Traffic Engineering in Cisco Crosswork Network Controller

Traffic engineering (TE) is a method of optimizing and steering traffic in a network to achieve an operational goal or provide custom services, such as using guaranteed bandwidth routes for prioritized traffic. One way TE can improve network performance is by forcing traffic to take predetermined routes and by effectively using available resources.

One of the biggest advantages of using Crosswork Network Controller is the ability to visualize SR-TE policies and RSVP-TE tunnels on a topology map. By visually examining your network, the complexity of provisioning and managing these SR-TE policies is significantly reduced.

This section contains the following topics:

Supported SR-TE policies and RSVP tunnels

Crosswork Network Controller traffic engineering supports the visualization and provisioning of a variety of SR-TE policies and RSVP tunnels. It simplifies service provisioning by exposing YANG model-based forms in its UI and providing APIs for integration with external systems, while Cisco NSO acts as the underlying provisioning engine.

Additionally, Crosswork Network Controller can discover and visualize pre-existing services that it did not create (such as brownfield service implementations) using telemetry and interaction with the SR-PCE. These services will be marked as unmanaged in Crosswork Network Controller. To modify these services, administrators can use a combination of device CLI, NSO's service models or APIs, the Crosswork Network

Controller UI tool set, and in some case scripts to migrate pre-existing services from being un-mamanged to being managed.

Operators can collaborate with Cisco CX Professional Services or leverage resources and articles on the Cisco DevNet to customize or expand the capabilities of Crosswork Network Controller. This can include developing custom function packs tailored to their specific use cases.

Table 1: Supported TE Technologies

TE Technology	Crosswork Network Controller	
	Visualize	**Provision (PCE-initiated)**
SR-MPLS	✓	✓
SRv6	✓	✓
RSVP	✓	✓
Flexible Algorithm	✓	✗
Tree-SID	✓	✓[1]
Circuit Style	✓	✓

[1] Only static Tree-SID policies are supported. While dynamic Tree-SID policies can only be provisioned manually on devices or via APIs, they can be visualized in Crosswork Network Controller UI.

Note Crosswork supports the use of Role-based Access Control (RBAC) to limit not only what functions a user can perform, but also on which devices they are allowed to perform those functions, see the "Cisco Crosswork Network Controller Administration Guide".

Segment Routing (SR)

Segment routing for traffic engineering takes place through a tunnel between a source and destination pair. Segment routing for traffic engineering uses the concept of source routing, where the source calculates the path and encodes it in the packet header as a segment. Segments are an identifier for any type of instruction. For example, topology segments identify the next hop toward a destination. Each segment is identified by the segment ID (SID) consisting of an unsigned 32-bit integer. Each segment is an end-to-end path from the source to the destination and instructs the routers in the provider core network to follow the specified path calculated by the IGP. The destination is unaware of the presence of the tunnel.

Segments

Interior gateway protocol (IGP) distributes two types of segments: prefix segments and adjacency segments. Each router (node) and each link (adjacency) has an associated segment identifier (SID).

- A prefix SID is associated with an IP prefix. It is manually configured from the segment routing global block (SRGB) range of labels and distributed by IS-IS (Intermediate System to Intermediate System) or OSPF (Open Shortest Path First). The prefix segment steers traffic along the shortest path to its destination. A node SID is a special type of prefix SID that identifies a specific node. It is configured under the loopback interface with the node's loopback address as the prefix.

  A prefix segment is a global segment, so a prefix SID is globally unique within the segment routing domain.

- An adjacency segment is identified by a label called an adjacency SID. This label represents a specific adjacency, such as an egress interface, to a neighboring router. The adjacency SID is distributed by IS-IS or OSPF. The adjacency segment steers traffic to a specific adjacency.

  An adjacency segment is a local segment, so the adjacency SID is locally unique relative to a specific router.

By combining prefix (node) and adjacency segment IDs in an ordered list, any path within a network can be constructed. At each hop, the top segment is used to identify the next hop. Segments are stacked in order at the top of the packet header. When the top segment contains the identity of another node, the receiving node uses equal-cost multi-path (ECMP) to move the packet to the next hop. When the identity is that of the receiving node, the node pops the top segment and performs the task required by the next segment.

SR policies

Segment routing for traffic engineering uses a “policy” to steer traffic through the network. An SR policy path is expressed as a list of segments that specifies the path, called a segment ID (SID) list. Each segment is an end-to-end path from the source to the destination, instructing the network routers to follow the specified path instead of the shortest path calculated by the IGP. If a packet is steered into an SR policy, the head-end pushes the SID list on the packet. The rest of the network executes the instructions embedded in the SID list.

Crosswork supports the visualization (and some provisioning) of the following SR-related policies:

- SR-MPLS and SRv6
- Flexible Algorithm
- Tree Segment Identifier (Tree-SID) Multicast Traffic Engineering
- SR Circuit Style

There are two types of SR policies: dynamic and explicit.

Dynamic SR policy

A dynamic path is based on an optimization objective and a set of constraints. The head-end computes a solution, resulting in a SID list or a set of SID lists. When the topology changes, a new path is computed. If the head-end does not have enough information about the topology, the head-end might delegate the computation to a path computation engine (PCE).

Explicit SR policy

When configuring an explicit policy, you specify an explicit path consisting of a list of prefixes or adjacency SIDs, each representing a node or link along the path.

Disjointness

Crosswork Network Controller uses disjoint policies to compute two sets of segment lists that steer traffic from two source nodes to two destination nodes along disjoint paths. These disjoint paths can originate from the same head-end or from different head-ends.

The disjoint level specifies the type of resources that the two computed paths should not share. The following disjoint path computations are supported:

- **Link** – Paths do not share the same interfaces or physical links.
- **Node** – Paths do not share the same nodes, ensuring complete independence of routing devices.
- **SRLG** – Paths avoid Shared Risk Link Group (SRLG), which represent links that share a common risk.
- **SRLG-node** – Paths avoid both shared SRLGs and shared nodes, offering the highest level of fault isolation.

When the first request is received with a given disjoint-group ID, a list of segments is computed, encoding the shortest path from the first source to the first destination. When the second request is received with the same disjoint-group ID, the information received in both requests is used to compute two disjoint paths: one path from the first source to the first destination and another from the second source to the second destination.

Note

- Disjointness is supported for two policies with the same disjoint ID.
- Configuring affinity and disjointness at the same time is not supported.

Segment Routing Path Computation Element (SR-PCE)

Crosswork Network Controller uses a combination of telemetry and data collected from the Cisco Segment Routing Path Computation Element (SR-PCE) to analyze and compute optimal TE tunnels.

Cisco SR-PCE is provided by the Cisco IOS XR operating system running on either a physical device or a virtual router running within a virtual machine. SR-PCE provides stateful PCE functionality that helps control and reroute TE tunnels to optimize the network. PCE describes a set of procedures by which a Path Computation Client (PCC) can report and delegate control of headend tunnels sourced from the PCC to a PCE peer. The PCC and PCE establish a Path Computation Element Communication Protocol (PCEP) connection that SR-PCE uses to push updates to the network.

Crosswork Network Controller discovers all devices in the IGP domain, including those that do not establish PCEP peering with SR-PCE. However, PCEP peering is required to deploy TE tunnels.

Note To avoid any compatibility issues, refer to the Cisco Crosswork Network Controller Release Note for SR-PCE version support and compatibility.

For SR-PCE and HA configuration, see **Cisco SR-PCE providers** in the Cisco Crosswork Network Controller 7.1 Administration Guide.

SR-TE policy PCC and PCE configuration sources

SR-TE policies that are configured using the UI or API are the only types of policies that you can modify or delete in Crosswork Network Controller. However, SR-TE policies that are discovered and reported by Crosswork Network Controller may have been configured from these sources:

- Path Computation Client (PCC) initiated—Policies configured directly on a PCC (see PCC-initiated SR-TE policy example, on page 7). These policies display as Unknown in the UI because they are not provisioned or managed by Crosswork Network Controller. However, Bandwidth on Demand (BWoD) and Circuit Style (CS) policies are exceptions. These are not labeled as Unknown because Crosswork Network Controller recognizes and categorizes them based on their attributes and purpose, even if they are PCC-initiated.

Note Circuit Style policies are always PCC-initiated.

- Path Computation Element (PCE) initiated—Policies configured on a PCE or created dynamically by Crosswork Network Controller. Examples of PCE Initiated policy types:
  - Dynamic
  - Explicit
  - Bandwidth on Demand (can be either PCC or PCE)
  - Local Congestion Mitigation
  - SR Circuit Style Manager

Resource Reservation Protocol (RSVP)

Resource Reservation Protocol (RSVP) is a signaling protocol that enables systems to request resource reservations from the network. RSVP processes protocol messages from other systems, processes resource requests from local clients, and generates protocol messages. As a result, resources are reserved for data flows on behalf of local and remote clients. RSVP creates, maintains, and deletes these resource reservations.

The RSVP-TE process contains the following functionalities:

- Endpoint control - is associated with establishing and managing TE tunnels at the headend and tail end.
- Link-management - manages link resources to do resource-aware routing of TE Label-Switched Path (LSP) and to program MPLS labels.
- Fast Reroute (FRR) - manages the LSPs that need protection and assigns backup tunnel information to these LSPs.

The interactions between TE and RSVP assume the existence of the endpoint control, link-management, and FRR functionality within TE.

RSVP-TE explicit routing (Strict, Loose)

RSVP-TE explicit routes are particular paths in the network topology that you can specify as abstract nodes in the Explicit Route Object (ERO). These nodes could be a sequence of IP prefixes or a sequence of autonomous systems. The explicit path can be administratively specified or automatically computed using an algorithm such as constrained shortest path first (CSPF).

The explicit path specified in the ERO could be a strict path or a loose one.

A strict path means that a network node and its preceding node in the ERO must be adjacent and directly connected.

A loose ERO (hop) means that a network node specified in the ERO must be in the path but is not required to be directly connected to its preceding node. If a loose hop is encountered during ERO processing, the node that processes the loose hop can update the ERO with one or more nodes along the path from itself to the next node in the ERO. The advantage of a loose path is that the entire path does not need to be specified or known when creating the ERO. The disadvantage of a loose path is that it can result in forwarding loops during transients in the underlying routing protocol.

Note RSVP-TE tunnels cannot be configured with loose hops when provisioning using the UI.

RSVP FRR (Fast Reroute)

When a router’s link or neighboring device fails, the router often detects this failure by receiving an interface-down notification. When a router notices that an interface has gone down, it switches LSPs going out of that interface onto their respective backup tunnels (if any).

The FRR (Fast Reroute) object is used in the PATH message and contains a flag that identifies the backup method to be used as facility-backup. The FRR object specifies setup and hold priorities, which are included in a set of attribute filters and bandwidth requirements to be used in the selection of the backup path.

The Record Route Object (RRO) in the RESV (Reservation) message reports the availability or use of local protection (such as FRR) on an LSP. It also indicates whether bandwidth protection and node protection are available for that LSP.

The signaling of the FRR requirements is initiated at the TE tunnel headend. Along the path, Points of Local Repair (PLRs) evaluate the FRR requirements based on the availability of backup tunnels at the PLR. If a suitable backup tunnel is available, the PLR selects it and signals the backup tunnel information to the headend. When an FRR event is triggered (e.g., a link or node failure), the PLR sends PATH messages through the backup tunnel to the merge point (MP), where the backup tunnel rejoins the original LSP. The MP, in turn, sends RESV messages back to the PLR using the RSVP-Hop object included by the PLR in its PATH message. This mechanism ensures that the original LSP is not torn down by the MP during the failover process.

Additionally, the PLR signals the TE tunnel headend with a PATH-ERROR message to indicate the failure along the original LSP and that FRR is actively in use for the affected LSP. Using this information, the headend establishes a new LSP for the TE tunnel. Once the new LSP is set up (using make-before-break techniques), the headend tears down the failed path.

RSVP-TE tunnel PCC and PCE configuration sources

RSVP-TE tunnels discovered and reported by Crosswork may have been configured from the following sources:

- Path Computation Client (PCC) initiated—RSVP-TE tunnels configured directly on a PCC (see PCC-initiated RSVP-TE tunnel example, on page 8).
- Path Computation Element (PCE) or PCC initiated dynamically—RSVP-TE tunnels dynamically computed and established by a PCE or requested by a PCC.

RSVP-TE tunnels configured on a PCC or dynamically initiated by a PCE or PCC can be visualized in Crosswork Network Controller.

Sample policy and device configurations

This section provides samples of policy and device configurations related to Traffic Engineering and Optimization functions.

To ensure that Traffic Engineering and telemetry functions operate successfully within Crosswork Network Controller, you must properly configure the devices. For more details on configuring devices to work with other Crosswork Network Controller functions, see the "Onboard Devices" chapter in the Cisco Crosswork Infrastructure and Applications Administration guide.

Crosswork Network Controller can discover and visualize pre-existing services that it did not create (such as brownfield service implementations). The details of these service configurations will be visible in the topology screen when you select a policy from the table. However, these policies will be marked as unmanaged in Crosswork Network Controller. To modify these services, administrators can use a combination of device CLI, NSO's service models or APIs, the Crosswork Network Controller UI tool set, and in some case scripts to migrate pre-existing services from being un-mamanged to being managed.

PCC-initiated SR-TE policy example

This example demonstrates the configuration of an SR-TE policy on the headend router. The policy uses a dynamic path that is computed by the headend router based on specified affinity constraints. In this example, a policy named **SampleSRTE** is created with the following attributes: a color value of 100, a candidate preference of 100, a metric of type **TE**, and an affinity constraint to exclude links assigned the color **red**.

See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example, *Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers*).

```
segment-routing
 traffic-eng
  policy sampleSRTE
   color 100 end-point ipv4 1.1.1.2
   candidate-paths
    preference 100
     dynamic
      metric
       type te
      !
     !
     constraints
      affinity
       exclude-any
        name RED
       !
      !
     !
    !
   !
```

Policy source-address configuration to support multiple loopback IP addresses

In order to support multiple loopback IP addresses, these policy configurations must be included on any PCC device that will act as the headend or orignation point for a policy.

Global configuration for all policies

```
Router# segment-routing traffic-eng candidate-paths all source-address ipv4 ip-address
```

Configuration for a specific policy

```
Router# segment-routing traffic-eng policy policy-name source-address ipv4 ip-address
```

PCC-initiated RSVP-TE tunnel example

The following is a sample device configuration for a PCC-initiated RSVP-TE tunnel. See the appropriate documentation to view descriptions and supported RSVP-TE tunnel configuration commands for your particular device (for example, *MPLS Command Reference for Cisco NCS 5500 Series, Cisco NCS 540 Series, and Cisco NCS 560 Series Routers*).

```
interface tunnel-te777
 ipv4 unnumbered Loopback0
 destination 192.168.0.8
 path-option 10 dynamic
 pce
  delegation
!
```

Affinity map configurations

Affinity maps allow network operators to associate human-readable names (such as "red," "low delay," or "high bandwidth") with specific bit positions that represent link attributes. If an affinity mapping is not defined in the Crosswork Network Controller UI, the affinity name is displayed as "UNKNOWN". To configure the affinity attribute for visualization purposes as part of an SR-TE policy, Tree-SID, RSVP-TE tunnel, or any other policy supported by Crosswork Network Controller, the affinity map configured on the device must also be recreated in Crosswork Network Controller. Start by collecting the affinity mappings configured on the device, and then define the same mappings in the Crosswork Network Controller UI with matching names and bit positions.

SR-TE affinity map configuration on a device

This example is a sample SR-TE affinity mapping configuration on a device. For more information, see Configure TE link affinities in Crosswork Network Controller.

```
RP/0/RP0/CPU0:c12#sh running-config segment-routing traffic-eng affinity-map
Wed Jul 27 12:14:50.027 PDT
segment-routing
 traffic-eng
  affinity-map
   name red bit-position 1
   name blue bit-position 5
   name green bit-position 4
  !
 !
!
```

Flexible Algorithm affinity map configuration on a device

This example is a sample Flexible Algorithm affinity mapping configuration on a device. For more information, see Configure Flexible Algorithm affinities in Crosswork Network Controller.

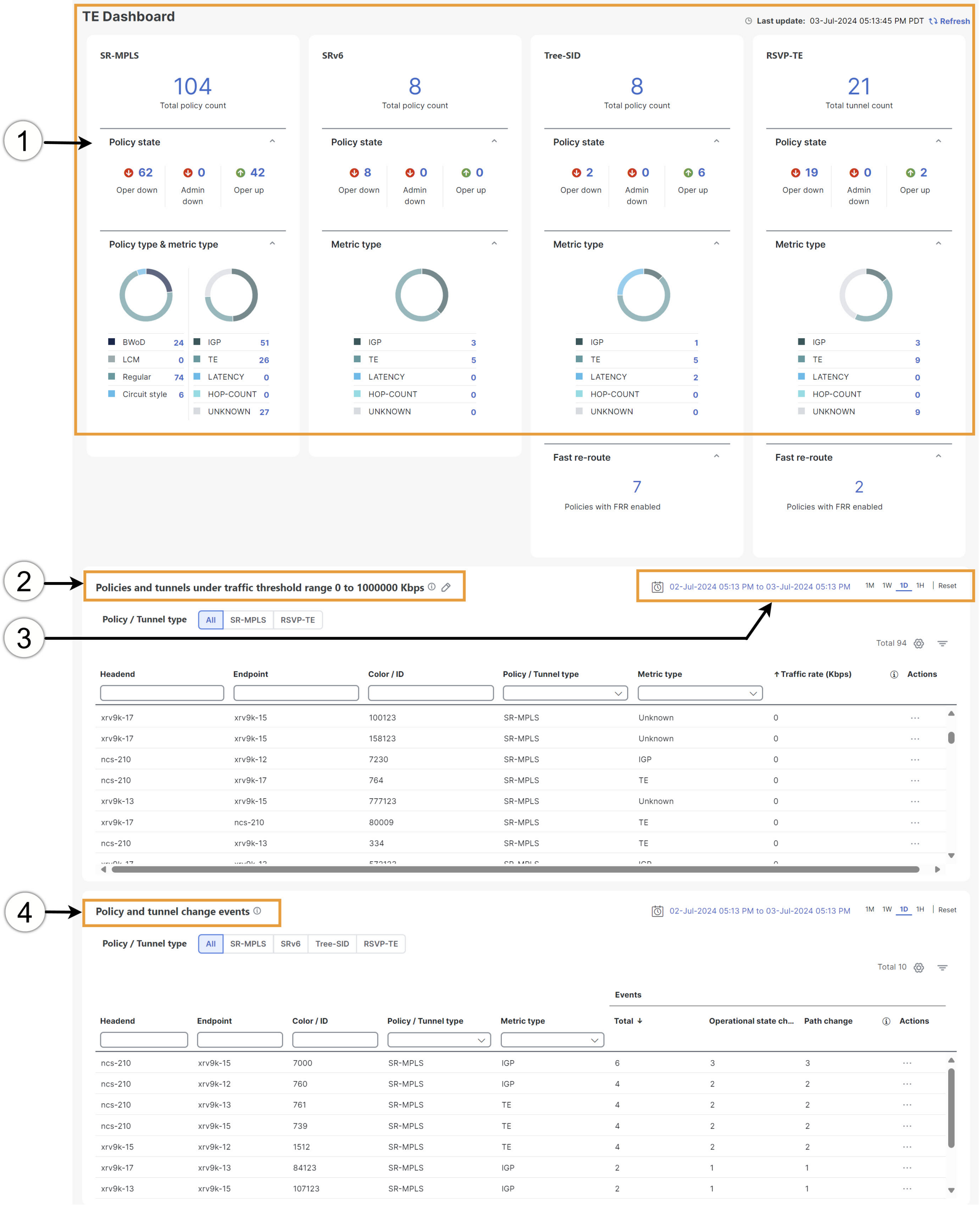
```
router isis CORE
 is-type level-2-only
 net 49.0001.0000.0000.0002.00
 log adjacency changes
 affinity-map b33 bit-position 33
 affinity-map red bit-position 1
 affinity-map blue bit-position 5
 flex-algo 128
  priority 228
  advertise-definition
  affinity exclude-any blue indigo violet black
 !
```

The Traffic Engineering Dashboard

The Traffic Engineering Dashboard provides a high-level summary of RSVP-TE tunnel, SR-MPLS, SRv6, and Tree-SID policy information.

To see the Traffic Engineering Dashboard, choose **Services & Traffic Engineering** > **TE Dashboard**.

Figure 1: Traffic Engineering Dashboard



TE Dashboard

Last update: 03-Jul-2024 05:13:45 PM PDT Refresh

	SR-MPLS	SRv6	Tree-SID	RSVP-TE
Total count	104 Total policy count	8 Total policy count	8 Total policy count	21 Total tunnel count
Policy state: Oper down	62	8	2	19
Policy state: Admin down	0	0	0	0
Policy state: Oper up	42	0	6	2

SR-MPLS – Policy type & metric type

Policy type	
BWoD	24
LCM	0
Regular	74
Circuit style	6

Metric type	SR-MPLS	SRv6	Tree-SID	RSVP-TE
IGP	51	3	1	3
TE	26	5	5	9
LATENCY	0	0	2	0
HOP-COUNT	0	0	0	0
UNKNOWN	27	0	0	9

Fast re-route

Tree-SID: 7 Policies with FRR enabled

RSVP-TE: 2 Policies with FRR enabled

Policies and tunnels under traffic threshold range 0 to 1000000 Kbps

02-Jul-2024 05:13 PM to 03-Jul-2024 05:13 PM 1M 1W 1D 1H | Reset

Policy / Tunnel type: All | SR-MPLS | RSVP-TE

Total 94

Headend	Endpoint	Color / ID	Policy / Tunnel type	Metric type	↑ Traffic rate (Kbps)	Actions
xrv9k-17	xrv9k-15	100123	SR-MPLS	Unknown	0	...
xrv9k-17	xrv9k-15	158123	SR-MPLS	Unknown	0	...
ncs-210	xrv9k-12	7230	SR-MPLS	IGP	0	...
ncs-210	xrv9k-17	764	SR-MPLS	TE	0	...
xrv9k-13	xrv9k-15	777123	SR-MPLS	Unknown	0	...
xrv9k-17	ncs-210	80009	SR-MPLS	TE	0	...
ncs-210	xrv9k-13	334	SR-MPLS	TE	0	...

Policy and tunnel change events

02-Jul-2024 05:13 PM to 03-Jul-2024 05:13 PM 1M 1W 1D 1H | Reset

Policy / Tunnel type: All | SR-MPLS | SRv6 | Tree-SID | RSVP-TE

Total 10

					Events			
Headend	Endpoint	Color / ID	Policy / Tunnel type	Metric type	Total ↓	Operational state ch...	Path change	Actions
ncs-210	xrv9k-15	7000	SR-MPLS	IGP	6	3	3	...
ncs-210	xrv9k-12	760	SR-MPLS	IGP	4	2	2	...
ncs-210	xrv9k-13	761	SR-MPLS	TE	4	2	2	...
ncs-210	xrv9k-15	739	SR-MPLS	TE	4	2	2	...
xrv9k-15	xrv9k-12	1512	SR-MPLS	TE	4	2	2	...
xrv9k-17	xrv9k-13	84123	SR-MPLS	IGP	2	1	1	...
xrv9k-13	xrv9k-15	107123	SR-MPLS	IGP	2	1	1	...

Note If you are viewing the HTML version of this guide, click the images to view them in full-size.

Callout No.	Description
1	**Traffic Engineering Dashlet**: Displays the total policy count and count of policies according to the policy state. It also displays the number of all TE policies and the number of policies or tunnels according to the metric types for all TE services. To drill down for more information, click on a value. The topology map and TE table appear, displaying only the filtered data you clicked on.
2	**Policies and Tunnels Under Traffic Threshold**: Displays RSVP-TE tunnels and SR-MPLS policies with traffic below the defined threshold in the selected time period. This information may be used to find and filter the unused policies or tunnels. Click ✎ to update the LSP threshold range and change the units from Kbps to Mbps. **Note** Traffic utilization is not captured for SRv6 and Tree-SID policies.
3	Allows you to filter the data on the dashlet based on the time range you want to view (date, 1 month, 1 week, 1 day, and 1 hour).
4	**Policy and tunnel change events**: Displays all the policies and tunnels that have had a path or state change event ordered by the event count, within the selected time range. This information helps identify the unstable policies and tunnels. **Note** The addition or deletion of leaf nodes for Tree-SID policies is captured as events.

View TE event and utilization history

The historical data captures the traffic rate and event changes for a policy or tunnel. Traffic rate is not captured for SRv6 or Tree-SID policies. Follow these steps to view traffic engineering events and utilization history.

Before you begin

Ensure that you enable LSP utilization collection and set how long data should be retained. See <c_configure-te-services.xml>.

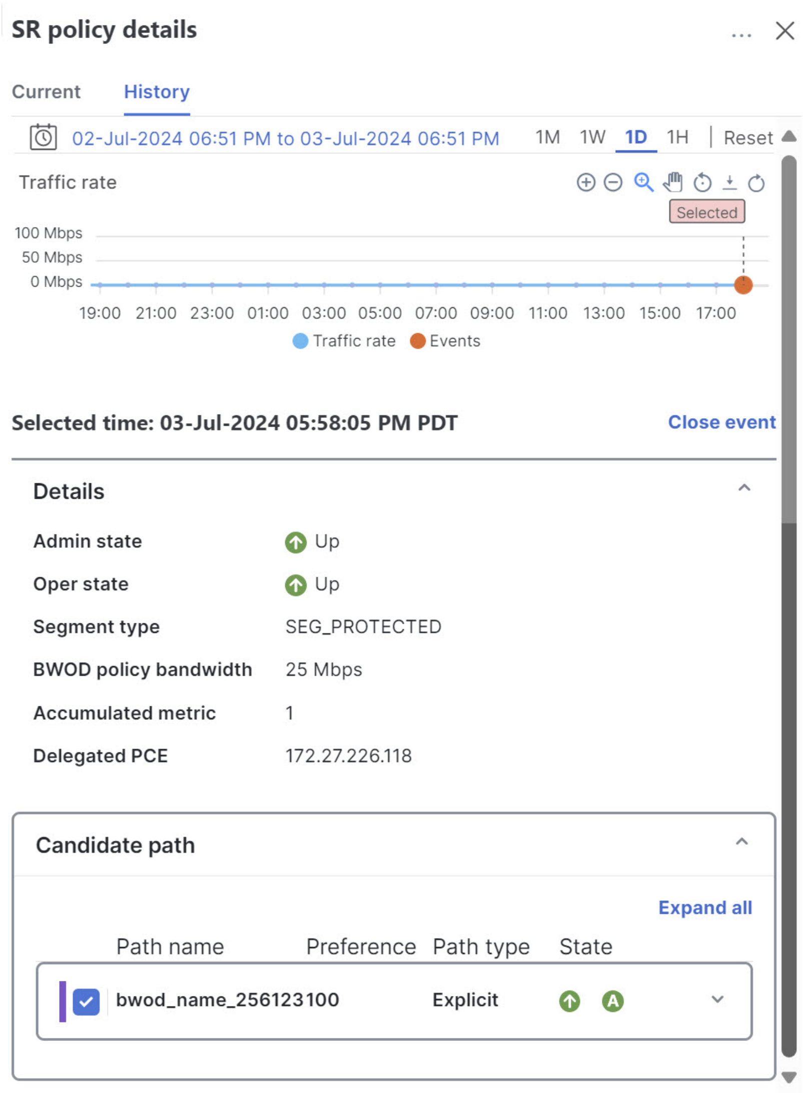
Procedure

Step 1 Choose **Services & Traffic Engineering** > **Traffic Engineering**.

Step 2 From the **Actions** column, choose ⋯ > **View Details** > **History** for a policy or tunnel. The History page displays associated historical data for that device.

Step 3 Click on the event to see the path or state change event information.

Figure 2: TE event and utilization history



Selected time: 03-Jul-2024 05:58:05 PM PDT

Details

Admin state	Up
Oper state	Up
Segment type	SEG_PROTECTED
BWOD policy bandwidth	25 Mbps
Accumulated metric	1
Delegated PCE	172.27.226.118

Candidate path

	Path name	Preference	Path type	State
☑	bwod_name_256123100		Explicit	↑ A

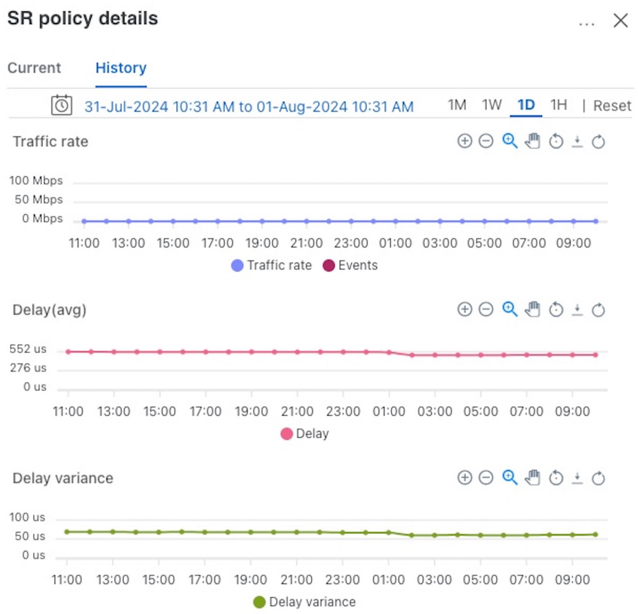
Additional Delay Data

When Crosswork Service Health is installed, Delay (avg) and Delay variance information is available. For more information, see "*Enable SR PM Monitoring for Links and TE Policies*" in the Cisco Crosswork Network Controller Service Health Monitoring Guide.

The extended TE link delay metric (minimum-delay value) can be used to compute paths for SR policies as an optimization metric or as an accumulated delay bound.

This can be used to monitor the end-to-end delay experienced by the traffic sent over an SR policy to ensure that the delay does not exceed the requested “upper-bound” and violate SLAs. You can verify the end-to-end delay values before activating the candidate-path or the segment lists of the SR policy in forwarding table, or to deactivate the active candidate-path or the segment lists of the SR policy in forwarding table.

Figure 3: Example of VPN service when monitoring is enabled



View TE device details

Follow these steps to view traffic engineering device details (SR-MPLS, SRv6, RSVP-TE, and Flexible Algorithm information).

Procedure

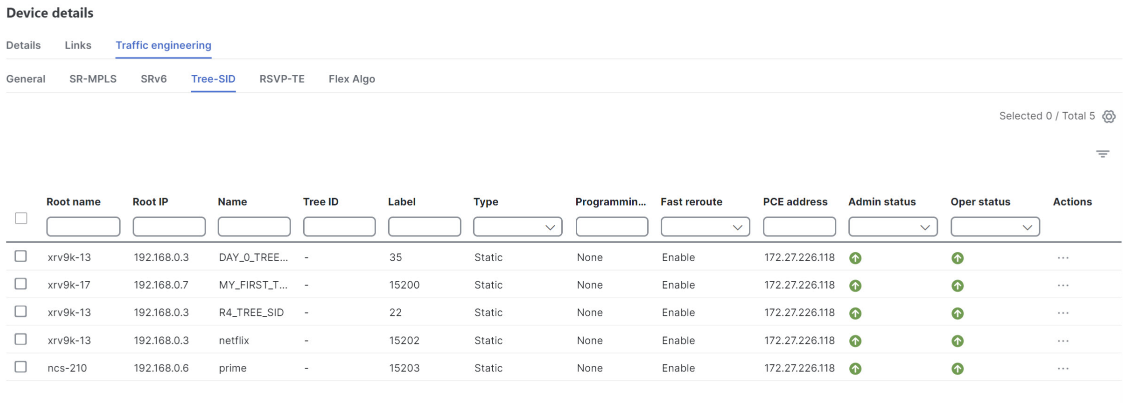
Step 1 Choose **Services & Traffic Engineering** > > **Traffic Engineering**.

Step 2 In the topology map, select a device.

Step 3 Under **Device details** , choose **Traffic engineering** > ***policy-tunnel-type***. Each tab displays associated policy or tunnel data for that device.

This example shows the Tree-SID information details for the selected device.

Figure 4: Traffic engineering device details



Device details

Selected 0 / Total 5

□	Root name	Root IP	Name	Tree ID	Label	Type	Programmin...	Fast reroute	PCE address	Admin status	Oper status	Actions
□	xrv9k-13	192.168.0.3	DAY_0_TREE...	-	35	Static	None	Enable	172.27.226.118	●	●	···
□	xrv9k-17	192.168.0.7	MY_FIRST_T...	-	15200	Static	None	Enable	172.27.226.118	●	●	···
□	xrv9k-13	192.168.0.3	R4_TREE_SID	-	22	Static	None	Enable	172.27.226.118	●	●	···
□	xrv9k-13	192.168.0.3	netflix	-	15202	Static	None	Enable	172.27.226.118	●	●	···
□	ncs-210	192.168.0.6	prime	-	15203	Static	None	Enable	172.27.226.118	●	●	···

Note
If you are viewing the HTML version of this guide, click the image to view it in full-size.

Step 4 (Optional) To share this information you can copy the URL and send the link to others.

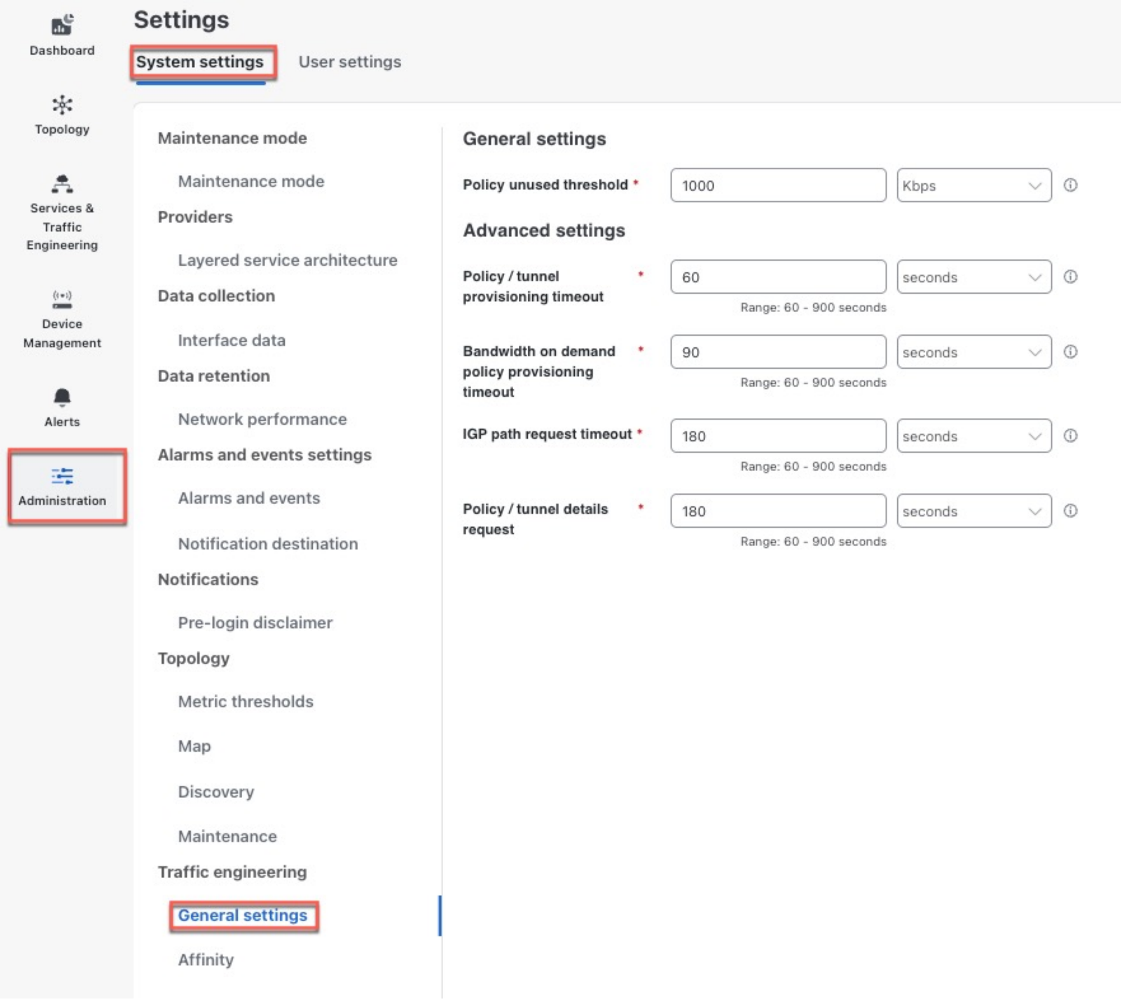
Configure TE settings

Configure TE timeout settings

To configure timeout settings for the provisioning and retrieval of data for SR-TE policies, RSVP-TE tunnels, Bandwidth on Demand and IGP paths, select **Administration** > **Settings** > **System settings** tab > **Traffic engineering** > **General settings**. Enter the timeout duration options. For more information, click ⓘ.

Note Timeouts change the response time of action if SR-PCE is slow in responding. You can modify the settings for a large-scale topology or to address slow SR-PCE response due to latency or load.

Figure 5: Traffic engineering timeout settings



General settings

Policy unused threshold * 1000 Kbps

Advanced settings

Policy / tunnel provisioning timeout * 60 seconds
Range: 60 - 900 seconds

Bandwidth on demand policy provisioning timeout * 90 seconds
Range: 60 - 900 seconds

IGP path request timeout * 180 seconds
Range: 60 - 900 seconds

Policy / tunnel details request * 180 seconds
Range: 60 - 900 seconds

Configure how device groups are displayed for TE

You can configure what is shown on the topology map when a device group is selected, and a device in the selected SR policy, service, or RSVP-TE tunnel does not belong in the group. To set the behavior, choose **Administration** > **Settings** > **User settings** tab > **Switch device group** and select one of the behavior options.

By default, the user is asked to choose the device group view each time.

Configure TE data retention settings

To see a historical view of LSP utilization (Historical tab), you must enable LSP utilization collection and specify how long data should be retained. To do this, choose **Administration** > **System settings** > **Data retention** > **Network performance** and check the **LSP utilization** check box. Optionally, you can edit the default data retention periods.

Note If the retention period is reduced, all data older than the new retention period is lost. For example, if the daily retention interval is set to 31 days, then reduced to 7 days, then all data older than 7 days will be deleted.

Resolve SR-TE policies and RSVP-TE tunnels

Orphaned TE policies are any PCE initiated SR-TE policies (SRv6, SR-MPLS, and Tree-SID) or RSVP-TE tunnels that were created within Crosswork Network Controller and *after* the last cluster data synchronization. After a switchover in a High Availability setup, the system automatically checks for any orphaned TE policies. Orphaned policies/tunnels may also happen after a backup/restore operation. You can view policy details but not modify them since they were not included in the last data synchronization. Crosswork Network Controller will display an alarm when it finds orphan TE policies (**Alerts** > **Alarms and Events**).

Crosswork Network Controller provides APIs to help clear these orphans. To get a list of orphan SR-TE policies or RSVP-TE tunnels, use **cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** or **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** where **is-orphan=True** and default action is GET. To make the orphans manageable again, use a SAVE action for the corresponding URL per policy type. For more information, see API documentation on Devnet (**API Reference** > **Crosswork Optimization Engine**).