLS transport labels when no MPLS service labels are imposed
  - Up to 9 MPLS transport labels when MPLS service labels are imposed

  This enhancement is enabled and disabled dynamically, as the label count changes. For example, if a path requires only 3 MPLS transport labels, the MPLS Label Imposition Enhancement feature is not enabled.

  You can disable labeled services for SR-TE policies. The label switching database (LSD) needs to know if labeled services are disabled on top of an SR-TE policy to perform proper label stack splitting.

- **path-invalidation drop**:

  By default, if an SR Policy becomes invalid, traffic would fall back to the native SR forwarding path. In some scenarios, a network operator may require that certain traffic be only carried over the path associated with an SR policy and never allow the native SR LSP to be used. This command is introduced to meet this requirement.

  With **path-invalidation drop** enabled, an SR policy that would become invalid (for example, no valid candidate path available) is programmed to drop traffic. At the same time, the SR policy stays up in the control plane to prevent prefixes mapped to the SR policy from falling back to the native SR LSP.

When the SR policy becomes valid again, forwarding over the SR policy resumes.

Example

The following example shows how enable the dropping of traffic when an On-Demand SR Policy becomes invalid.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 10
Router(config-sr-te-color)# steering
Router(config-sr-te-on-demand-color-steering)# path-invalidation drop
```

The following example shows how to disable steering of labeled-services for on-demand color policies:

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 10
Router(config-sr-te-color)# steering
Router(config-sr-te-on-demand-color-steering)# labeled-services disable
```

path-invalidation drop

To enable the dropping of traffic when an SR Policy becomes invalid, use the **path-invalidation drop** command.

policy *policy* **steering path-invalidation drop**

on-demand color *color* **steering path-invalidation drop**

pcc profile *profile* **steering path-invalidation drop**

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

SR-TE Policy

SR-TE ODN

SR-TE PCC

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

By default, if an SR Policy becomes invalid, traffic would fall back to the native SR forwarding path. In some scenarios, a network operator may require that certain traffic be only carried over the path associated with an SR policy and never allow the native SR LSP to be used. This command is introduced to meet this requirement.

With **path-invalidation drop** enabled, an SR policy that would become invalid (for example, no valid candidate path available) is programmed to drop traffic. At the same time, the SR policy stays up in the control plane to prevent prefixes mapped to the SR policy from falling back to the native SR LSP.

When the SR policy becomes valid, forwarding over the SR policy resumes.

Example

The following example shows how enable the dropping of traffic when an SR Policy becomes invalid.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 10
Router(config-sr-te-color)# steering
Router(config-sr-te-on-demand-color-steering)# path-invalidation drop
```

The following example shows how enable the dropping of traffic when an On-Demand SR Policy becomes invalid.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
```

```
Router(config-sr-te)# policy FOO
Router(config-sr-te-policy)# steering
Router(config-sr-te-policy-steering)# path-invalidation drop
```

The following example shows how enable the dropping of traffic when a PCE-Initiated SR Policy becomes invalid.

```
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc profile 7
Router(config-pcc-prof)# steering
Router(config-pcc-prof-steering)# path-invalidation drop
```

pcc pce address

To configure the SR-PCE address and options, use the **pcc pce address** command in SR-TE configuration mode.

pcc pce address ipv4 *address* [{ **keychain** *word* | **password** { **clear** | **encrypted** } *password* | **precedence** *0-255* | **tcp-ao** *word* [**include-tcp-options**] }]

Syntax Description

keychain *keychain-name*	Configures keychain based authentication for PCC
password {**clear**	**encrypted**} *password*	Configures password for MD5 authentication
precedence *precedence*	Specifies the precedence for the PCC peer. The value range is from 0 to 255.
tcp-ao *tcp-ao-keychain-name*	Configures AO keychain based authentication
include-tcp-options	Includes other TCP options in the header.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

A PCE can be given an optional precedence. If a PCC is connected to multiple PCEs, the PCC selects a PCE with the lowest precedence value. If there is a tie, a PCE with the highest IP address is chosen for computing path. The precedence value range is from 0 to 255.

Example

The following shows how to configure the SR-PCE address.

```
Router(config)# segment-routing traffic-engineering
Router(config-sr-te)# pcc pce address ipv4 1.1.1.2 precedence 250
```

pcc report-all

To enable the PCC to report all SR policies in its database to the PCE, use the **pcc report-all** command in SR-TE configuration mode.

pcc report-all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to enable the PCC to report all SR policies in its database to the PCE:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc report-all
```

pcc source-address

To configure the PCC source address, use the **pcc source-address** command in SR-TE configuration mode.

pcc source-address ipv4 *address*

Syntax Description

address	Specifies the local IPv4 address of the PCC.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

The following example shows how to configure the PCC source address:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc source-address ipv4 1.1.1.4
```

pcc timers

To configure PCEP-related timers, use the **pcc timers** command in SR-TE configuration mode.

pcc timers { **deadtimer** *seconds* | **delegation-timeout** *seconds* | **initiated** { **orphan** *seconds* | **state** *seconds* } | **keepalive** *seconds* }

Syntax Description

deadtimer *seconds*	Specifies how long the remote peers wait before bringing down the PCEP session if no PCEP messages are received from this PCC. The range is from 1 to 255 seconds.
delegation-timeout *seconds*	Specifies how long a delegated SR policy can remain up without an active connection to a PCE. The range is from 0 to 3600 seconds.
initiated orphan *seconds*	Specifies the amount of time that a PCE-initiated SR policy will remain delegated to a PCE peer that is no longer reachable by the PCC. The range is from 10 to 180 seconds.
initiated state *seconds*	Specifies the amount of time that a PCE-initiated SR policy will remain programmed while not being delegated to any PCE. The range is from 15 to 14440 seconds (24 hours).
keepalive *seconds*	Specifies how often keepalive messages are sent from PCC to its peers. The range is from 0 to 255 seconds.

Command Default

Deadtimer: 120 seconds

Delegation timeout: 60 seconds

Initiated orphan: 180 seconds

Initiated state: 600 seconds

Keepalive: 30 seconds

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

To better understand how the PCE-initiated SR policy timers operate, consider the following example:

1. PCE A instantiates SR policy P at head-end N.
2. Head-end N delegates SR policy P to PCE A and programs it in forwarding.
3. If head-end N detects that PCE A is no longer reachable, then head-end N starts the PCE-initiated orphan and state timers for SR policy P.
4. If PCE A reconnects before the orphan timer expires, then SR policy P is automatically delegated back to its original PCE (PCE A).

5. After the orphan timer expires, SR policy P will be eligible for delegation to any other surviving PCE(s).
6. If SR policy P is not delegated to another PCE before the state timer expires, then head-end N will remove SR policy P from its forwarding

Example

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc
Router(config-sr-te-pcc)# timers keepalive 20
Router(config-sr-te-pcc)# timers deadtimer 60
Router(config-sr-te-pcc)# timers delegation-timeout 30
Router(config-sr-te-pcc)# timers initiated orphan 60
Router(config-sr-te-pcc)# timers initiated state 1200
```

policy bfd

To enable SBFD on an SR-TE policy or an SR on-demand (SR-ODN) color template and enter BFD configuration mode, use the **policy bfd** command in SR-TE configuration mode

policy *policy* **bfd** { **disable** | **invalidation-action** { **down** | **none** } | **logging session-state-change** | **minimum-interval** *interval* | **multiplier** *multiplier* | **reverse-path binding-label** *label* }

Syntax Description

disable	Disables BFD session.
invalidation-action {**down** | **none**}	Specifies the action to be taken when BFD session is invalidated. • **down**: LSP can only be operationally up if the BFD session is up. • **none**: BFD session state does not affect LSP state, use for diagnostic purposes
loggingsession-state-change	Displays a syslog when the state of the session changes.
minimum-interval *interval*	Specifies the interval between sending BFD hello packets to the neighbor. The range is from 50 to 30000 milliseconds.
multiplier *multiplier*	Specifies the number of times a packet is missed before BFD declares the neighbor down. The range is from 2 to 10.
reverse-path binding-label *label*	(SR-TE policy only) Spcifies BFD packets return to head-end by using a binding label.

Command Default

minimum-interval = 150

multiplier = 3

Command Modes

SR-TE policy

SR-TE ODN

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

Do not use BFD with disjoint paths. The reverse path might not be disjoint, causing a single link failure to bring down BFD sessions on both the disjoint paths.

reverse-path binding-label: (**SR-TE policy only**) Use the **reverse-path binding-label** label command to specify BFD packets return to head-end by using a binding label.

By default, the S-BFD return path (from tail-end to head-end) is via IPv4. You can use a reverse binding label so that the packet arrives at the tail-end with the reverse binding label as the top label. This label is meant to point to a policy that will take the BFD packets back to the head-end. The reverse binding label is configured per-policy.

Note that when MPLS return path is used, BFD uses echo mode packets, which means the tail-end's BFD reflector does not process BFD packets at all.

The MPLS label value at the tail-end and the head-end must be synchronized by the operator or controller. Because the tail-end binding label should remain constant, configure it as an explicit BSID, rather than dynamically allocated.

Example

The following example shows how to enable SBFD on an SR-TE policy:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# bfd
Router(config-sr-te-policy-bfd)# invalidation-action down
Router(config-sr-te-policy-bfd)# minimum-interval 250
Router(config-sr-te-policy-bfd)# multiplier 5
Router(config-sr-te-policy-bfd)# reverse-path binding-label 24036
Router(config-sr-te-policy-bfd)# logging session-state-change
```

The following example shows how to enable SBFD on an SR-ODN color:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# on-demand color 10
Router(config-sr-te-color)# bfd
Router(config-sr-te-color-bfd)# minimum-interval 250
Router(config-sr-te-color-bfd)# multiplier 5
Router(config-sr-te-color-bfd)# logging session-state-change
Router(config-sr-te-color-bfd)# invalidation-action down
```

policy binding-sid mpls

To specify the explicit BSID, use the **policy binding-sid mpls** command in SR-TE policy mode.

binding-sid mpls *label*

Syntax Description

label	Explicit binding SID label

Command Default

None

Command Modes

SR-TE policy

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

Explicit BSIDs are allocated from the segment routing local block (SRLB) or the dynamic range of labels. A best-effort is made to request and obtain the BSID for the SR-TE policy. If requested BSID is not available (if it does not fall within the available SRLB or is already used by another application or SR-TE policy), the policy stays down.

Example

The following example shows how to configure an SR policy to use an explicit BSID of 1000:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy FOO
Router(config-sr-te-policy)# binding-sid mpls 1000
```

policy candidate-paths constraints affinity

To configure affiity constraints on an SR-TE policy, use the **policy candidate-paths constraints affinity** command in SR-TE configuration mode.

policy *policy* **candidate-paths preference** *preference* **constraints affinity** { **include-all** | **include-any** | **exclude-any** } **name** *name*

Syntax Description

policy *policy*	Specifies the name of the policy.
candidate-paths preference *preference*	Configures the candidate path preference. The range is from 1 to 65535.
constraints affinity {**include-allinclude-anyexclude-any**}	Configures the affinity constraints.
name *name*	Specifies the affinity name.

Command Default

None

Command Modes

SR-TE policy

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

The candidate path with the highest preference is the active candidate path (highlighted below) and is installed in forwarding.

You can apply a color or name to links or interfaces by assigning affinity bit-maps to them. You can then specify an affinity (or relationship) between an SR policy path and link colors. SR-TE computes a path that includes or excludes links that have specific colors,or combinations of colors

Example

The following example shows how to associate affinity constraints for an SR-TE policy:

```
Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# color 20 end-point ipv4 1.1.1.4
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 200
Router(config-sr-te-policy-path-pref)# constraints affinity exclude-any red
```

policy candidate-paths constraints disjoint-path

To configure the disjoint-path constraints, use the **on-demand dynamic disjoint-path** command in SR-TE sub-mode.

policy *policy* **candidate-paths preference** *preference* **constraints disjoint-path group-id** *id* **type** { **link** | **node** | **srlg** | **srlg-node** } [{ **sub-id** *sub_id* | **shortest-path** | **fallback disable** }]

Syntax Description

group-id *id*	Specify the group ID of the disjoint path. Valid values are from 1 to 65535.
type {**link** | **node** | **srlg** | **srlg-node** }	Specify the type of disjointness.
sub-id *id*	Specify the sub-group ID of the disjoint path. Valid values are from 1 to 65535.
shortest-path	Enable shortest path computation for the selected candidate path.
fallback disable	Disable all fallback behavior in case the requested disjointness cannot be achieved.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 24.1.1	The **shortest-path** and **fallback disable** keywords were introduced.
Release 6.3.1	This command was introduced.

Usage Guidelines

Configures the disjoint group ID and defines the preferred level of disjointness (the type of resources that should not be shared by the two paths):

- link—Specifies that links are not shared on the computed paths.
- node—Specifies that nodes are not shared on the computed paths.
- srlg—Specifies that links with the same SRLG value are not shared on the computed paths
- srlg-node—Specifies that SRLG and nodes are not shared on the computed paths.

If a pair of paths that meet the requested disjointness level cannot be found, then the paths will automatically fallback to a lower level:

- If the requested disjointness level is SRLG or node, then link-disjoint paths will be computed.
- If the requested disjointness level was link, or if the first fallback from SRLG or node disjointness failed, then the lists of segments encoding two shortest paths, without any disjointness constraint, will be computed.

Example

```
Router(config-sr-te)# policy FOO
Router(config-sr-te-policy)# candidate-paths preference 100
Router(config-sr-te-poliilojkl,.cy-path-pref)# constraints disjoint-path group-id 775 type
 link
```

The following example indicates how to configure the shortest path preference for a disjoint path:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#policy dynamic_pcep_policy_disjoint
Router(config-sr-te-policy)#candidate-paths
Router(config-sr-te-policy-path)#preference 100
Router(config-sr-te-policy-path-pref)#constraints disjoint-path group-id 1 type link
shortest-path
```

The following example indicates how to configure strict disjointness for a SR-TE policy:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#policy foo
Router(config-sr-te-policy)#color 1 end-point ipv4 10.10.10.1
Router(config-sr-te-policy)#candidate-paths preference 100
Router(config-sr-te-policy-path-pref)#constraints disjoint-path group-id 1 type node fallback
 disable
Router(config-sr-te-policy-path-pref)#commit
```

policy candidate-paths constraints resources

To exclude IP addresses from the path computation for SR-TE policies, use the **policy candidate-paths constraints resources** command in the SR-TE configuration mode.

policy *policy* **candidate-paths preference** *preference* **constraints resources** { **exclude resource-list** *name* | **exclude-group** *group_name* | **apply-group** *group_name* }

Syntax Description

resources {**exclude-group** | **exclude** | **apply-group**}	Specify the resource constraints for path computation: • exclude. Excludes resources from the path computation. • exclude-group. Excludes the apply-group configuration from the group. • apply-group. Applies configuration from a group.
resource-list *name*	Specify the name of the resource-list to exclude from the path computation.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

None.

Example

The following example shows how to exclude a list of IPv4 addresses from the network resource list:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#resource-list node_resc_list
Router(config-sr-te-rl)#index 1 ipv4 10.10.10.1
Router(config-sr-te-rl)#index 2 ipv4 10.10.10.8
```

The following example shows how to associate the excluded IPv4 addresses to one or more candidate paths for SR-TE policies:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#policy dynamic_pcep_policy
Router(config-sr-te-policy)#candidate-paths
Router(config-sr-te-policy-path)#preference 100
Router(config-sr-te-policy-path-pref)#constraints resources exclude resource-list
node_resc_list
```

policy candidate-paths dynamic

To configure the SR-TE head-end or SR-PCE to compute a path that is encoded using Anycast prefix SIDs of nodes along the path, use the **policy candidate-paths dynamic** command.

policy *policy* **candidate-paths preference** *preference* **dynamic** { **anycast-sid-inclusion** | **pcep** }

Syntax Description

anycast-sid-inclusion	Specifies a PCC-initiated path computation at the head-end router, encoded using Anycast prefix SIDs of nodes along the path.
pcep	Specifies that the path computation is at the SR-PCE.

Command Default

None

Command Modes

SR-TE

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

An Anycast SID is a type of prefix SID that identifies a set of nodes and is configured with n-flag clear. The set of nodes (Anycast group) is configured to advertise a shared prefix address and prefix SID. Anycast routing enables the steering of traffic toward multiple advertising nodes, providing load-balancing and redundancy. Packets addressed to an Anycast address are forwarded to the topologically nearest nodes.

Example

The following example shows how to request a PCC-initiated Anycast SID-aware path computation at the head-end router:

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy FOO
Router(config-sr-te-policy)# color 10 end-point ipv4 1.1.1.10
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# dynamic
Router(config-sr-te-pp-info)# anycast-sid-inclusion
```

policy candidate-paths dynamic metric

policy *policy* **candidate-paths preference** *preference* **dynamic metric** { **margin** { **absolute** | **relative** } *margin* | **sid-limit** *value* | **type** { **hopcount** | **igp** | **latency** | **te** } }

Syntax Description

metric {**absolute**	**relative** } *margin*	Specify the On-Demand dynamic path metric margin. The range for *margin* is from 0 to 2147483647.
sid-limit *value*	Specify the maximun SID depth (MSD).
type { **hopcount**	**igp**	**latency**	**te** }	Specify the metric type for use in path computation.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

If the configured MSD values are different, the per-LSP MSD takes precedence over the per-node MSD.

Example

```
Router(config-sr-te-policy-path-pref)# dynamic metric type te
Router(config-sr-te-policy-path-pref)# dynamic metric margin absolute 5
```

policy candidate-paths explicit

policy *policy* **candidate-paths preference** *preference* **explicit segment-list** *sid_list* [**weight** *weight*]

Syntax Description

segment-list	*sid_list*	Specify the explicit segment list.
weight	*weight*	Path option weight. Range is from 1 to 4294967295.

Command Default

None

Command Modes

ST-TE policy

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# color 10 end-point ipv4 1.1.1.4
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# explicit segment-list SIDLIST1
```

policy candidate-paths per-flow

To map a forward class to a per-flow policy, use the **policy candidate-paths per-flow** command.

policy *policy* **candidate-paths preference** *preference* **per-flow forward-class** { *value* **color** *color* | **default** *value* }

Syntax Description

forward-class *value*	Specify the forward class (FC). Values are from 0 to 7.
color *color*	Specify the color of the policy.
default *value*	Explicitly specify a default FC.

Command Default

When not explicitly configured, FC 0 is the default FC.

Command Modes

SR-TE policy

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Usage Guidelines

When not explicitly configured, FC 0 is the default FC.

A Per-Flow Policy (PFP) defines an array of FC-to-PDP mappings. A PFP can then be used to steer traffic into a given PDP based on the FC assigned to a packet.

A Per-Flow Policy (PFP) is considered valid as long as its default FC has a valid Per-Destination Policy (PDP).

A color associated with a PFP SR policy cannot be used by a non-PFP SR policy. For example, if a per-flow ODN template for color 100 is configured, then the system will reject the configuration of any non-PFP SR policy using the same color. You must assign different color value ranges for PFP and non-PFP SR policies.

Example

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy FOO
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy-path)# preference 100
Router(config-sr-te-policy-path-pref)# per-flow
Router(config-sr-te-pol-cp-pfp)# forward-class 0 color 10
Router(config-sr-te-pol-cp-pfp)# forward-class 1 color 20
```

policy candidate-paths preference lock duration

To enable a new lock duration for the Protect candidate path, use the **policy candidate-paths preference lock duration** command in the SR-TE configuration mode. To remove the lock function for a Protect path, use the **no** form of the command.

policy *name* [**candidate-paths** [**preference** *preference* [**lock** [**duration** *seconds*]]]]

Syntax Description

candidate-paths [**preference** *preference*]	(Optional) Configures the candidate path preference. The range is from 1 to 65535.
lock [**duration** *seconds*]	(Optional) Enables the specified lock duration for the Protect candidate path. The default lock duration is 300 seconds.

Command Default

The default Protect path lock duration is 300 seconds.

Command Modes

SR-TE configuration (config-sr-te)

Command History

Release	Modification
Release 7.4.2	This command was introduced.

Usage Guidelines

When the Working path is invalid, the Protect path becomes active. After the Working path has recovered, the Protect path remains active until the default lock duration (300 seconds) expires. You can configure a different lock duration using this command.

The duration range is 0 (disabled) to 3000 seconds. If the lock duration is 0 (disabled), then the Working path becomes active as soon as it recovers. If duration is not specified, the Protect path remains active.

Example

This example shows how to enable a new lock duration of 600 seconds for the Protect candidate path:

```
RP/0/RSP0/CPU0:ios# configure
RP/0/RSP0/CPU0:ios(config)# segment-routing traffic-eng
RP/0/RSP0/CPU0:ios(config-sr-te)# policy foo candidate-paths preference 50 lock duration
600
RP/0/RSP0/CPU0:ios(config-sr-te)# commit
```

policy color end-point

To configure the SR-TE color and end-point address, use the **policy color end-point** command.

policy *policy* **color** *color* **end-point** { **ipv4** | **ipv6** } *ip_addr*

Syntax Description

color *color*	Specify the color of the SR policy.
end-point {**ipv4**|**ipv6**} *ip_addr*	Specify the IPv4 or IPv6 address of the end-point.

Command Default

None

Command Modes

SR-TE policy

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

An SR-TE policy is identified as an ordered list (head-end, color, end-point):

- Head-end – Where the SR-TE policy is instantiated
- Color – A numerical value that distinguishes between two or more policies to the same node pairs (Head-end – End point)
- End-point – The destination of the SR-TE policy

  Every SR-TE policy has a color value. Every policy between the same node pairs requires a unique color value.

Example

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy POLICY1
Router(config-sr-te-policy)# color 10 end-point ipv4 1.1.1.4
```

policy ipv6 disable

To disable IPv6 encapsulation (IPv6 caps) for a particular color and IPv4 NULL end-point, use the **ipv6 disable** command is SR-TE configuration mode.

policy ipv6 disable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

SR-TE configuration mode

Command History

Release	Modification
Release 6.5.1	This command was introduced.

Usage Guidelines

IPv6 caps for IPv4 NULL end-point is enabled automatically when the policy is created in Segment Routing Path Computation Element (SR-PCE). The binding SID (BSID) state notification for each policy contains an "ipv6_caps" flag that notifies SR-PCE clients (PCC) of the status of IPv6 caps (enabled or disabled).

An SR-TE policy with a given color and IPv4 NULL end-point could have more than one candidate path. If any of the candidate paths has IPv6 caps enabled, then all of the remaining candidate paths need IPv6 caps enabled. If IPv6 caps is not enabled on all candidate paths of same color and end-point, traffic drops can occur.

You can disable IPv6 caps for a particular color and IPv4 NULL end-point using the **ipv6 disable** command on the local policy. This command disables IPv6 caps on all candidate paths that share the same color and IPv4 NULL end-point.

Example

This example shows how to disable IPv6 caps for a particular color and IPv4 NULL end-point:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy P1
Router(config-sr-te-policy)# color 1 end-point ipv4 0.0.0.0
Router(config-sr-te-policy)# ipv6 disable
```

policy path-protection

To enable path-protection for an SR-TE policy's candidate paths, use the **policy path-protection** command in the SR-TE configuration mode. To disable SR-TE policy path-protection, use the **no** form of the command.

policy *name* [**path-protection**]

Syntax Description

path-protection	(Optional) Specifies that path-protection should be enabled for the specified policy.

Command Default

Path-protection is not enabled for an SR-TE policy's candidate paths.

Command Modes

SR-TE configuration (config-sr-te)

Command History

Release	Modification
Release 7.4.2	This command was introduced.

Example

This example shows how to enable SR-TE policy path-protection for the policy **foo**:

```
RP/0/RSP0/CPU0:ios# configure
RP/0/RSP0/CPU0:ios(config)# segment-routing traffic-eng
RP/0/RSP0/CPU0:ios(config-sr-te)# policy foo path-protection
RP/0/RSP0/CPU0:ios(config-sr-te-path-pref-protection)#commit
```

policy performance-measurement

To apply a performance measurement profile to an SR policy, use the **performance-measurement** command in SR-TE configuration mode.

{ **policy performance-measurement** [**delay-measurement delay-profile name** *name* [**logging delay-exceeded**]] | [{ **liveness-detection liveness-profile name** *name* [**invalidation-action** { **down** | **none** }] | **logging session-state-change** }] | [**reverse-path label** *label*] }

Syntax Description

policy *policy*	Specifies the SR policy name.
liveness-detection	Enables end-to-end SR Policy Liveness Detection
invalidation-action {**none** | **down**}	Specifies the action to take when the PM liveness session goes down: • **down (default)**: The candidate path is immediately operationally brought down. • **none**: No action is taken. If logging is enabled, the failure is logged but the SR Policy operational state is not modified.
logging session-state-change	Enables Syslog messages when the session state changes.
logging delay-exceeded	Enables Syslog messages when the delay exceeds the threshold.
delay-profile name *profile*	Specifies the SR Policy delay profile name.
reverse-path label {*BSID-value* | *NODE-SID-value*}	Specifies the MPLS label to be used for the reverse path for the reply. If you configured liveness detection with ECMP hashing, you must specify the reverse path. The default reverse path uses IP Reply. • *BSID-value*: The Binding SID (BSID) label for the reverse SR Policy. (This is practical for manual SR policies with a manual BSID.) • *NODE-SID-value*: The absolute SID label of the (local) Sender Node to be used for the reverse path for the reply.

Command Default

None

Command Modes

SR-TE configuration

Command History

Release	Modification
Release 6.5.2	This command was introduced.
Release 7.3.1	The **liveness-detection** options were introduced.

Example

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy TEST
Router(config-sr-te-policy)# color 4 end-point ipv4 10.10.10.10
Router(config-sr-te-policy)# performance-measurement
Router(config-sr-te-policy-perf-meas)# delay-measurement delay-profile name profile2
```

policy shutdown

To shutdown an SR policy, use the **policy** *name* **shutdown** command in SR-TE configuration mode.

policy *name* **shutdown**

Syntax Description

policy*name*	Specifies the SR policy name.

Command Default

None

Command Modes

SR-TE configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# policy TEST shutdown
```

resource-list

To configure a list of IPv4 addresses that you want to exclude from the network resource list for a candidate path, use the **resource-list** command in SR-TE configuration mode.

resource-list *name* **index** *"1-65535"* **ipv4** *ipv4-addr*

Syntax Description

resource-list *name*	Specify the resource-list name to exclude from the path computation.
index *1-65535*	Specify the index entry. Ranges from 1–65535.
ipv4 *ipv4-addr*	Specify the IPv4 address that you want to exclude from the network resource list.

Command Default

None

Command Modes

SR-TE configuration mode

Command History

Release	Modification
Release 24.1.1	This command was introduced.

Usage Guidelines

None.

Example

The following example shows how to configure a list of IPv4 addresses that you want to exclude from the network resource list:

```
Router(config)#segment-routing traffic-eng
Router(config-sr-te)#resource-list node_resc_list
Router(config-sr-te-rl)#index 1 ipv4 10.10.10.1
Router(config-sr-te-rl)#index 2 ipv4 10.10.10.8
```

segment-list

To create a segment list for explicit policy path, use the **segment-list** command in SR-TE configuration mode.

segment-list [**name**] *name* **index** *index* **mpls** { **label** *label* | **adjacency** { *ipv4-addr ipv6-addr* } }

Syntax Description

index *index*	Specifies the index entry.
mpls	Enters MPLS configure mode.
label *label*	Specify the MPLS label value.
adjacency {*ipv4-addr* | *ipv6-addr*}	Specify the IP address.

Command Default

None

Command Modes

SR-TE configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

A segment list can use IPv4/IPv6 addresses (adjacency) or MPLS labels, or a combination of both.

- The IP address can be link or a Loopback address.
- Once you enter an MPLS label, you cannot enter an IP address.

Example

The following example shows how to create a segment list with IP addresses:

```
Router(config-sr-te)# segment-list name SIDLIST1
Router(config-sr-te-sl)# index 10 mpls adjacency 1.1.1.2
Router(config-sr-te-sl)# index 20 mpls adjacency ipv4 1.1.1.3
Router(config-sr-te-sl)# index 30 mpls adjacency ipv4 1.1.1.4
```

The following example shows how to create a segment list with MPLS labels:

```
Router(config-sr-te)# segment-list name SIDLIST2
Router(config-sr-te-sl)# index 10 mpls label 16002
Router(config-sr-te-sl)# index 20 mpls label 16003
Router(config-sr-te-sl)# index 30 mpls label 16004
```

The following example shows how to create a segment list with IP addresses and MPLS labels:

```
Router(config-sr-te)# segment-list name SIDLIST3
Router(config-sr-te-sl)# index 10 mpls adjacency ipv4 1.1.1.2
Router(config-sr-te-sl)# index 20 mpls label 16003
```

```
Router(config-sr-te-sl)# index 30 mpls label 16004
```

te-latency

To enable ECMP-aware path computation for TE metric, use the **te-latency** command in SR-TE configuration mode.

te-latency

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes SR-TE configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines ECMP-aware path computation is enabled by default for IGP and LATENCY metrics

Example

This example shows how to enable ECMP-aware path computation for TE metric:

```
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# te-latency
```

timers

To configure SR-TE reoptimization timers, use the **timers** command in SR-TE configuration mode.

timers { **candidate-path cleanup-delay** *seconds* | **cleanup-delay** *seconds* | **init-verify-restart** *seconds* | **init-verify-switchover** *seconds* | **init-verify-startup** *seconds* | **periodic-reoptimization** *seconds* | **install-delay** *seconds* }

Syntax Description

candidate-path cleanup-delay *seconds*	Specifies the delay before cleaning up candidate paths. Range of *seconds* is from 0 (immediate cleanup) to 86400.
cleanup-delay *seconds*	Specifies the delay before cleaning up previous path. Range of *seconds* is from 0 (immediate cleanup) to 300.
init-verify-restart *seconds*	Specifies the delay before topology convergence after topology starts populating for restart case. Range of *seconds* is from 10 to 10000.
init-verify-switchover *seconds*	Specifies the delay before topology convergence after topology starts populating for switchover case. Range of *seconds* is from 10 to 10000.
init-verify-startup *seconds*	Specifies the delay before topology convergence after topology starts populating for startup case. Range of *seconds* is from 10 to 10000.
install-delay *seconds*	Specifies the delay before switching to a reoptimized path. Range of *seconds* is from 0 (immediate cleanup) to 300.
periodic-reoptimization *seconds*	Specifies how often to perform periodic reoptimization of policies. Range of *seconds* is from 0 (disables reoptimization) to 86400.

Command Default

- **candidate-path cleanup-delay**: 120 seconds
- **cleanup-delay**: 10 seconds
- **init-verify-restart**: 40 seconds
- **init-verify-switchover**: 60 seconds
- **init-verify-startup**: 120 seconds
- **install-delay**: 10 seconds
- **periodic-reoptimization**: 600 seconds

Command Modes

SR-TE configuration mode

Command History

Release	Modification
Release 6.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

```
Router(config)# segment-routing traffic-eng
Router(config-sr-te)# timers
Router(config-sr-te-timers)# candidate-path cleanup-delay 600
Router(config-sr-te-timers)# cleanup-delay 60
Router(config-sr-te-timers)# init-verify-restart 120
Router(config-sr-te-timers)# init-verify-startup 600
Router(config-sr-te-timers)# init-verify-switchover 30
Router(config-sr-te-timers)# install-delay 60
Router(config-sr-te-timers)# periodic-reoptimization 3000
```