Visualize SR Policies and RSVP-TE Tunnels

Note Throughout this document TE tunnels refer to both SR policies and RSVP-TE tunnels.

Cisco Crosswork Optimization Engine visualization provides the most value by giving you the ability to easily view and manage SR policies and RSVP-TE tunnels. By visually examining your network, the complexity of provisioning and managing these TE tunnels is significantly reduced.

To view supported TE tunnel features and limitations, see SR Policy and RSVP-TE Tunnel Support, on page 1.

This section contains the following topics:

SR Policy and RSVP-TE Tunnel Support

The following lists provide an overview of SR policy and RSVP-TE tunnel supported and unsupported features. Contact your Cisco Crosswork Optimization Engine representative for any capabilities that are not documented in the following lists.

Table 1: Supported Features

Category	Capability	Notes
RSVP-TE	• PCE-initiated tunnels (provisioned or discovered by Crosswork Optimization Engine) • PCC-initiated tunnels (discovered by Crosswork Optimization Engine)	—
	• ERO strict hops • ERO loose hops (PCC-initiated only)	—
	FRR protection on tunnels provisioned by Crosswork Optimization Engine	—
	Path optimization objective min-metric (IGP,TE, or Latency)	—
	Path constraints (affinity and disjointness)	Only 2 RSVP tunnels per disjoint group or sub-id is supported
	Binding Label for explicit and dynamic tunnels	—
	Signaled Bandwidth	—
	Setup/Hold Priority	—

Category	Capability	Notes
SR Policy	• PCE-initiated tunnels (provisioned or discovered by Crosswork Optimization Engine) • PCC-initiated tunnels (discovered by Crosswork Optimization Engine) • SR On-Demand Next Hop (ODN) policies discovered by Crosswork Optimization Engine	—
	Single consistent Segment Routing Global Block (SRGB) configured on routers throughout domain covered by Crosswork Optimization Engine	If index SIDs are used and there are different SRGB bases along a path of a policy, the label can change along the path.
	• Prefix SID • Adjacency SID • EPE adjacency SID	—
	Protected and Unprotected adjacency SIDs	—
	Regular and Strict prefix SIDs	—
	SR policy optimization objective min-metric (IGP, TE, and Latency)	—
	SR policy path constraints (affinity and disjointness)	Only 2 SR policies per disjoint group or sub-id are supported
	Binding SID for explicit or dynamic policies	—
	Profile ID	—

Table 2: Unsupported Features and Limitations

Category	Description	Notes
RSVP-TE	Configuring loose hop ERO in COE	Only strict hops can be configured. If strict hops are not configured for every hop along the path and those hops are not remote interface IPs or loopback IPs, unexpected behavior may occur. For example, a tunnel may remain operationally down, hops may be modified, and so on.
	Named tunnels configured on PCCs	These tunnels are not discovered byCrosswork Optimization Engine.
	Tunnels with Loopback IPs other than TE router ID for headend or endpoint and path hops	—
	Display of active FRR protected paths in the topology map.	Crosswork Optimization Engine discovers FRR tunnels which are displayed in the topology map, but will not associate an actively protected tunnel with the FRR tunnel being used. The path in the topology map will not include FRR protected paths when protection is active.
	P2MP tunnels	—

Category	Description	Notes
SR Policy	Provisioning multiple candidate paths via Crosswork Optimization Engine	These paths are not discovered if configured on PCC. Crosswork Optimization Engine does not support configuration of these paths.
	Weighted Equal-Cost Multipath (WECMP)	—
	Multiple segment lists per candidate path	• Crosswork Optimization Engine does not support this configuration • If configured on a PCC, Crosswork Optimization Engine will not discover these segment lists.
	Visualization of multiple candidate paths	Only the current active path can be seen in the UI.
	Binding SIDs as Segment List Hops	—
	SR IGP Flexible Algorithm (Flex Algo)	—
	Anycast SIDs	—
	Hop count metric type for policies	Crosswork Optimization Engine does not support provisioning with this metric type and does not discover this metric type if configured on the PCC
	Routers that are not SR-capable	The assumption is that all routers discovered by Crosswork Optimization Engine are SR-capable
	SR policies with Loopback IPs other than TE router ID for headend/endpoint and prefix SIDs in segment list	—
	SR policy provisioned with IPv6 endpoints/hops	—
	SRv6	Only 2 SR policies per disjoint group/sub-id
	SR policy optimization objective min-metric with margin	Not supported for policies provisioned by Crosswork Optimization Engine. Margin is not discovered for PCC-initiated policies.

Category	Description	Notes
	SR policy constraints (resource exclusion or metric bound)	Not supported for policies provisioned by Crosswork Optimization Engine. Constraints are not discovered for PCC-initiated policies.

SR Policy and RSVP-TE Tunnel Configuration Sources

SR policies and RSVP-TE tunnels discovered and reported by Cisco Crosswork Optimization Engine may have been configured from the following sources:

- For SR policies:
  - PCC initiated—Policies configured on a PCC (see PCC-Initiated SR Policy Example, on page 6).
  - PCE initiated—Policies configured on PCE or policies created dynamically by Cisco Crosswork Optimization Engine. A TE tunnel that is configured using Cisco Crosswork Optimization Engine is the only type of TE tunnel that Cisco Crosswork Optimization Engine can modify or delete (see Create and Manage SR Policies, on page 25 or Create and Manage RSVP-TE Tunnels, on page 34).
- For RSVP-TE tunnels:

  Note These tunnels cannot be configured directly on a PCE.

  - PCC initiated—Policies configured on a PCC (see PCC-Initiated RSVP-TE Tunnel Example, on page 7 and Path Computation Client (PCC) Support).
  - Dynamically created.

PCC-Initiated SR Policy Example

The following example shows a configuration of an SR policy at the headend router. The policy has a dynamic path with affinity constraints computed by the headend router. 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 foo
   color 100 end-point ipv4 1.1.1.2
   candidate-paths
    preference 100
     dynamic
      metric
       type te
      !
     !
     constraints
```

```
    affinity
     exclude-any
      name RED
     !
    !
   !
  !
 !
```

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-te0
 ipv4 unnumbered Loopback0
 destination 172.16.255.5
 path-option 10 dynamic
!
```

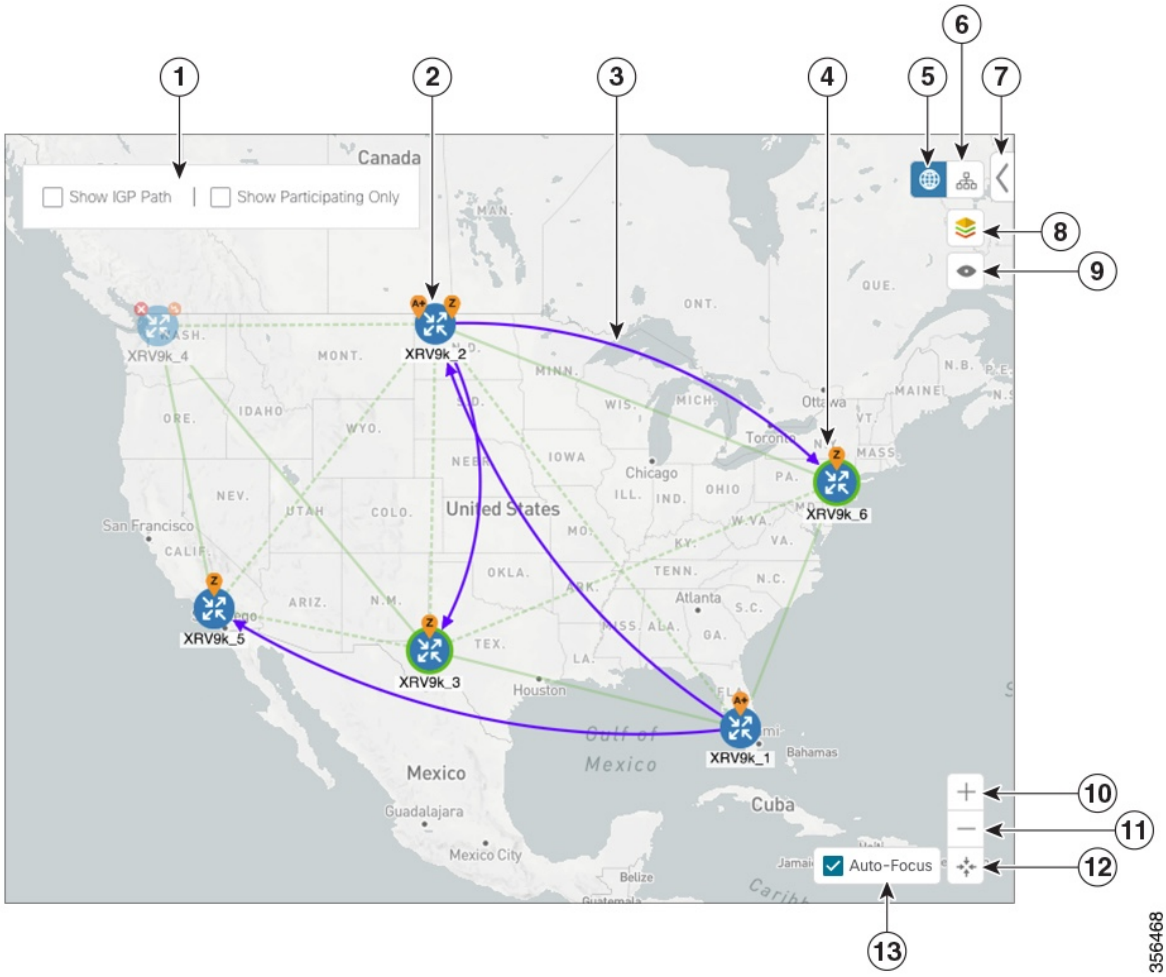
SR Policies and RSVP-TE Tunnels Topology Map

To get to the topology map, choose **Optimization Engine** from the left navigation bar, and click **Traffic Engineering**.

For information on topology issues, or using the map to get information about devices and links, see Network Topology Map and Troubleshoot Network Topology Map.

The following example shows the topology map with SR policies highlighted.

Figure 1: SR Policies Topology Map Example

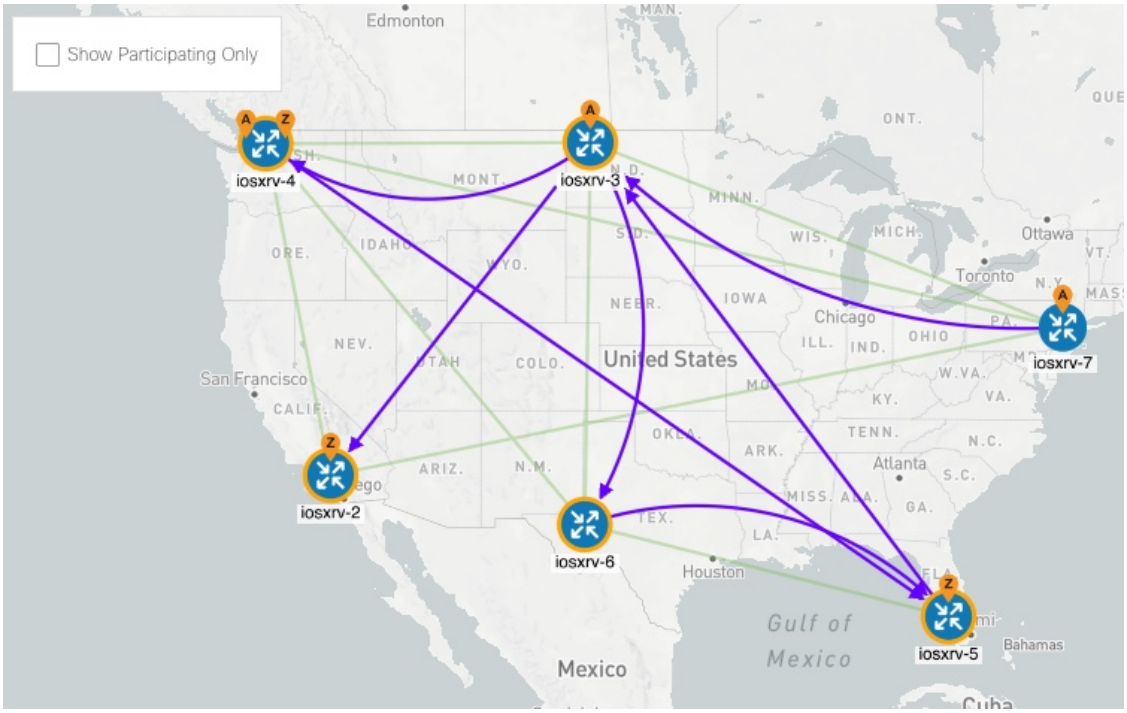


The display of RSVP TE tunnels is similar except for the following:

- The **Show IGP Path** option is not available.
- Record Route Object (RRO) paths are shown as straight lines.
- Explicit Route Object (ERO) paths are shown as curved lines.

Note If both RRO and ERO paths are available, the RRO path is displayed by default.

Figure 2: RSVP-TE Tunnels

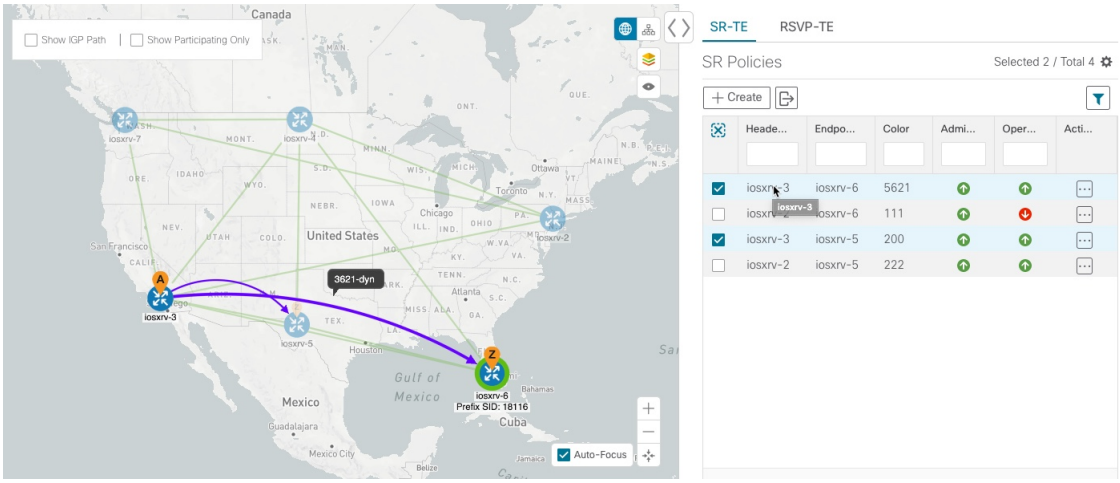


Callout No.	Description
1	Click the appropriate check box to enable the following options: • **Show IGP Path**—Displays the IGP path for the selected SR policy. This option is not available when viewing RSVP TE tunnels. • **Show Participating Only**—Displays only links that belong to selected TE tunnels. All other links and devices disappear.
2	**SR Policy and RSVP-TE Tunnel Origin and Destination**: If both **A** and **Z** are displayed in a device cluster, at least one node in the cluster is a source and another is a destination. The **A+** denotes that there is more than one SR policy or RSVP-TE tunnel that originates from a node. The **Z+** denotes that the node is a destination for more than one TE tunnel.
3	**SR Policies and RSVP-TE Tunnels**: When SR policies or RSVP-TE tunnels are selected from the SR Policies Table, on page 12 or RSVP-TE Tunnels Table, on page 14, they show as purple directional lines on the map indicating source and destination. An adjacency segment ID (SID) is shown as a green dot on a link along the path ( ).

Callout No.	Description
4	SR Policies—A device with a green () outline indicates there is a node SID associated with that device or a device in the cluster. RSVP-TE Tunnels—A device with a solid orange outline ()indicates that it is a strict hop. A dashed orange outline indicates that a loose hop was discovered. **Note** RSVP-TE tunnels cannot be configured with loose hops when using the Crosswork Optimization Engine UI.
5	**Geographical Map**: Click this icon to view the geographical map. The geographical map shows single devices, device clusters, links, and TE tunnels, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory.
6	**Logical Map**: Click this icon to toggle from the geographical map to the logical map. The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm; see Change the Layout of a Logical Map. The logical map displays up to 5000 devices and never displays devices in clusters. If you drill down to the logical map from a geographical cluster at the maximum zoom level, the logical map shows devices that are located in the same location. See Identify the Members of a Cluster.
7	**Expand/Collapse/Hide Side Panel**: Expand or collapse the side panel to see the full and truncated versions of the right-side panel. Close the side panel to get a larger view of the topology map.
8	**Display Preferences**: Lets you edit display settings for devices, links, and SR policy and RSVP-TE tunnel (with RRO) metrics. See Change Display Settings for Links, Devices, and TE Tunnel Metrics. **Note** If path names and metrics are displayed and overlap one another, move the nodes out to show a clearer view of them.
9	**Custom Map View**: Lets you create a named custom view using the settings and layout for your current map, or display a custom view you have created previously. See Create Custom Map Views.
10	**Zoom In**: Click this icon to zoom in on the selected area; for example, to view clustered devices on the geographical map.
11	**Zoom Out:** Click this icon to zoom out from a selection area.
12	**Zoom Fit**: Lets you automatically scale the map to fit your zoom area.
13	**Auto-Focus**: Zooms in on selected TE tunnels. This option is selected by default. If you uncheck this option, navigate away from the map, and later return to the map; it will revert to the default option.

Highlight a TE Tunnel on the Map

When many SR policies or RSVP-TE tunnels are displayed on the map, it may be difficult to view a particular path. To highlight a particular TE tunnel path on the map, navigate to **Optimization Engine** > **Traffic Engineering** > **SR-TE / RSVP-TE** tab, and hover over the SR policy or RSVP-TE tunnel. Prefix SID information will display under the node if it is part of the highlighted path.



Show Participating Nodes and Links

To view only the nodes and links that are part of selected TE tunnels, do the following:

Step 1 From the **SR Policies** or **RSVP-TE Tunnels** table, select the TE tunnel you are interested in.

Step 2 From the top left box in the topology map, check the **Show Participating Only** check box.

Show IGP, Delay, and Traffic Engineering Metrics

Each link is assigned a metric value. The distance between two nodes is the sum of all the metric values of links along a path. To view IGP, Delay, or Traffic Engineering (TE) metrics on the topology map:

Step 1 Navigate to **Optimization Engine** > **Traffic Engineering**.

Step 2 Click the **SR-TE** or **RSVP-TE** tab and check the checkboxes next to the TE tunnels you are interested in. The TE tunnels are highlighted in the topology map.

Step 3 If viewing SR policies from the topology map, check the **Show IGP Path** checkbox.

Step 4 Click .

Step 5 Click the **Metrics** tab.

Step 6 Check the applicable metric check boxes you want displayed.

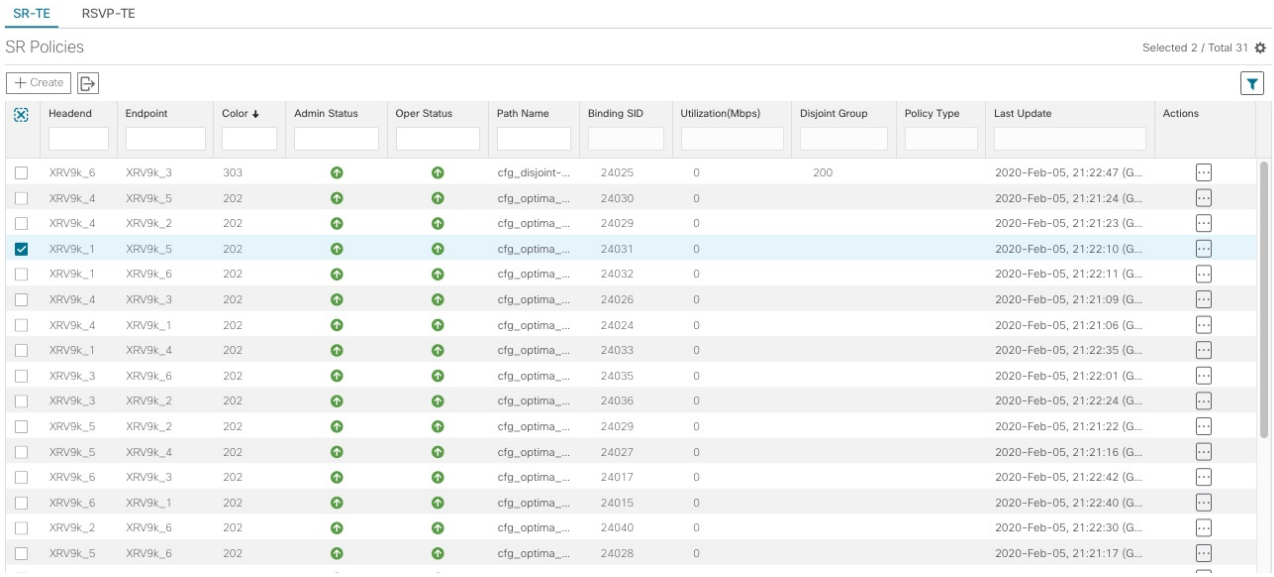
What to do next

To configure a TE tunnel based on one of these metrics, see Create Dynamic Path SR Policies, on page 28 or Create Dynamic Path RSVP-TE Tunnels, on page 36.

SR Policies Table

To get to the **SR Policies** table, choose **Optimization Engine** from the left navigation bar, and click **Traffic Engineering**. You will see the topology map and, to the right of the map, click the **SR-TE** tab.

Figure 3: SR Policies Table



The **SR Policies** table provides the following functions:

- Display a list of all SR Policies discovered from the network.
- Configure new SR policies.
- Export the list of SR policies (click).
- Highlight SR policies on the map when selected from the table. To clear all selected policies, click .
- View SR policy details (click). See Get More Information About an SR Policy, on page 32). From the SR Policy Details page you can edit SR policies. However, only SR policies created from Crosswork Optimization Engine can be modified or deleted on the Crosswork Optimization Engine UI.
- Refresh ( ) the table or policy details (if in the **SR Policy Details** table). You can also view the date and time as to when the last refresh occured.

Note When creating or modifying SR policies, the refresh and auto-refresh functions are disabled in the tables.

The following information is available in the **SR Policies** table:

Note

- If a hostname is not available, click ⚙ and check the Headend IP and Endpoint IP checkboxes to show the respective IP addresses.
- Some fields may be blank depending on the SR policy type.

Table 3:

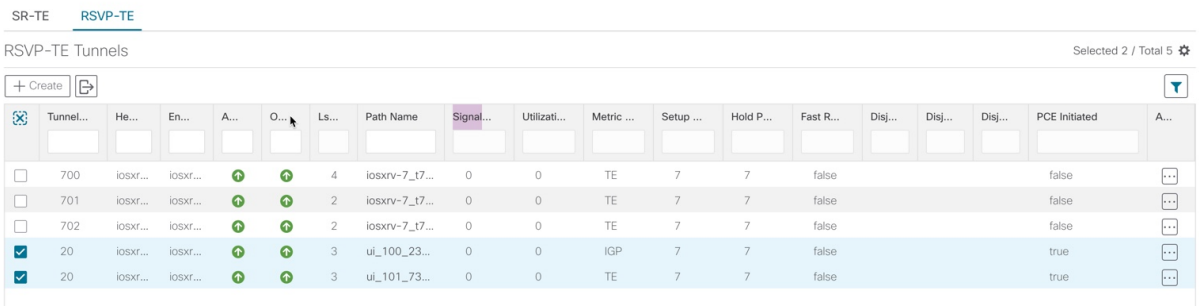
Column Heading	Description
Headend	Where the SR policy is instantiated.
Endpoint	The destination of the SR policy.
Color	A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headed and endpoint must have a unique color.
Admin Status	Administrative status of the SR policy.This is the status defined by the user.
Oper Status	Operational status of the SR policy. This is the state of the policy as reported by the system. For example, the user can define the Admin status as Up. However, if the policy is operationally down due to some network issues, then the Oper Status will display as Down.
Path Name	Name of SR policy path.
Binding SID	The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID).
Utilization	Percentage of total bandwidth being used.
Disjoint Group	If applicable, the disjoint group the SR policy belongs in.

Column Heading	Description
Policy Type	• Bandwidth Optimization • Bandwidth on Demand • Explicit • Dynamic
Last Update	Time when the most recent update for the policy was received from the network.
Actions	Click ⋯ to Get More Information About an SR Policy, on page 32.

RSVP-TE Tunnels Table

To get to the **RSVP-TE Tunnels** table, choose **Optimization Engine** from the left navigation bar, and click **Traffic Engineering**. You will see the topology map and, to the right of the map,select the **RSVP-TE** tab.

Figure 4: RSVP-TE Tunnels Table



The **RSVP-TE Tunnels** table provides the following functions:

- Displays a list of all RSVP-TE tunnels discovered from the network.
- Configure new RSVP-TE tunnels.
- Edit RSVP-TE tunnels created using Crosswork Optimization Engine (click ⋯).

Note Only tunnels created from Crosswork Optimization Engine can be modified or deleted on the Crosswork Optimization Engine UI.

- Highlight RSVP-TE tunnels on the map when selected from the table. To clear all selected tunnels, click .

- View RSVP-TE tunnel details (click on ⋯ link). See Get More Information About an RSVP-TE Tunnel, on page 39.
- Refresh ( ) the table. You can also view the date and time as to when the last refresh occurred.

Note When creating or modifying RSVP-TE tunnels, the refresh and auto-refresh functions are disabled in the tables.

The following information is available in the **RSVP-TE Tunnels** table:

Note If a hostname is not available, click and check the Headend IP and Endpoint IP checkboxes to show the respective IP addresses.

Table 4: RSVP-TE Tunnels

Column Heading	Description
Tunnel ID	The assigned tunnel ID value. The tunnel ID range is taken from the headend configuration.
Headend	Where the RSVP-TE tunnel is instantiated.
Endpoint	The destination of the RSVP-TE tunnel.
Admin Status	Administrative status of the RSVP-TE tunnel. This is the status defined by the user.
Oper Status	Operational status of the RSVP-TE tunnel. This is the state of the policy as reported by the system. For example, the user can define the Admin status as Up. However, if the policy is operationally down due to some network issues, then the Oper Status will display as Down.
LSP ID	This value is updated when there is a change to the path.
Utilization	Percentage of total bandwidth being used.
Metric Type	Type of metric (IGP, TE, or Delay).
Setup Priority	There are 8 (0 - 7) setup priorities. 0 is the most preferred. The setup priority is used to define preference for preempting less preferred tunnels. The most preferred tunnels can push the other less preferred tunnels out of the way.

Column Heading	Description
Hold Priority	There are 8 (0 - 7) hold priorities. The holding priority is used to define a priority maintaining the currently established tunnel. You can have a tunnel that you never want go down, but only establish it if there are plenty of resources. In that case you could configure the setup priority to be 7 and the holding priority to be 0. In this configuration, the tunnel will never get preempted once established.
Fast Reroute	The value is "True" if Fast Reroute is enabled.
Disjoint Group	If applicable, the disjoint group the RSVP-TE tunnel belongs in.
Disjoint Type	Whether is node, link, or SRLG.
PCE Initiated	The value is "true" if the RSVP-TE tunnel was configured directly on the PCE device. It will be "false" if PCC-initiated.
Actions	Click ··· to get more information about the tunnel. If the tunnel was created using the UI, you can also edit or delete this tunnel.

Visualize SR Policies and RSVP-TE Tunnels

This section describes the visualization features provided in the topology map for TE tunnels that have been discovered during the onboard of devices or provisioned using Cisco Crosswork Optimization Engine. To create and manage TE tunnels using Cisco Crosswork Optimization Engine see Create and Manage SR Policies, on page 25 and Create and Manage RSVP-TE Tunnels, on page 34.

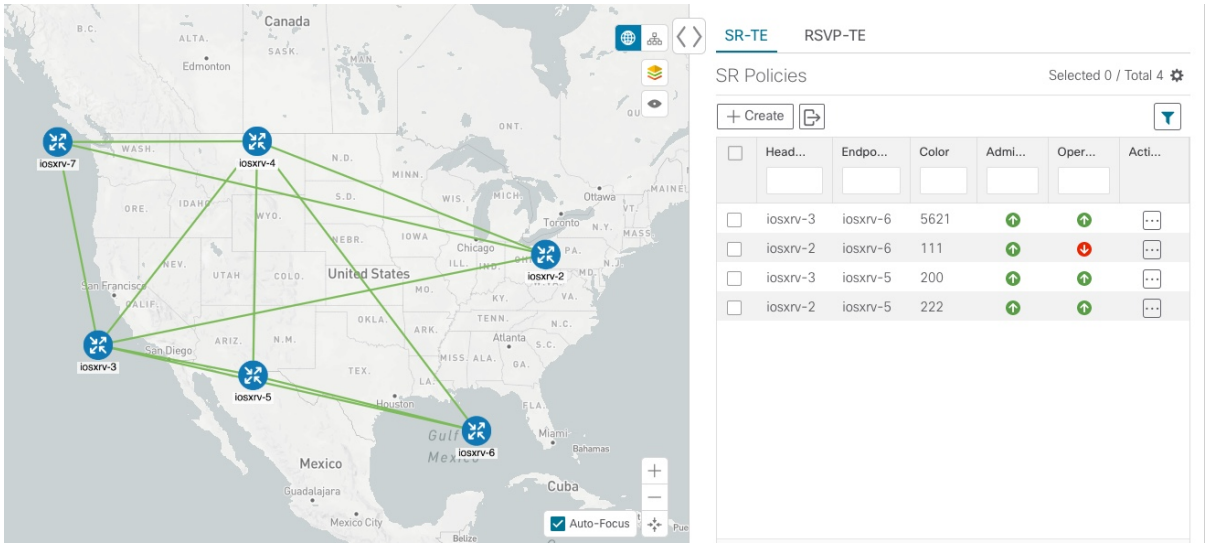
This section contains the following topics:

Visualize TE Tunnels Example

Follow the steps in this example to quickly familiarize yourself with a number of TE tunnel visualization features that are available from the topology map.

In this example, we are using the following geographical map with devices and links that have SR policies configured. SR policies are not yet highlighted in the map.

Figure 5: Topology Map Example

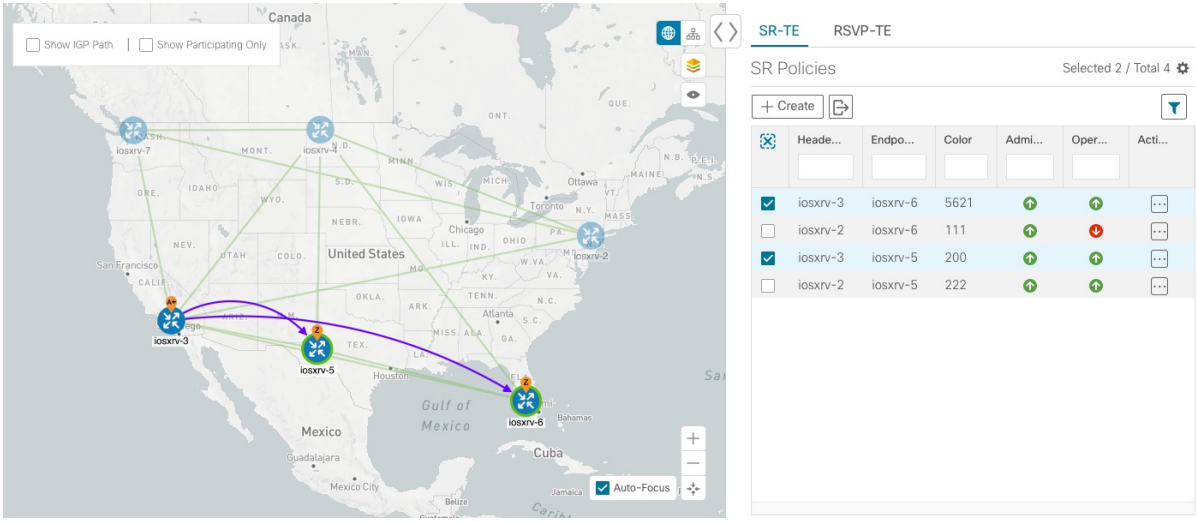


Before you begin

In this example, we assume that devices and SR policies have already been added to Crosswork Optimization Engine (see Get Started). While this example uses SR policies, the basic functionality of the maps for both SR policies and RSVP TE tunnels are the same.

Step 1 From the **SR Policies** table, click the checkbox next to the SR policies you are interested in. In this example, there are two SR policies selected.

Figure 6: SR Policy Selection



After SR policy selection, the map displays the following:

- SR policies appear as purple links with arrows that indicate the path direction.

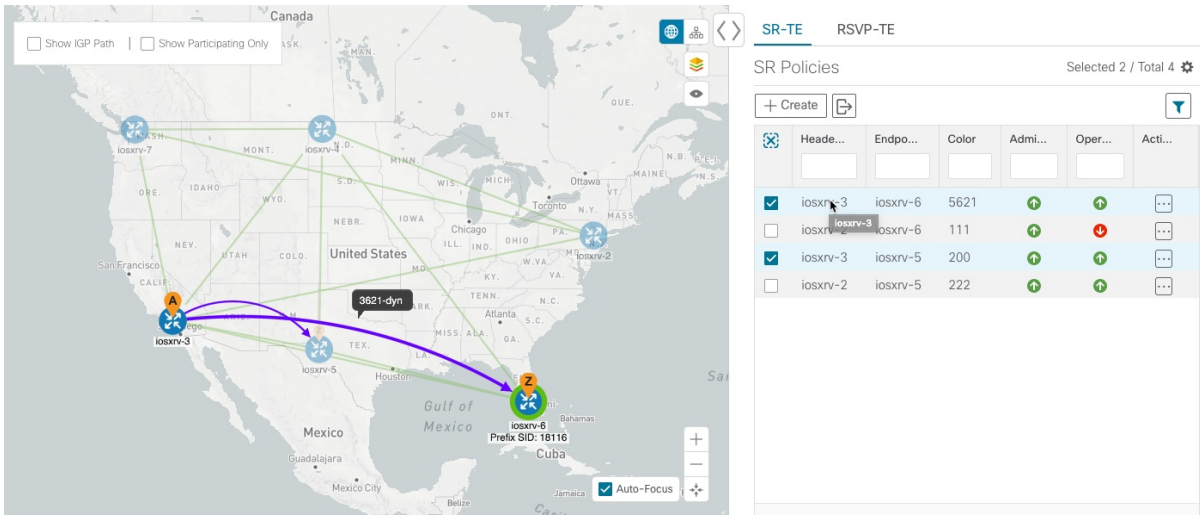
- iosxrv-3 is an origin for the both selected policies. iosxrv-5 and iosxrv-6 are destinations for the selected policies. SR policy origin and destination are marked with **A** and **Z**, respectively. The **A+** denotes that there is more than one policy that originates from a device. A Z+ would denote that the device is a destination for more than one policy.

  Note If both **A** and **Z** are displayed in a device cluster, at least one device in the cluster is a source and another is a destination.

-  indicates that iosxrv-5 and iosxrv-6 have node SIDs.

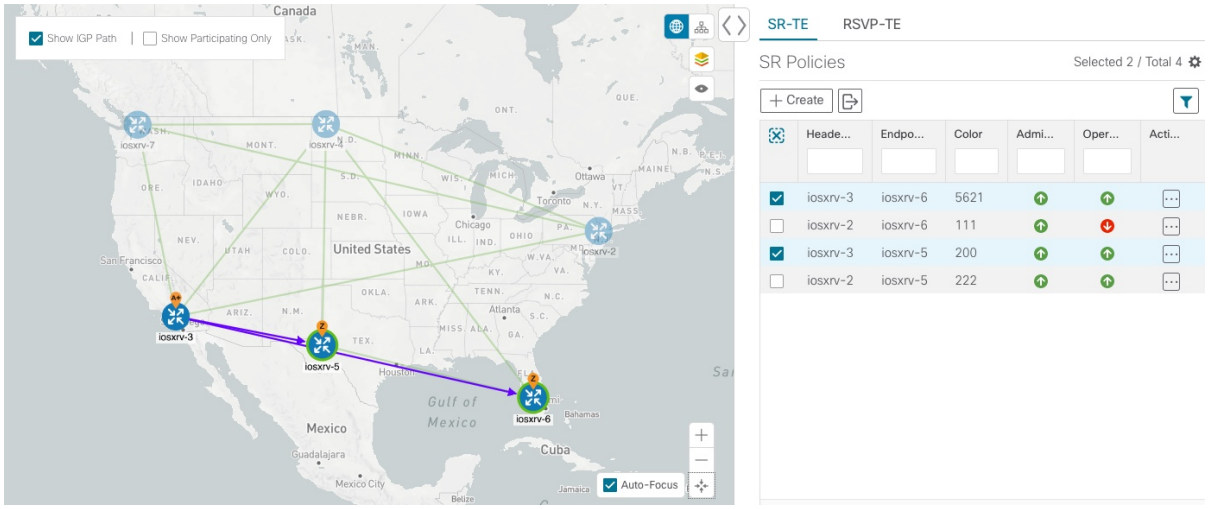
Step 2 From the **SR Policies** table, *hover* over a selected policy. The path name of that policy is highlighted on the topology view. You will also see prefix SID information.

Figure 7: Hover over an SR Policy



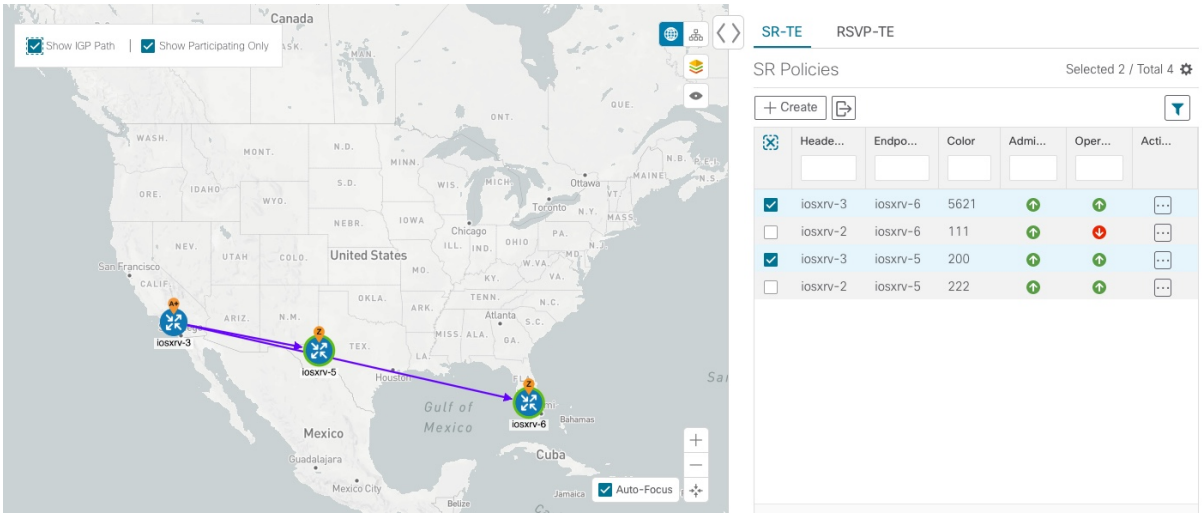
Step 3 Check the **Show IGP Path** check box (available only with SR policies). The IGP paths for the selected SR policies are displayed, with straight lines, instead of the segment hops.

Figure 8: IGP Paths



Step 4 Check the **Show Participating Only** check box. All non-participating links and devices disappear. Only participating policies are displayed.

Figure 9: Participating SR Policies



Step 5 To view the IGP, TE or Delay metrics for each tunnel along a policy's path, do the following:

a) For SR policies only, confirm that the Show IGP Path checkbox is checked.

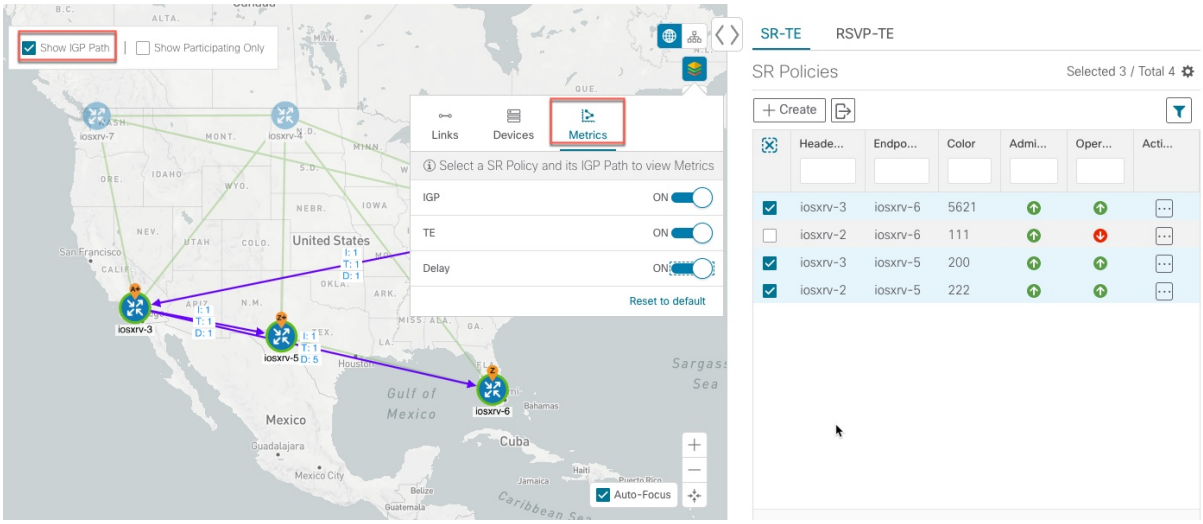
b) Click .

c) Click the **Metrics** tab.

d) Check the applicable metric check boxes.

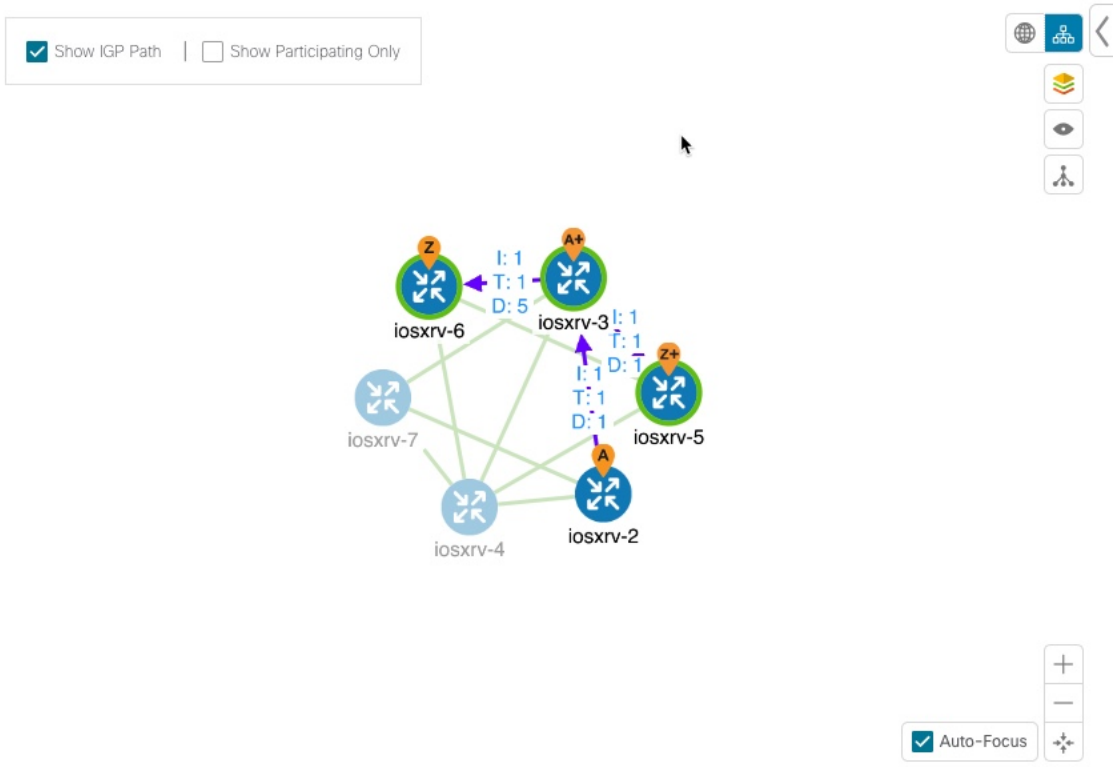
The metric details are displayed for each policy on the map.

Figure 10: IGP, Delay, and TE Metrics



Step 6 Click the logical map icon ( ).

Figure 11: Logical Map

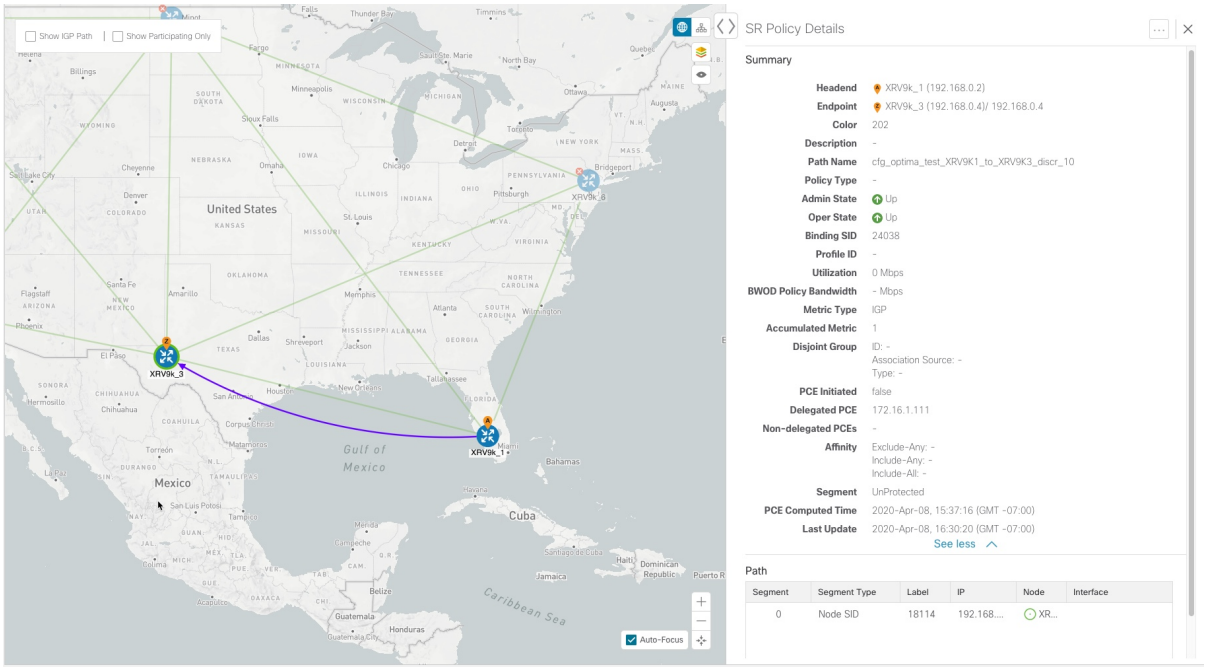


You are able to see the same information (aside from geographical location) that is available on the geographical topology map. You also have the ability to move devices and links on the map to make it easier to view.

Step 7 To view SR policy details such as disjoint groups, metric type, segment hop information, and so on, click ··· under the **Actions** column from the table.

The **SR Policy Details** page is displayed in the side panel (see Get More Information About an SR Policy, on page 32). Note that only the selected policy is now highlighted on the topology map.

Figure 12: SR Policy Details



Note To return to the **SR Policies** table, close (✕) the current view.

What to do next

Provision and manage TE tunnels. See Create and Manage SR Policies, on page 25 and Create and Manage RSVP-TE Tunnels, on page 34.

Configure Affinity Mapping

Affinity of a an SR policy or RSVP-TE tunnel is used to specify the link attributes for which the SR policy or RSVP-TE tunnel has affinity for. It determines which links are suitable to form a path for the SR policy or RSVP-TE tunnel. It is a 32-bit value, with each bit position (0 - 31) representing a link attribute. Affinity mapping is used to map each bit position or attribute to a color. This makes it easier to refer to link attributes.

Note The affinity mapping name is only used for visualization in Cisco Crosswork Optimization Engine. Affinities defined on devices are not collected by Cisco Crosswork Optimization Engine. Define affinity mapping in Cisco Crosswork Optimization Engine with the same name and bits that are used on the device interface. Cisco Crosswork Optimization Enginewill only send bit information to SR-PCE during provisioning.

Step 1 From the main menu choose **Optimization Engine** > **Affinity Mapping**. You can also define affinities while creating an SR policy or RSVP-TE tunnel (Create Dynamic Path SR Policies, on page 28 or Create Dynamic Path RSVP-TE Tunnels, on page 36) by clicking **Manage Mapping**.

Step 2 To add a new affinity mapping, click **Create Mapping**.

a) Enter the name (color) and the bit it will be assigned to.

b) Click to save the mapping.

Step 3 To edit an affinity mapping, click .

a) Make the necessary changes. If you want to cancel your changes, click .

b) Click to save the changes.

Step 4 To delete an affinity mapping, click

Note You should remove the TE tunnel before removing the affinity to avoid orphan TE tunnels. If you have removed an affinity associated to a TE tunnel, the affinity is shown as "UNKNOWN" in the **SR Policy / RSVP-TE Tunnel Details** window.

What to do next

After defining affinities, you can Create Dynamic Path SR Policies, on page 28 or Create Dynamic Path RSVP-TE Tunnels, on page 36.

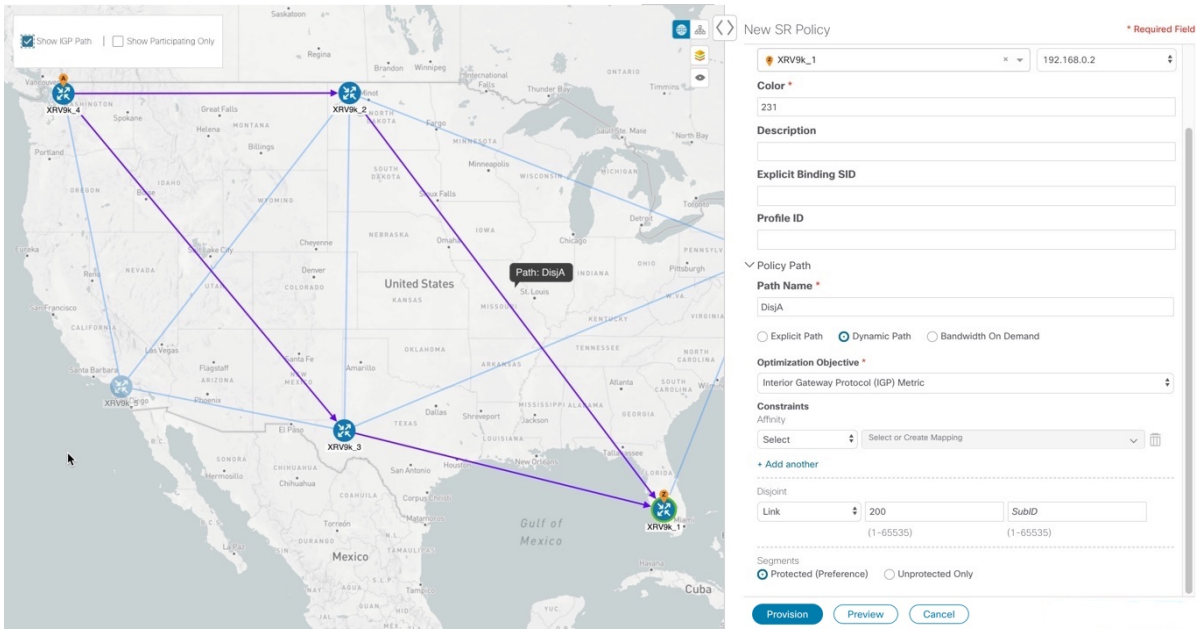
Preview Disjoint SR Policies and RSVP-TE Tunnels

The following example shows how the SR policy and RSVP-TE tunnel provisioning preview feature can be used for disjoint SR policies and RSVP-TE tunnels. In this example, two SR policies will be provisioned with link disjointness. After the first one is provisioned, the preview of the second will show both policies in the map view and how the path of the first would be re-optimized by SR-PCE to make them link disjoint from each other.

Note There cannot be more than 2 disjoint policies in the same disjoint group or subgroup

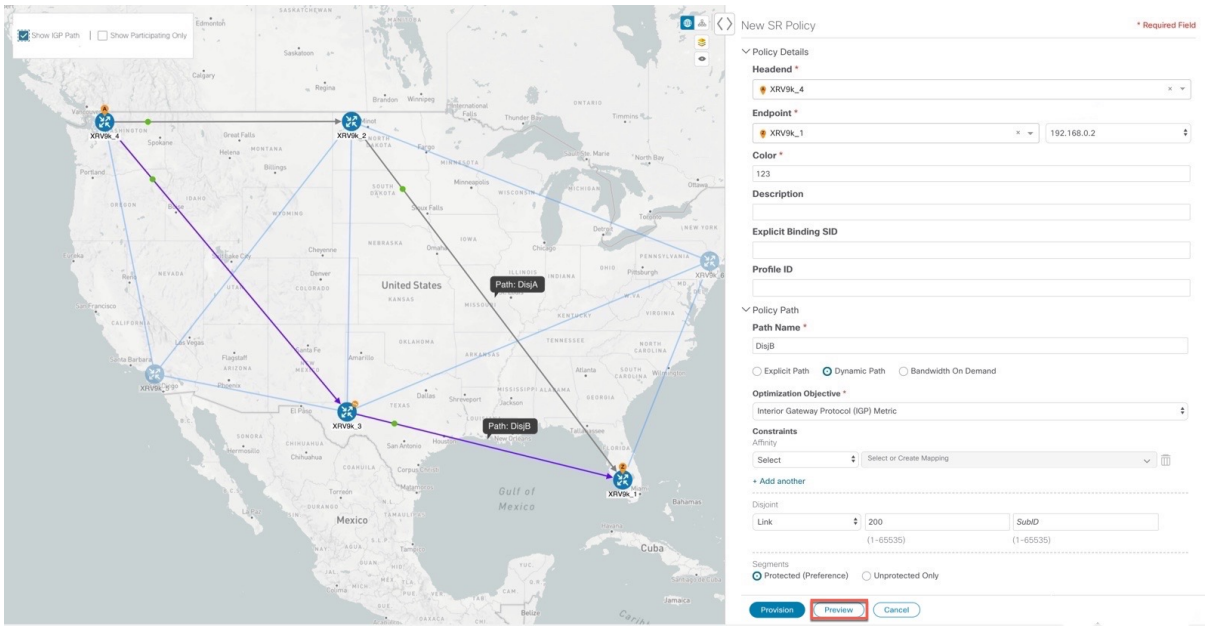
Below is a provisioned dynamic policy (DisjA) belonging to disjoint link group 200. The SR policy has a path that ECMP splits between XRV9k_4 and XRV9k_1 as shown in the following figure.

Figure 13: Example: DisjA SR Policy



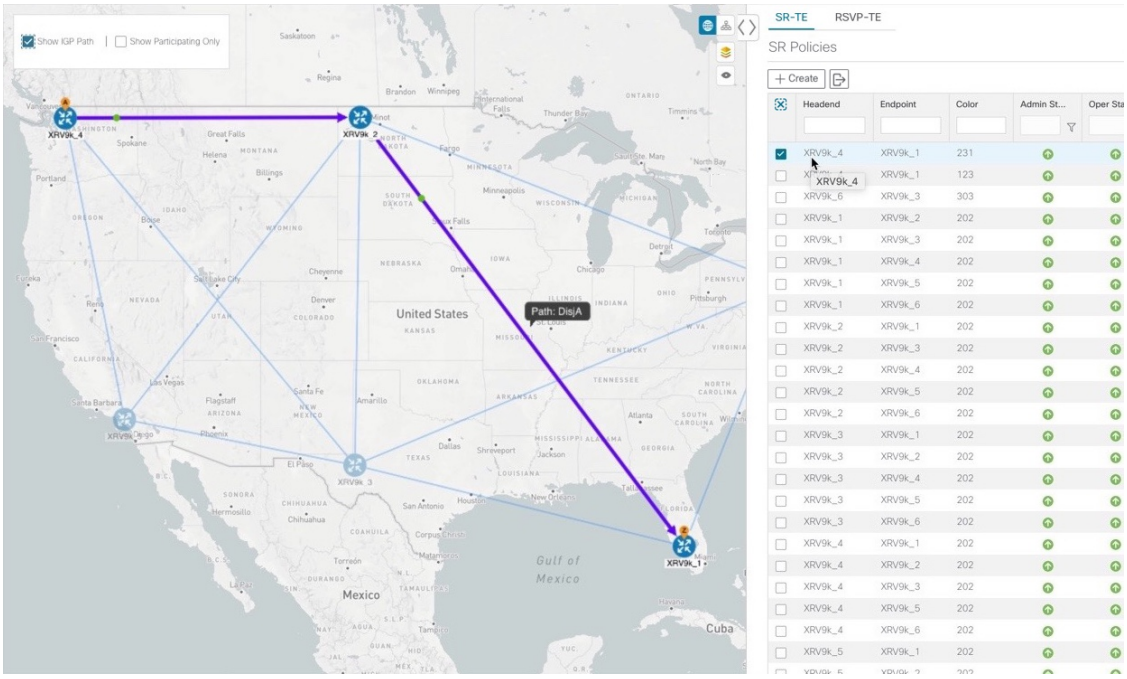
A second policy (DisjB) is now configured in the same disjoint group as the first. When we preview this policy you see both DisjA and DisjB are displayed. You also see the path of DisjA has been reoptimized to ensure both policies are link disjoint. This path change to the existing policy DisjA will be made by SR-PCE if DisjB is provisioned.

Figure 14: Example: Preview Disjoint SR Policies



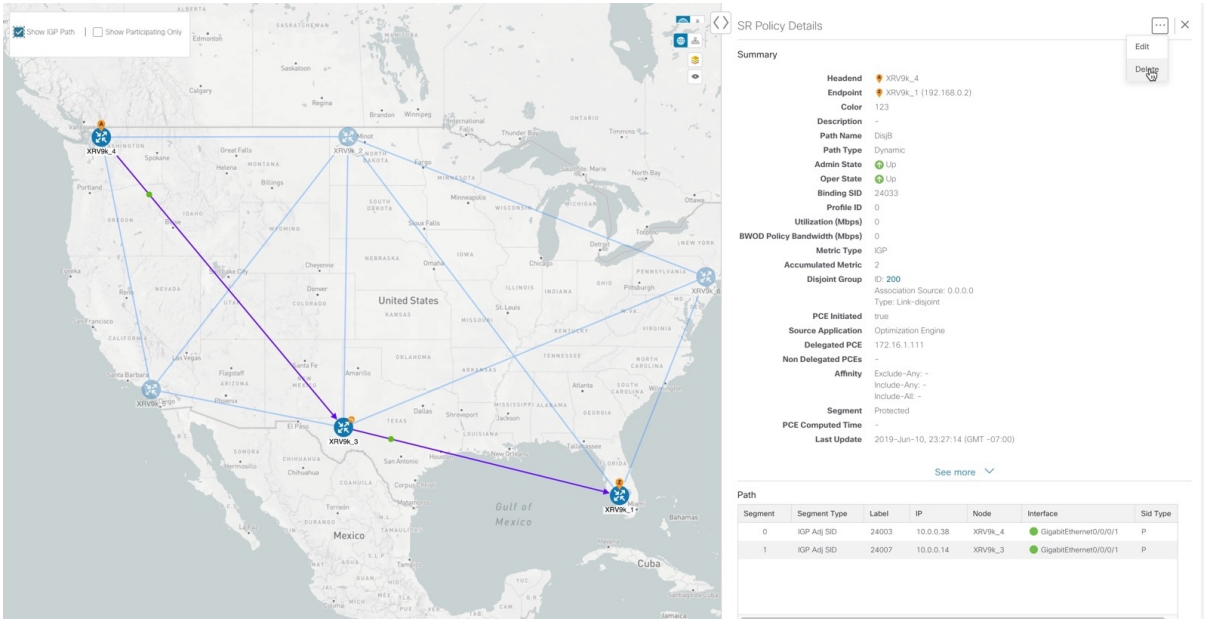
After DisjB is provisioned, we select **View SR Policy List** and check the checkbox next to the DisjA policy to confirm that the path for DisjA has been rerouted.

Figure 15: Example: DisjA SR Policy Rerouted



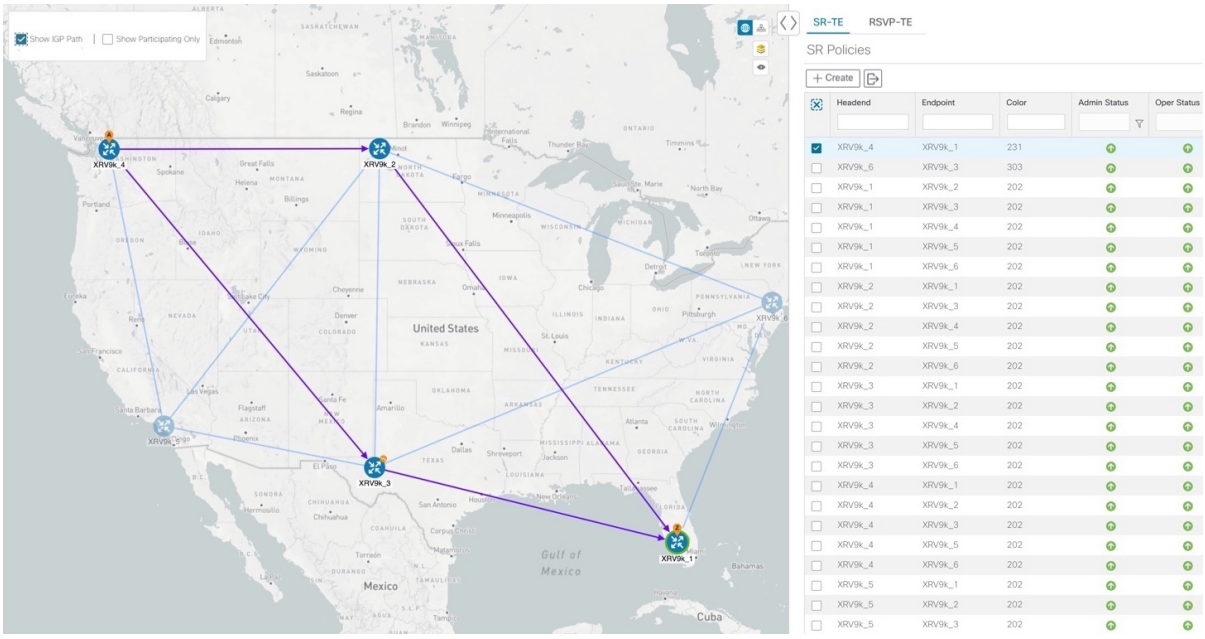
From the SR Policies table, check the checkbox next to DisjB, and delete it.

Figure 16: Example: Delete DisjB SR Policy



After a few seconds, display DisjA again. You will see that it has reset itself and shows two paths from XR.

Figure 17: Example: DisjA SR Policy Reset



View TE Tunnels Belonging to a Disjoint Group

From the **SR Policy Details** or **RSVP-TE Tunnel Details** window, click the **Disjoint Group** ID number to view all TE tunnels that belongs to the disjoint group.

Figure 18: Disjoint Group

To go back to the **SR Policy Details** or **RSVP-TE Tunnel Details** window, click .

Create and Manage SR Policies

This section describes how to provision and manage SR policies using the Cisco Crosswork Optimization Engine UI. The Cisco Crosswork Optimization Engine UI gives you the capability of provisioning SR policies in a variety of methods (explicit, dynamic, and bandwidth constraint driven). As you provision an SR policy, you can select nodes on the topology map and also preview the path before deployment. This greatly reduces

the complexity of SR policy management. Before provisioning SR policies, you should understand some basic segment routing configuration concepts (see Segment Routing Basics).

Note Disjointness is supported for two policies with the same disjoint ID. When configuring disjoint policies do the following:

- Use the same delegated SR-PCE for both SR policies with the same association type, group and subgroup.
- Use the same headend with the same association type, group and subgroup.

Disjointness configuration may fail when the delegated PCE of an existing SR policy is removed or unreachable. This can occur if Cisco Crosswork Optimization Engine is not aware that the PCE is down or missing and, instead, another PCE is used for configuration.

Create Explicit Path SR Policies

This task creates an SR policy using an explicit path (segments) that you define.

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 From the **SR Policies** table, click **+ Create**.

Step 3 Enter the following SR policy values:

a) Required fields:

- **Headend**—Where the SR policy is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the SR policy.
- **Node Prefix**—After the endpoint is selected, the Node Prefix list is populated and you can select the loopback IP address.
- **Color**—A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headed and endpoint must have a unique color. The bit value must match the value that is configured on the device.
- **Path Name**—Enter a name for this SR policy path. SR policy paths from the same headend must be unique. Policy path names are not case sensitive.

b) Optional values:

- **Description**—Enter details or a description of this policy.
- **Explicit Binding SID**—The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated for each SR policy when the policy is instantiated. If you wish to use a specific segment ID, rather than the default one that is automatically assigned, then enter it here.
- **Profile ID**—Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.

Step 4 Under Tunnel Path, click **Explicit Path**.

Step 5 Add segments that are part of the SR policy path.

a) You can either select a node from the drop-down list or enter part of the node name to filter the node list. After a node is selected, the **Select SID** drop-down list is populated with associated prefix and adjacency segment IDs.

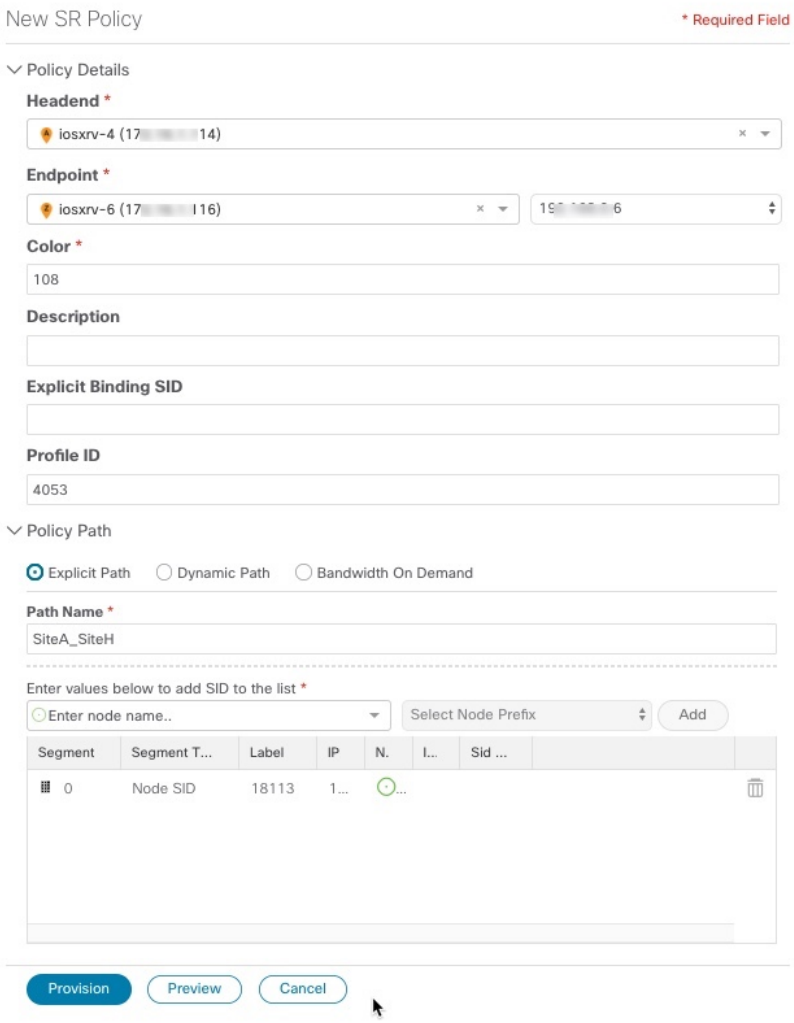
b) Select a segment ID from the **Select SID** drop-down list. The drop-down list contains all available segments. The segment names indicate the associated node and whether it is a prefix or an adjacency segment. The name also includes whether the segment is protected (P) or unprotected (U).

c) Click **Add**. The segment appears in the table with segment values.

d) Repeat for each segment you want to add to the SR policy path. To reorder the segment hops, click and drag ⠿ next to the segment hop you want to move.

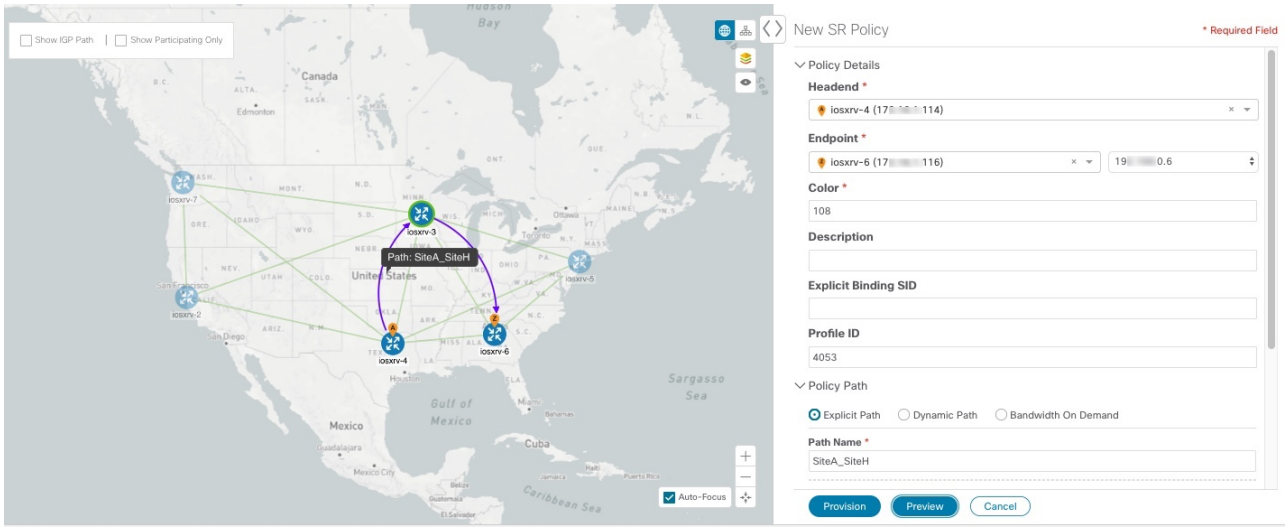
Note The segments must be in order or the path will not be created.

Figure 19: Explicit SR Policy Example



Step 6 Click **Preview**. The path is highlighted on the map and policy details are displayed on the right.

Figure 20: Explicit SR Policy Example



Step 7 If you are satisfied with the policy path, click **Provision**.

Step 8 When the policy is provisioned successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just created.
- **Create New**—Allows you to create another SR policy.

Note The newly provisioned SR policy may take some time, depending on network size and performance, to appear in the **SR Policies** table. The **SR Policies** table is refreshed every 30 seconds.

Note On a scaled setup with high node, policy, or interface counts, a timeout may occur during policy deployment. Please contact a Cisco representative to fine tune the timers involved.

Create Dynamic Path SR Policies

This task creates an SR policy with a dynamic path. SR-PCE computes a path for the policy based on metrics and path constraints (affinity or disjointness) defined by the user. A user can select from three available metrics to minimize in path computation: IGP, TE, or delay. SR-PCE may also automatically re-optimize the path as necessary based on topology changes.

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 From the **SR Policies** table, click **+ Create**.

Step 3 Enter the following SR policy values:

a) Required fields:

- **Headend**—Where the SR policy is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the SR policy.

- **Node Prefix**—After the endpoint is selected, the Node Prefix list is populated and you can select the loopback IP address.
- **Color**—A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headed and endpoint must have a unique color.
- **Path Name**—Enter a name for this SR policy path. SR policy paths from the same headend must be unique. Policy path names are not case sensitive.

b) Optional values:

- **Description**—Enter details or a description of this policy.
- **Explicit Binding SID**—The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated for each SR policy when the policy is instantiated. If you wish to use a specific segment ID, rather than the default one that is automatically assigned, then enter it here.
- **Profile ID**—Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.

Step 4 Under Tunnel Path, click **Dynamic Path**.

Step 5 Under Optimization Objective, select one of the following:

- **Interior Gateway Protocol (IGP) Metric**—Minimizes total path IGP metric.
- **Traffic Engineering (TE) Metric**—Minimize total path TE metric.
- **Latency**—Minimize total path latency.

Step 6 Define affinities:

Note Affinity constraints and disjointness cannot be configured on the same SR policy.

- **Exclude Any**—Does not traverse interfaces that have any of the specified affinities.
- **Include Any**—Includes only interfaces that have any of the specified affinities.
- **Include All**—Include only interfaces that have all of the specified affinities.
- **Select or Create Mapping**
  - If affinity mappings have been defined, select the applicable value.
  - To create an affinity mapping, click **Create Mapping**.

Note For more information, see Configure Affinity Mapping, on page 21.

- **Add Another**—Click this link to add more affinity rules.

Step 7 (Optional) Define disjointness. For more information on how Cisco Crosswork Optimization Engine handles disjoint policies and what options are supported, see the "Disjointness" section in Segment Routing Basics). Enter the disjoint group ID and subgroup ID. If there are existing SR policies belonging to a disjoint group that you define here, all SR policies that belong to that same disjoint group are shown during Preview.

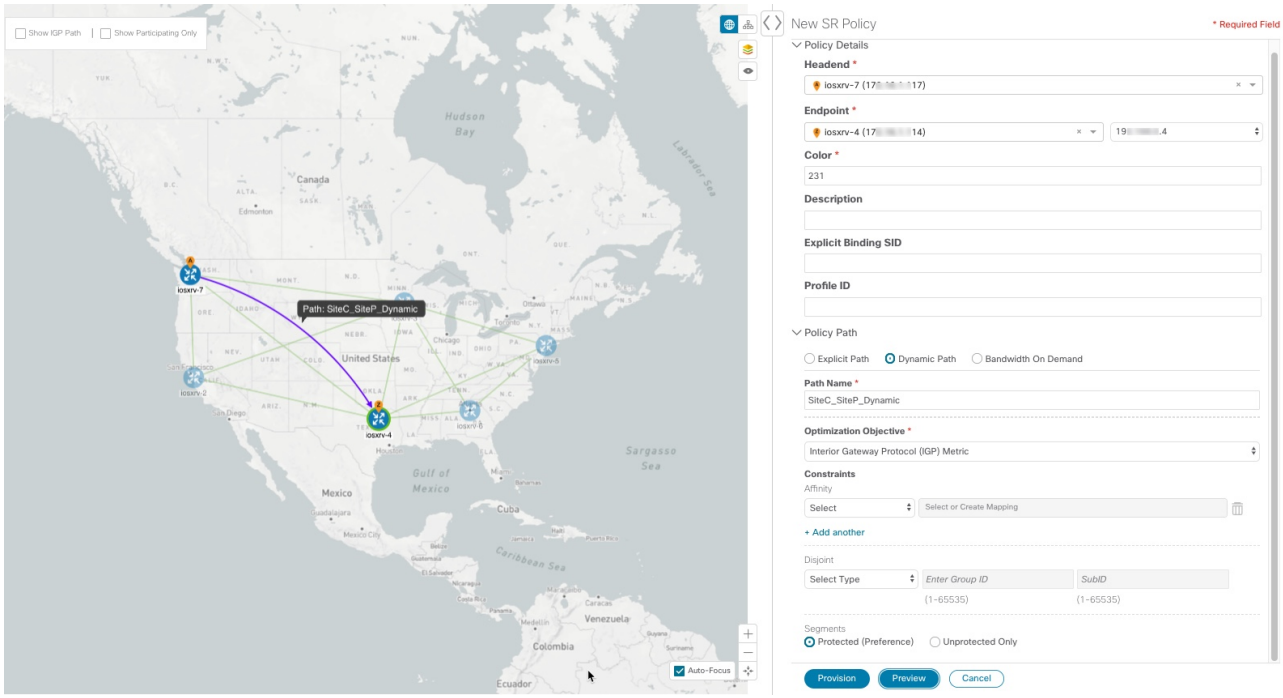
Note There cannot be more than two SR policies in the same disjoint group or subgroup.

Step 8 Under Segments, select one of the following:

- **Protected (Preference)**—Creates an SR policy that will use protected segments (provides a backup path) when available.
- **Unprotected Only**—Creates an SR policy that will only use unprotected segments. This option cannot be used when affinity constraints are defined.

Step 9 Click **Preview**. The path is highlighted on the map. Note in the following example that all policies belonging to the same disjoint group are displayed.

Figure 21: Dynamic SR Policy Preview



Step 10 If you are satisfied with the policy path, click **Provision**.

Step 11 When the policy is provisioned successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just created.
- **Create New**—Allows you to create another SR policy.

Modify SR Policies

To modify an SR policy:

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 Expand the **SR Policies** table. You will see a list of SR policies and various information such as headend, endpoint, Admin status, operating status, and so on.

Step 3 Locate the SR policy you are interested in and click ⋯ (under the **Actions** column). You may need to expand the SR Policies table to view the **Actions** column.

Step 4 From the top-right corner of the **SR Policy Details** window, click ⋯.

Note If the icon is grayed out, the tunnel cannot be modified for one of the following reasons:

- The policy was not created using the Crosswork Optimization Engine UI (**SR Policies** table > **Create**).
- The policy was created using the Bandwidth Optimization function pack.

Step 5 Click **Edit**.

Note For disjoint policies, the association type, group, and subgroup cannot be modified.

Step 6 In the **Policy Path** area, modify the values you want to change.

Step 7 (Optional) Click **Preview** to view visible updates on the topology map.

Step 8 Click **Update**.

Step 9 When the policy is updated successfully, a window appears with the following options:

- **View SR Policy List**—Displays the **SR Policies** table that lists all SR policies including the one that was just updated.
- **Create New**—Allows you to create a new SR policy.

Delete SR Policies

To delete an SR policy:

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 Expand the **SR Policies** table. You will see a list of SR policies and various information such as headend, endpoint, Admin status, operating status, and so on.

Step 3 Locate the policy you are interested in and click ⋯ (under the **Actions** column). You may need to expand the table to view the **Actions** column.

Step 4 From the top-right corner of the **SR Policy Details** window, click ⋯.

Note If the icon is grayed out, the tunnel cannot be modified for one of the following reasons:

- The policy was not created using the Crosswork Optimization Engine UI (**SR Policies** table > **Create**).
- The policy was created using the Bandwidth Optimization function pack.

Step 5 Click **Delete**.

Get More Information About an SR Policy

From the **SR Policies** table, locate the SR policy you are interested in and click ··· (under the **Actions** column). You may need to expand the **SR Policies** table to view the **Actions** column. The SR Policy Details window appears. It provides more detailed information about the policy and its associated paths. See the table below for field descriptions.

Figure 22: SR Policy Details

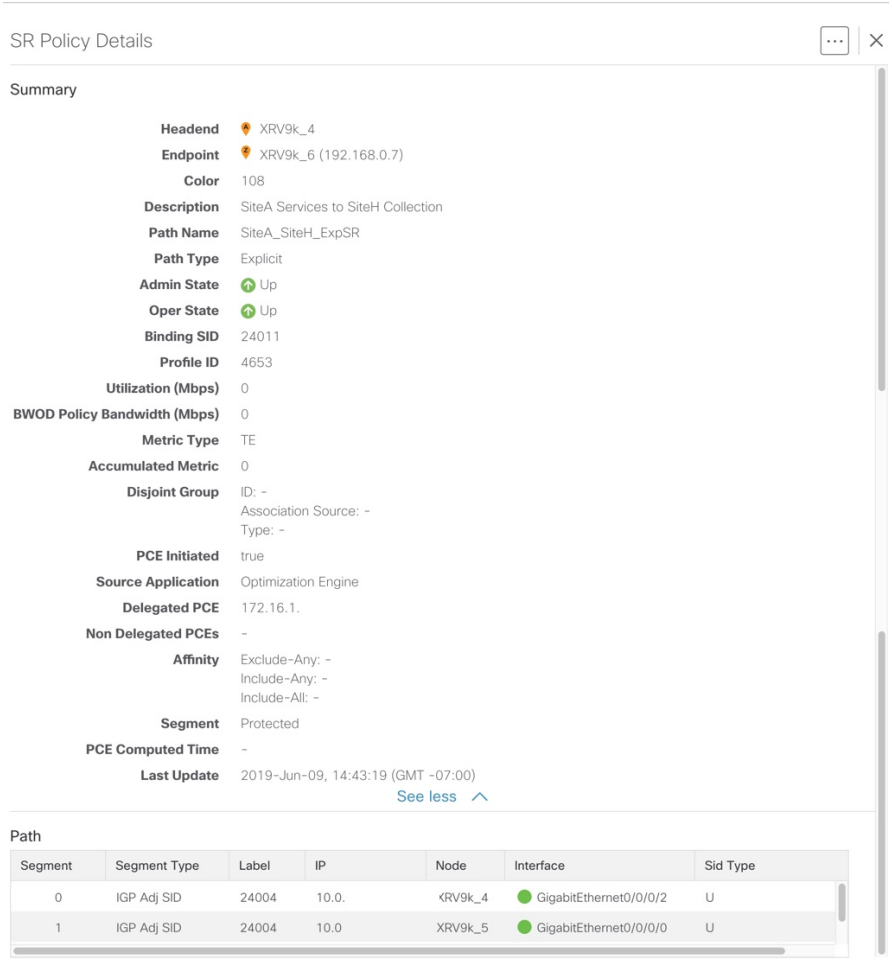


Table 5: SR Policy Details Fields

Field	Description
Headend	Where the SR policy is instantiated (source).
Endpoint	The destination of the SR policy.
Color	A numerical value that distinguishes between two or more policies to the same node pairs (Headend – Endpoint). Every SR policy between a given headend and endpoint must have a unique color.
Description	(Optional) If provisioned using the Cisco Crosswork Optimization Engine UI, it is the description entered by the user. This may be blank if the user did not enter a description.

Field	Description
Path Name	The name of the current active candidate path of the SR policy. For SR policies created using the Cisco Crosswork Optimization Engine UI, it will be the name provided by the user during configuration. For SR policies created through configuration on the headend router, the Path Name will be the base name configured for the policy on the CLI with "cfg_" appended to the beginning and the candidate path preference appended to the end.
Policy Type	Indicates whether an SR policy created through Cisco Crosswork Optimization Engine is explicit or dynamic.
Admin State	Administrative state is dictated by the user. For example, the user creates an SR policy and does not intentionally shut it down. The Admin State will be UP.
Oper State	Operational state received by the system. For example, the user has configured a policy and so the Admin State is UP. However, due to network issues it is operationally down. In this case, Oper State will display DOWN and Admin State will remain as UP.
Binding SID	The binding segment is a local segment identifying an SR policy. Each SR policy is associated with a binding segment ID (BSID). The BSID is a local label that is automatically allocated (or explicitly entered during manual provisioning) for each SR policy when the policy is instantiated.
Profile ID	Identification used to associate an SR policy with a set of features applied to the policy by the headend. It should correspond with a profile configured on the headend.
Utilization (Mbps)	The measured traffic on the SR policy.
BWOD Policy Bandwidth (Mbps)	The bandwidth constraint associated with a policy created through the Bandwidth on Demand function pack.
Metric Type	The metric type can be TE, IGP, or latency.
Accumulated Metric	Total metric calculation of the SR policy.
Disjoint Group	If applicable, displays disjointness information.
PCE Initiated	If the policy was initiated and provisioned by a PCE, the value is **True**.
Delegated PCE	The SR policy is delegated to this PCE IP address.
Non Delegated PCEs	PCEs reporting the policy, but not currently delegated.
Affinity	Lists any affinity constraints belonging to this policy.
Segment	Lists whether a dynamic path policy should prefer protected or require unprotected SIDs
PCE Computed Time	Time when PCE computed the path currently in effect.
Last Update	The last time the policy was updated.
Path	Lists segments that are part of the policy. It gives the following segment information: segment type, label, IP address, associated node, interface, and SID type (Protected or Unprotected).

Create and Manage RSVP-TE Tunnels

This section describes how to provision and manage RSVP-TE Tunnels using the Cisco Crosswork Optimization Engine UI. As you provision an RSVP-TE Tunnel, you can select nodes on the topology map and also preview the path before deployment. This greatly reduces the complexity of RSVP-TE Tunnel management.

Note Disjointness is supported for two policies with the same disjoint ID. When configuring disjoint RSVP-TE tunnels do the following:

- Use the same delegated SR-PCE for both RSVP-TE tunnels with the same association type, group and subgroup.
- Use the same headend with the same association type, group and subgroup.

Disjointness configuration may fail when the delegated PCE of an existing RSVP-TE tunnel is removed or unreachable. This can occur if Cisco Crosswork Optimization Engine is not aware that the PCE is down or missing and, instead, another PCE is used for configuration.

Create Explicit Path RSVP-TE Tunnels

This task creates an RSVP-TE tunnel using an explicit path (hops) that you define.

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering** and select the **RSVP-TE** tab.

Step 2 From the **RSVP-TE** table, click **+ Create**.

Step 3 Enter the following RSVP-TE Tunnel values:

a) Required fields (labeled with red asterisk):

- **Headend**—Where the RSVP-TE tunnel is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the RSVP-TE tunnel.
- **Path Name**—User specified name for the RSVP-TE tunnel.

Optional fields:

- **Description**—Details or a description of this TE tunnel.
- **Binding Label**—Numeric value of the binding label assigned to this tunnel. By default, the system will assign a value if the user does not enter one.
- **Signaled Bandwidth**—Required bandwidth.
- **Setup Priority**—The default value is 7. There are 8 (0 - 7) setup priorities. 0 is the most preferred. The setup priority is used to define preference for preempting less preferred tunnels. The most preferred tunnels can push the other less preferred tunnels out of the way.
- **Hold Priority**—The default value is 7. There are 8 (0 - 7) hold priorities. The holding priority is used to define a priority maintaining the currently established tunnel. You can have a tunnel that you never want go down, but

only establish it if there are plenty of resources. In that case you could configure the setup priority to be 7 and the holding priority to be 0. In this configuration, the tunnel will never get preempted once established.

- **Fast Reroute**—By default, Fast Re-route (FFR) is disabled. FFR provides fast traffic recovery when links fail.

Step 4 Under Tunnel Path, click **Explicit Path**.

Step 5 Add hops that will be part of the RSVP-TE tunnel.

a) Select a node from the drop-down node list.

b) Select the IP address from the **Select Interface** drop-down list. The drop-down list contains all available hops.

c) Select **Strict** as the type of hop. A strict path means that a network node and its preceding node in the ERO must be adjacent and directly connected. Each strict hop should be specified as a remote (ingress) interface or the Loopback IP (TE router ID) of the node.Crosswork Optimization Engine does not support configuration of loose hops in this release.

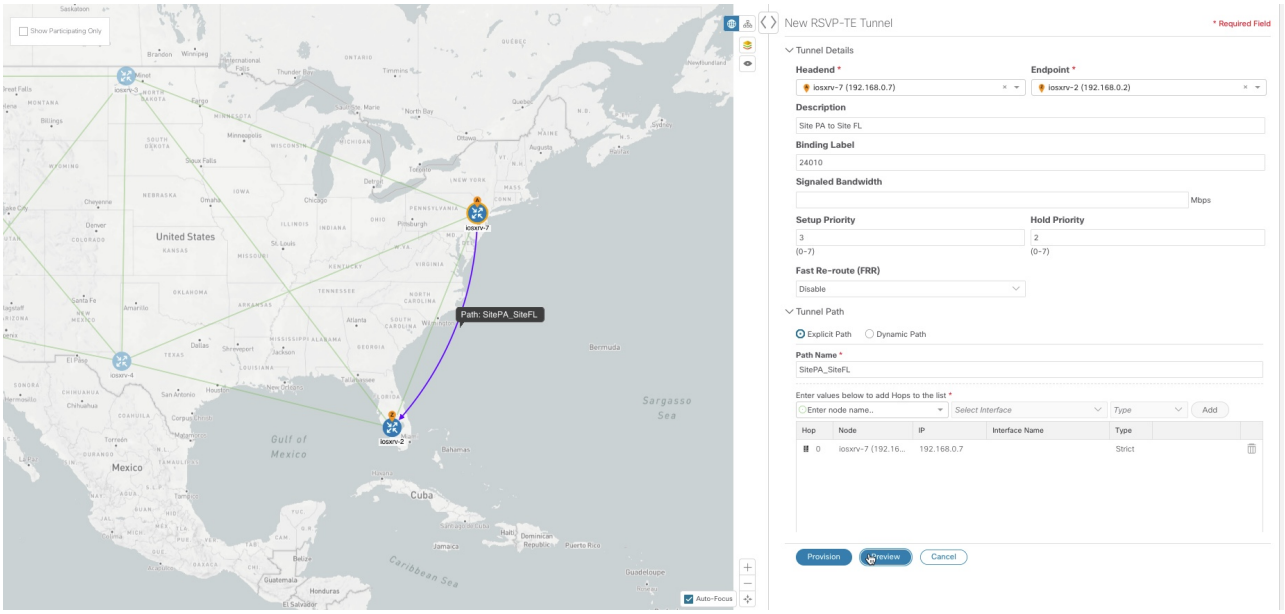
d) Click **Add**.

e) Repeat for each hop you want to add to the RSVP-TE tunnel. To reorder the hops, click and drag next to the hop you want to move.

Note The hops must be in order or the path will not be created.

Step 6 Click **Preview**. The path is highlighted on the map and policy details are displayed on the right. See the following figure to see a sample of RSVP-TE tunnel configuration details and a preview of the new tunnel.

Figure 23: Explicit RSVP-TE Tunnel Example



Step 7 If you are satisfied with the path, click **Provision**.

Step 8 When the RSVP-TE tunnel is provisioned successfully, a window appears with the following options:

- **View RSVP-TE List**—Displays the **RSVP-TE Tunnels** table that lists all RSVP-TE tunnels including the one that was just created.
- **Create New**—Allows you to create another TE tunnel.

Create Dynamic Path RSVP-TE Tunnels

This task creates an RSVP-TE tunnel with a dynamic path. SR-PCE computes a path for the tunnel based on metrics and path constraints (affinity or disjointness) defined by the user. A user can select from three available metrics to minimize in path computation: IGP, TE, or delay. SR-PCE may also automatically re-optimize the path as necessary based on topology changes.

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 From the **RSVP-TE Tunnel** table, click **+ Create**.

Step 3 Enter the following RSVP-TE Tunnel values:

a) Required fields (labeled with red asterisk):

- **Headend**—Where the RSVP-TE tunnel is instantiated. Note: You can either select a node (from the map or drop-down list) or enter part of the node name to filter the headend and endpoint node entries.
- **Endpoint**—The destination of the RSVP-TE tunnel.
- **Path Name**—User specified name for the RSVP-TE tunnel.

Optional fields:

- **Description**—Details or a description of this TE tunnel.
- **Binding Label**—Numeric value of the binding label assigned to this tunnel. By default, the system will assign a value if the user does not enter one.
- **Signaled Bandwidth**—Required bandwidth.
- **Setup Priority**—The default value is 7. There are 8 (0 - 7) setup priorities. 0 is the most preferred. The setup priority is used to define preference for preempting less preferred tunnels. The most preferred tunnels can push the other less preferred tunnels out of the way.
- **Hold Priority**—The default value is 7. There are 8 (0 - 7) hold priorities. The holding priority is used to define a priority maintaining the currently established tunnel. You can have a tunnel that you never want go down, but only establish it if there are plenty of resources. In that case you could configure the setup priority to be 7 and the holding priority to be 0. In this configuration, the tunnel will never get preempted once established.
- **Fast Reroute**—By default, Fast Re-route (FFR) is disabled. FFR provides fast traffic recovery when links fail.

Step 4 Under Tunnel Path, click **Dynamic Path**.

Step 5 Under Optimization Objective, select one of the following:

- **Interior Gateway Protocol (IGP) Metric**—Minimizes total path IGP metric.
- **Traffic Engineering (TE) Metric**—Minimize total path TE metric.
- **Latency**—Minimize total path latency.

Step 6 Define affinities:

Note Affinity constraints and disjointness cannot be configured on the same tunnel.

- **Exclude Any**—Does not traverse interfaces that have any of the specified affinities.
- **Include Any**—Includes only interfaces that have any of the specified affinities.
- **Include All**—Include only interfaces that have all of the specified affinities.
- **Select or Create Mapping**
  - If affinity mappings have been defined, select the applicable value.
  - To create an affinity mapping, click **Create Mapping**.

Note For more information, see Configure Affinity Mapping, on page 21.

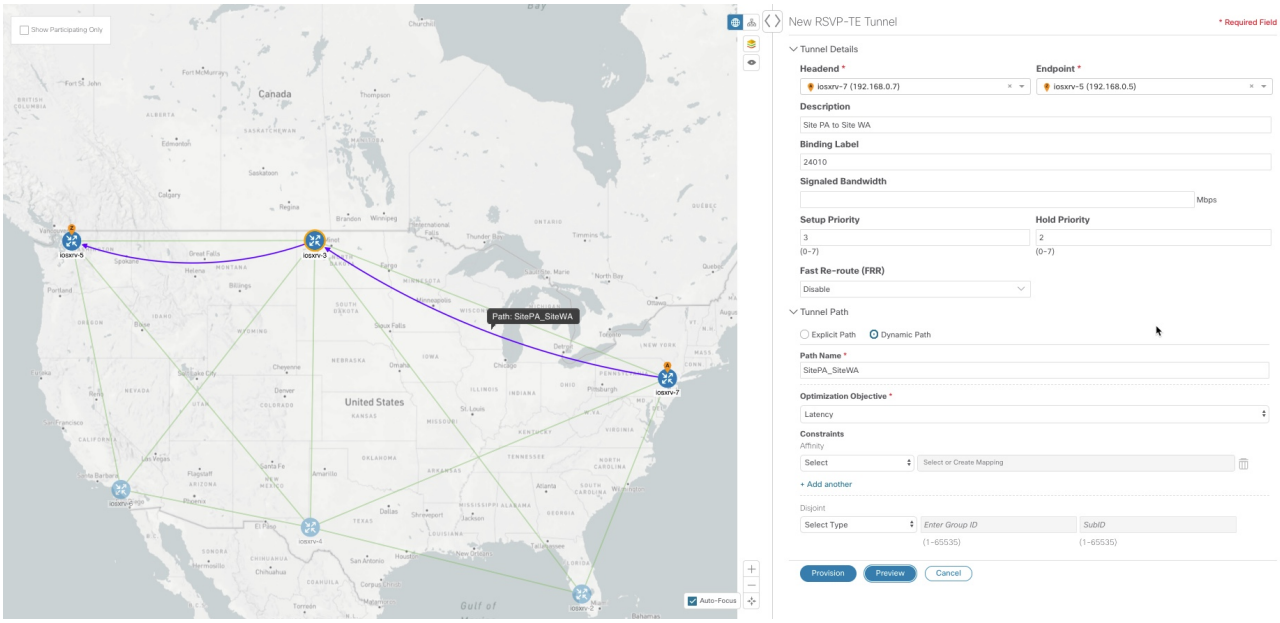
- **Add Another**—Click this link to add more affinity rules.

Step 7 (Optional) Define disjointness. For more information on how Cisco Crosswork Optimization Engine handles disjoint tunnels and what options are supported, see the "Disjointness" section in Segment Routing Basics (applies to RSVP-TE tunnels as well). Enter the disjoint group ID and subgroup ID. If there are existing tunnels belonging to a disjoint group that you define here, all tunnels that belong to that same disjoint group are shown during Preview.

Note There cannot be more than two TE tunnels in the same disjoint group or subgroup.

Step 8 Click **Preview**. The path is highlighted on the map. See the following figure to see a sample of RSVP-TE tunnel configuration details and a preview of the new tunnel.

Figure 24: Dynamic RSVP-TE Tunnel Preview



Step 9 If you are satisfied with the tunnel path, click **Provision**.

Step 10 When the tunnel is provisioned successfully, a window appears with the following options:

- **View RSVP List**—Displays the **RSVP-TE Tunnels** table that lists all RSVP-TE tunnels including the one that was just created.
- **Create New**—Allows you to create a new RSVP-TE tunnel.

Modify RSVP-TE Tunnels

To modify an RSVP-TE tunnel:

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 Expand the **RSVP-TE Tunnels** table. You will see a list of RSVP-TE tunnels and various information such as headend, endpoint, Admin status, operating status, and so on.

Step 3 Locate the RSVP-TE tunnel you are interested in and click ⋯ (under the **Actions** column). You may need to expand the table to view the **Actions** column.

Step 4 From the top-right corner of the **RSVP-TE Tunnel Details** window, click ⋯.

Note If the icon is grayed out, the policy cannot be modified because the policy was not created using the Crosswork Optimization Engine UI (**RSVP-TE Tunnel** table **> + Create** button).

Step 5 Click **Edit**.

Step 6 Modify the values you want to change.

Note For disjoint RSVP-TE tunnels, the association type, group, and subgroup cannot be modified.

Step 7 (Optional) Click **Preview** to view visible updates on the topology map.

Step 8 Click **Update**.

Step 9 When the tunnel is updated successfully, a window appears with the following options:

- **View RSVP List**—Displays the **RSVP-TE Tunnels** table that lists all RSVP-TE tunnels including the one that was just updated.
- **Create New**—Allows you to create a new RSVP-TE tunnel.

Delete RSVP-TE Tunnels

To delete an RSVP-TE tunnel:

Step 1 From the main menu, choose **Optimization Engine** > **Traffic Engineering**.

Step 2 Expand the **RSVP-TE Tunnels** table. You will see a list of RSVP-TE tunnels and various information such as headend, endpoint, Admin status, operating status, and so on.

Step 3 Locate the RSVP-TE tunnel you are interested in and click ⋯ (under the **Actions** column). You may need to expand the table to view the **Actions** column.

Step 4 From the top-right corner of the **RSVP-TE Tunnel Details** window, click ⋯.

Note If the icon is grayed out, the policy cannot be deleted because the tunnel was not created using the Crosswork Optimization Engine UI (**RSVP-TE Tunnel** table > **+ Create** button) or if it was created from another Crosswork Optimization Engine VM that knows of the same topology.

Step 5 Click **Delete**.

Get More Information About an RSVP-TE Tunnel

From the **RSVP-TE Tunnel** table, locate the TE tunnel you are interested in and click the ⋯ link (under the **Actions** column). You may need to expand the **RSVP-TE Tunnel** table to view the **Actions** column. The RSVP-TE Tunnel Details window appears, where you can view more detailed information about the TE tunnel and its associated paths. See the following table for field descriptions.

Figure 25: RSVP-TE Tunnel Details

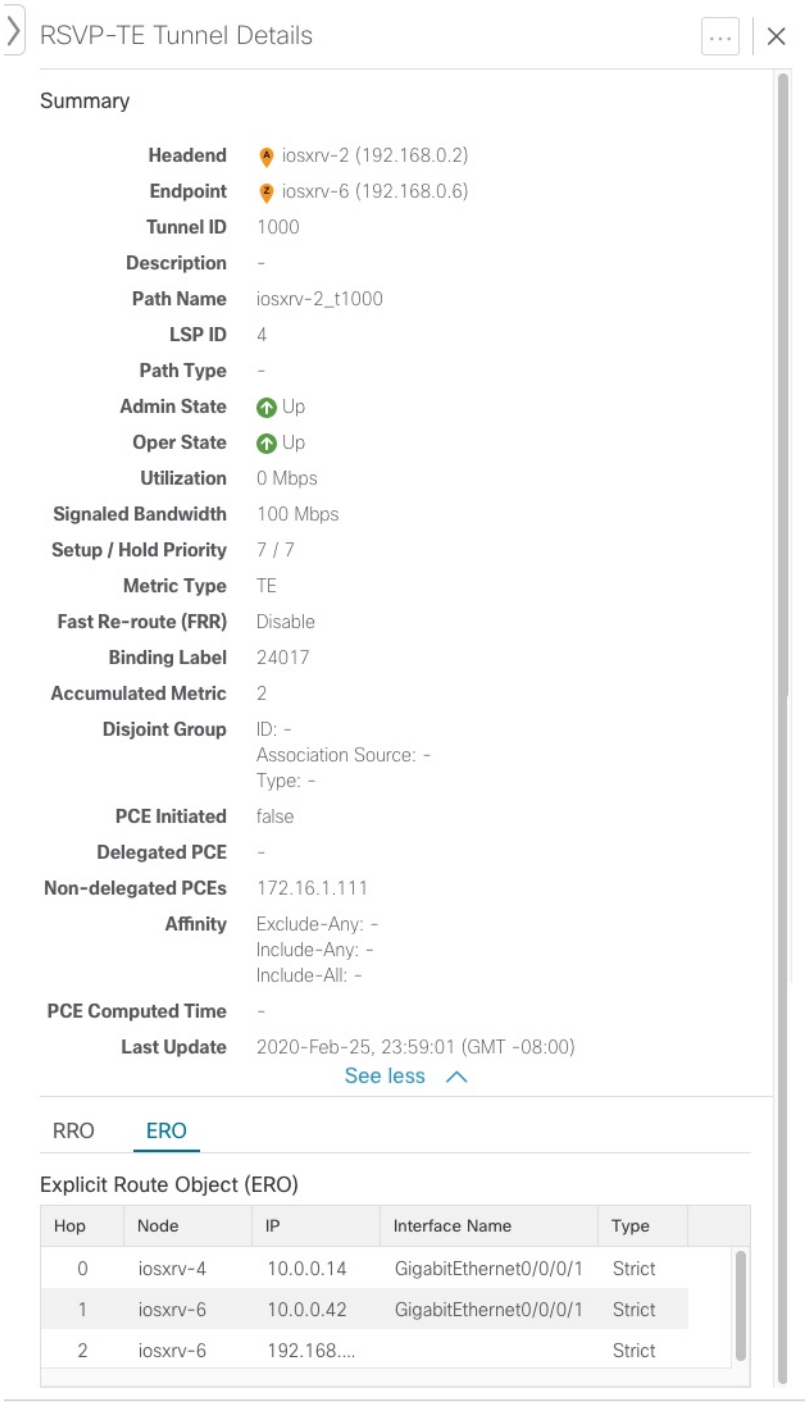


Table 6: RSVP-TE Tunnels

Field	Description
Headend	Where the RSVP-TE tunnel is instantiated.
Endpoint	The destination of the RSVP-TE tunnel.
Tunnel ID	Assigned RSVP-TE tunnel ID.
Path Name	For RSVP-TE tunnels created using the Cisco Crosswork Optimization Engine UI, it will be the name provided by the user during configuration. For RSVP-TE tunnels created through configuration on the headend router, the Path Name for Cisco PCCs will be an auto-generated string consisting of the node name as well as the Tunnel ID.
LSP ID	The LSP identification number.
Path Type	Indicates whether the TE tunnel created through Cisco Crosswork Optimization Engine is explicit or dynamic.
Admin State	Administrative status of the RSVP-TE tunnel. This is the status defined by the user.
Oper State	Operational status of the RSVP-TE tunnel. This is the state of the policy as reported by the system. For example, the user can define the Admin status as Up. However, if the policy is operationally down due to some network issues, then the Oper Status will display as Down.
Utilization	Tunnel's utilization against bandwidth.
Signaled Bandwidth	Bandwidth requirements.
Setup / Hold Priority	There are 8 (0 - 7) setup priorities. 0 is the most preferred. The setup priority is used to define preference for preempting less preferred tunnels. The most preferred tunnels can push the other less preferred tunnels out of the way. There are 8 (0 - 7) hold priorities. The holding priority is used to define a priority maintaining the currently established tunnel. You can have a tunnel that you never want go down, but only establish it if there are plenty of resources. In that case you could configure the setup priority to be 7 and the holding priority to be 0. In this configuration, the tunnel will never get preempted once established.
Metric Type	Type of metric (IGP, TE, or Delay).

Field	Description
Fast Re-route (FRR)	The value is **Enable** if Fast Reroute is enabled.
Binding Label	Defined binding SID label.
Accumulated Metric	Total metric calculation of the RSVP-TE tunnel.
Disjoint Group	If applicable, the disjoint group details the RSVP-TE tunnel belongs in.
PCE Initiated	If the RSVP-TE tunnel was initiated and provisioned by a PCE, the value is **true**. If it is PCC-initiated, the value is **false**.
Delegated PCE	If applicable, the RSVP-TE tunnel is delegated to this PCE IP address.
Non-delegated PCE	PCEs reporting the RSVP-TE tunnel, but not currently delegated.
Affinity	Lists any affinity constraints belonging to this TE tunnel.
PCE Computed Time	Time when PCE computed the path currently in effect.
Last Update	The last time the policy was updated.
Explicit Route Object (ERO)	Lists hop EROs that are part of the tunnel. It gives the following information: node, IP address, interface, and type (strict or loose). **Note** When the ERO tab is selected, the topology map displays the paths as curved lines. If both RRO and ERO paths are available, the RRO path is displayed by default.
Record Route Object (RRO)	Lists hop RROs that are part of the tunnel. It gives the following information: node, IP address, and interface. **Note** When the RRO tab is selected, the topology map displays the paths as straight lines. If both RRO and ERO paths are available, the RRO path is displayed by default.