SR-MPLS and SRv6

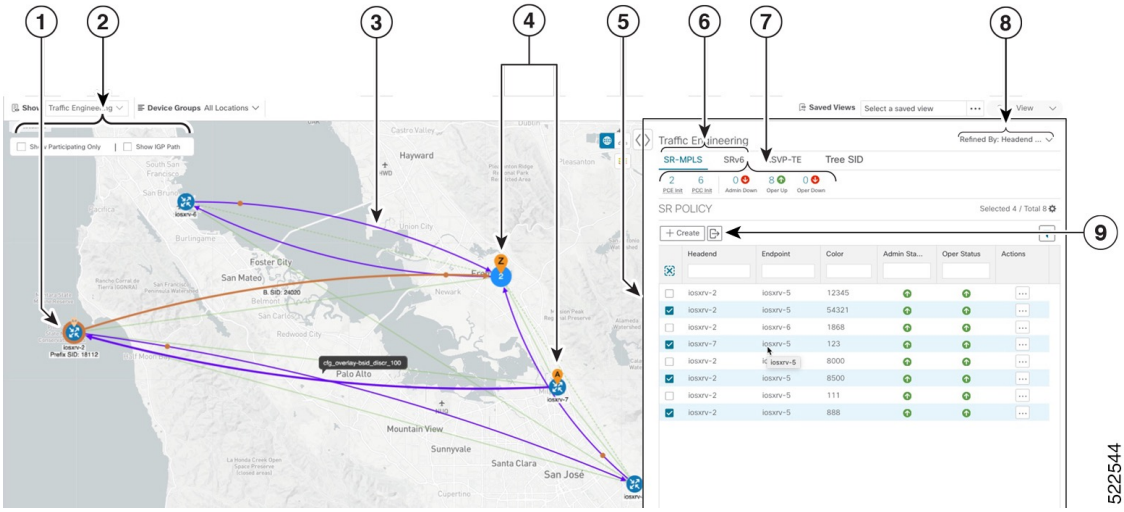
This section describes the SR-MPLS and SRv6 policy features that Crosswork Optimization Engine supports. For a list of known limitations and important notes, see the Cisco Crosswork Optimization Engine Release Notes Cisco Crosswork Network Controller Release Notes.

View SR-MPLS and SRv6 Policies on the Topology Map

Crosswork Optimization Engine visualization provides the most value by giving you the ability to easily view and manage SR-MPLS and SRv6 policies. By visually examining your network, the complexity of provisioning and managing these SR-TE policies is significantly reduced.

To get to the Traffic Engineering topology map, choose **Traffic Engineering** > **Traffic Engineering** > **Traffic Engineering**..

Figure 1: Traffic Engineering UI : SR-MPLS and SRv6 Policies



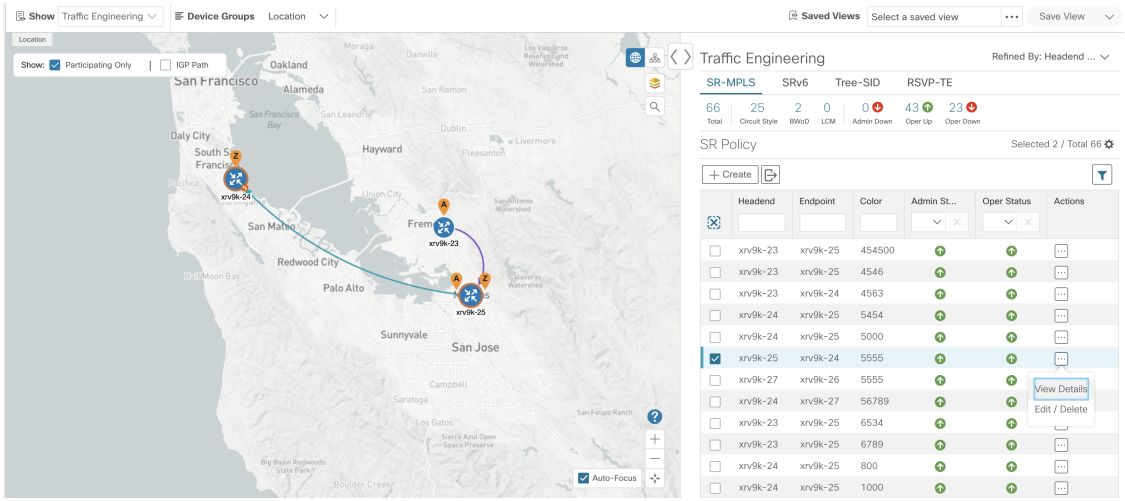
Callout No.	Description
1	A device with an orange ( ) outline indicates there is a node SID associated with that device or a device in the cluster.
2	Click the appropriate check box to enable the following options: • **Show IGP Path**—Displays the IGP path for the selected SR-TE policy. • **Show Participating Only**—Displays only links that belong to selected SR-TE policy. All other links and devices disappear.
3	When SR-TE policies are selected in the SR-MPLS or SRv6 tables, they show as purple directional lines on the map indicating source and destination. An adjacency segment ID (SID) is shown as an orange circle on a link along the path ( ).
4	**SR-MPLS and SRv6 Policy 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-TE policy that originates from a node. The **Z+** denotes that the node is a destination for more than one SR policy.
5	The content of this window depends on what has been selected or filtered. In this example, the SR-MPLS tab is selected and the SR Policy table is displayed.
6	Click on either the **SR-MPLS** or **SRv6** tabs to view the respective list of SR-TE policies.
7	The **Mini Dashboard** provides a summary of the operational SR-MPLS or SRv6 policy status. If filters are applied, the **Mini Dashboard** is updated to reflect what is displayed in the SR Policy and SRv6 Policy tables. In addition to the policy status, the **SR-MPLS Mini Dashboard** table displays the number of PCC and PCE initiated tunnels that are *currently* listed in the SR Policy table.

Callout No.	Description
8	This option allows you to choose how the group filter (when in use) should be applied on the table data. For example, if **Headend only** was selected, then it would only display policies where the headend device of the policy is in the selected group. This filter allows you to see specific configurations and is useful when you have a large network. Filter options: • **Headend or Endpoint**—Show policies with either the headend or endpoint device in the selected group. • **Headend and Endpoint**—Show policies if both the headend and endpoint are in the group. • **Headend only**—Show policies if the headend device of the policy is in the selected group. • **Endpoint only**—Show policies if endpoint device of the policy is in the selected group.
9	Exports *all* data into a CSV file. You cannot export selected or filtered data.

View SR-MPLS and SRv6 Policy Details

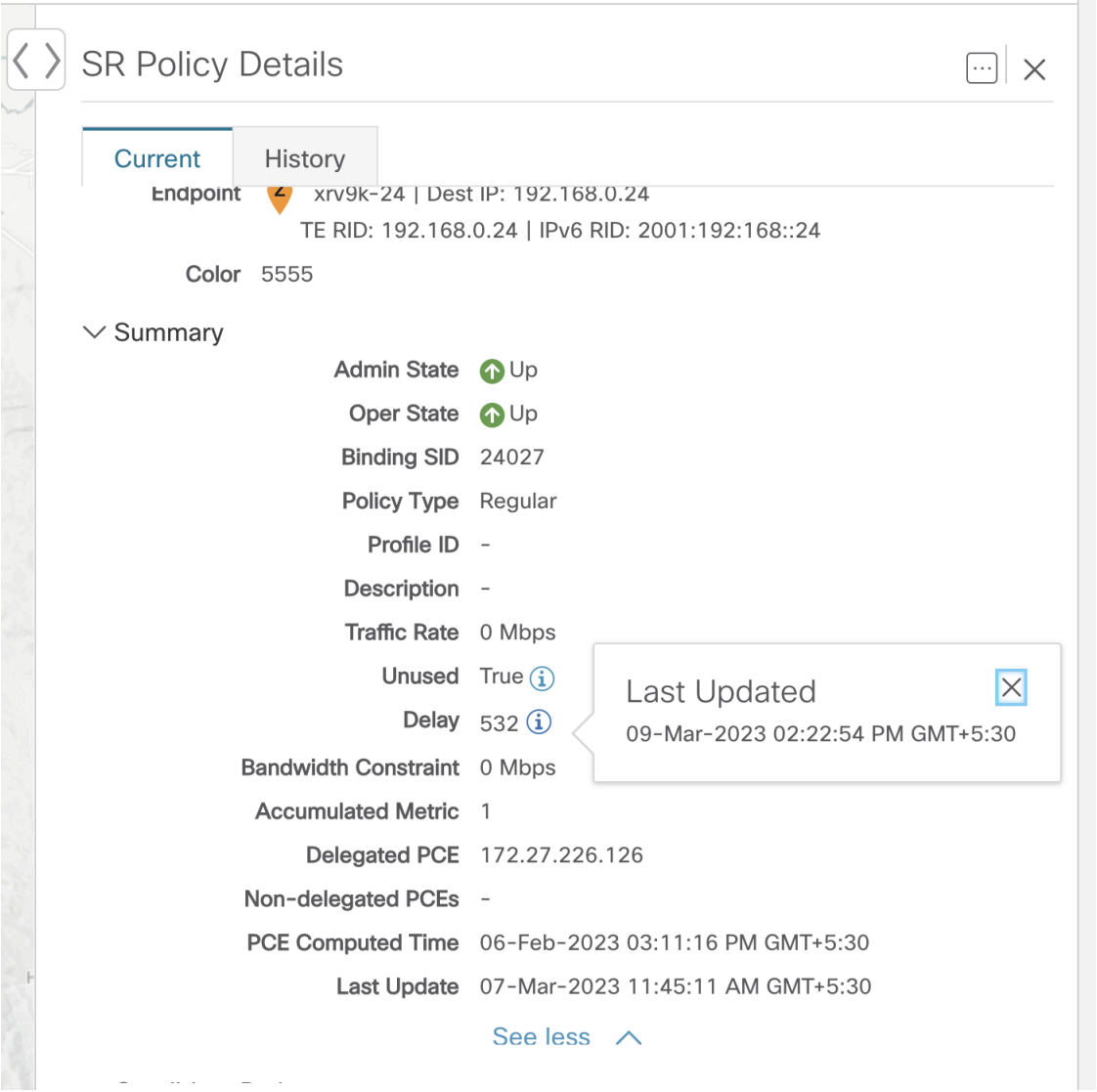
View SR-MPLS or SRv6 TE policy level details as well segment lists and any path computation constraints configured on a per-candidate path basis.

Step 1 From the **Actions** column, click ⋯ > **View Details** for one of the SR-MPLS or SRv6 policies.



Step 2 View SR-MPLS or SRv6 policy details.

Note The Delay value is calculated for all policies every 10 minutes. Hover your mouse over the "i" icon (next to the Delay value) to view the last time the value was updated.



Visualize SR-MPLS or SRv6 Policies Example

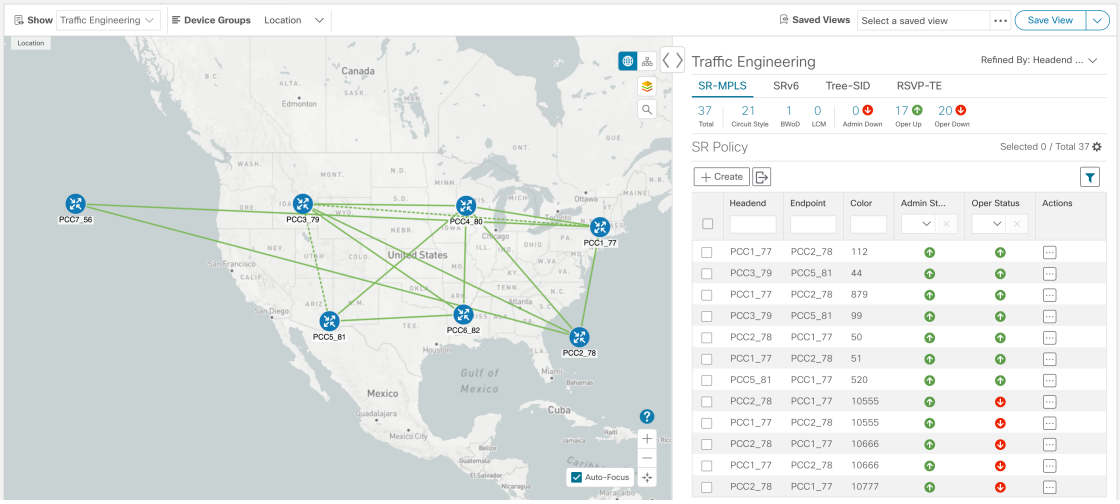
This example walks you through several SR-TE (SR-MPLS and SRv6) policy visualization features that are available from the topology map.

In this example, we assume that devices and SR-MPLS policies have been added and device groups have been created.

Note Although this example uses SR-MPLS policies, the basic functionality of the maps for both SR-MPLS policies and SRv6 policies is the same.

Click images to zoom in for a closer look.

Figure 2: Topology Map Example



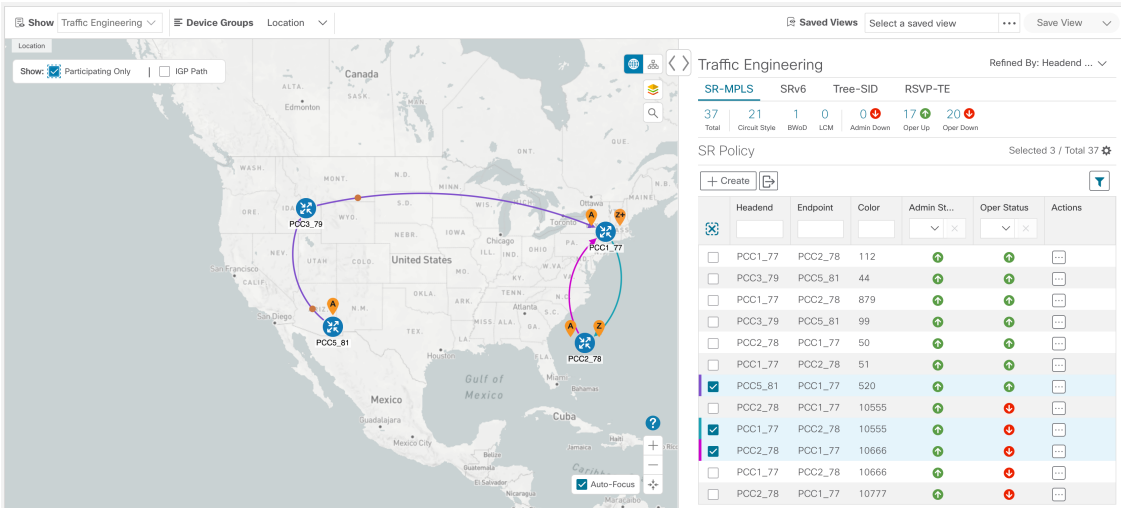
Step 1 Select SR-MPLS policies for visualization and isolate them on the map.

a) From the main menu, choose **Traffic Engineering** > **Traffic Engineering**.

b) From the **SR Policy** table, check the check box next to the SR-MPLS policies you are interested in.

c) Check the check box next to **Show Participating Only** so that other links and devices that are not part of the selected SR-TE policies are hidden.
In the following example, the topology map displays the following:

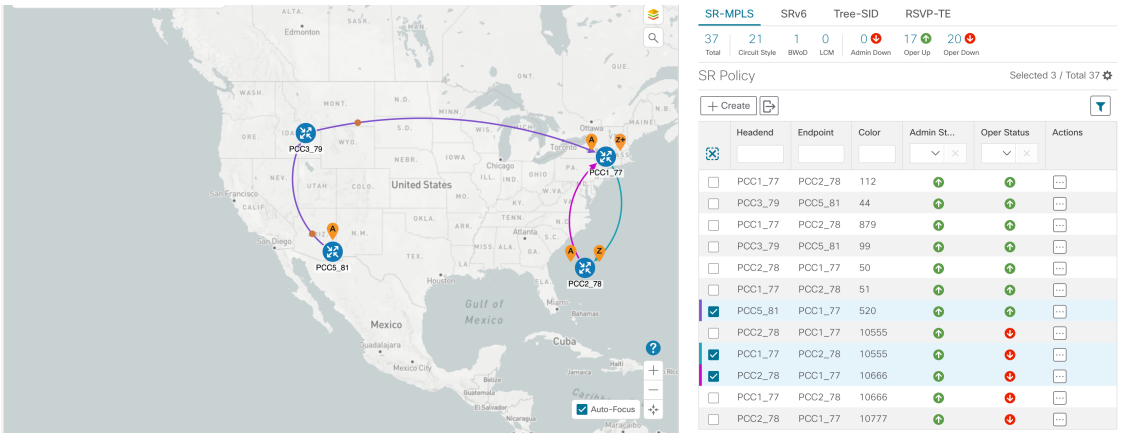
- Four SR-MPLS policies are selected.
- SR-MPLS policies appear as purple links with arrows that indicate the path direction.
- The **PCC1_77** node is the destination for two of the selected policies. Both **PCC5_81** and **PCC3_79** are destinations for the selected policies. SR-MPLS policy origin 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+** denotes that the device is a destination for more than one policy.



Step 2 Highlight and view more details for a particular SR-MPLS policy.

a) From the **SR Policy** table, *hover* over a selected policy.
The topology map displays the following details:

- The path is emphasized on the map. The path goes through **PCC5_81 > PCC3_79 > PCC1_77** .
- The prefix SID for PCC3_79 and PCC1_77 is displayed.



Step 3 View the physical path and metrics between the endpoints of the selected SR-MPLS policies.

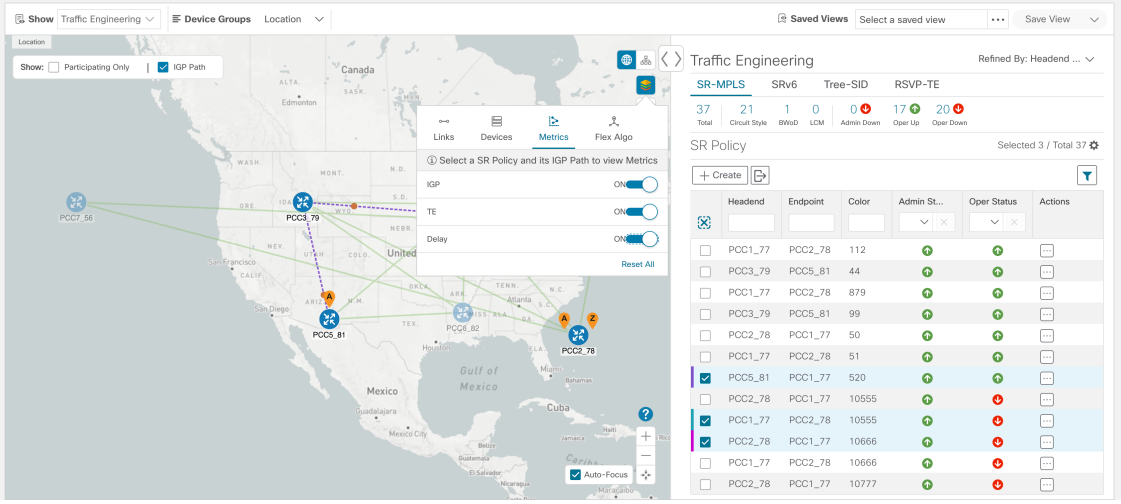
a) Check the **Show IGP Path** check box. The IGP paths for the selected SR-MPLS policies are displayed, with straight lines, instead of the segment hops.

b) Click .

c) Click the **Metrics** tab.

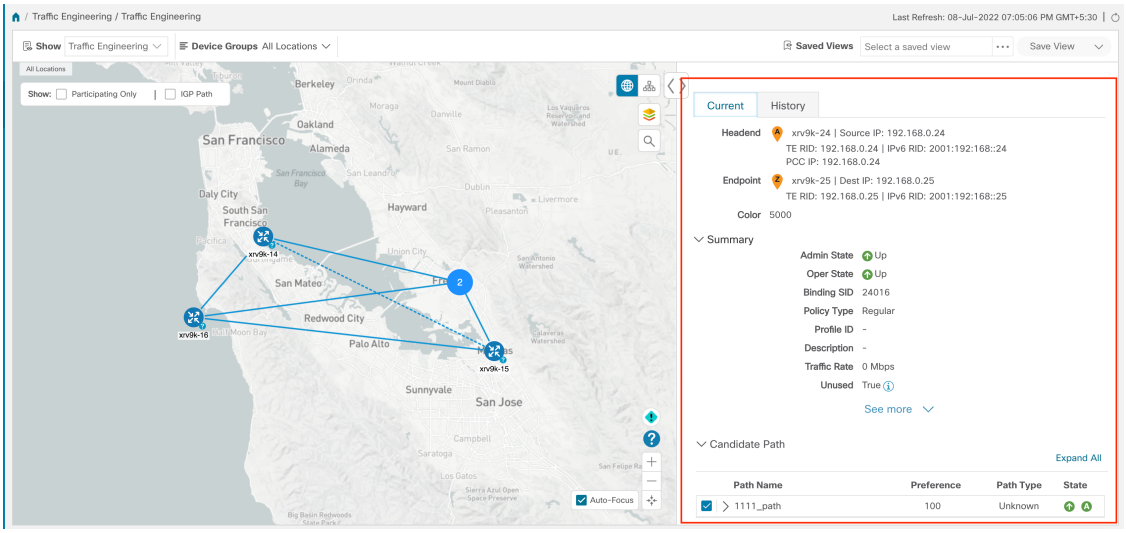
d) Toggle applicable metrics to **ON**.

Note You must check the **Show IGP Path** check box in order to view metrics.



Step 4 View SR-MPLS policy details such as disjoint groups, metric type, segment hop information, delay (calculated for all policies every 10 minutes), and so on.

a) From the **Actions** column, click ⋯ > **View Details** for one of the SR-MPLS policies.
The **SR Policy Details** window is displayed in the side panel. Note that only the selected policy is displayed on the topology map.

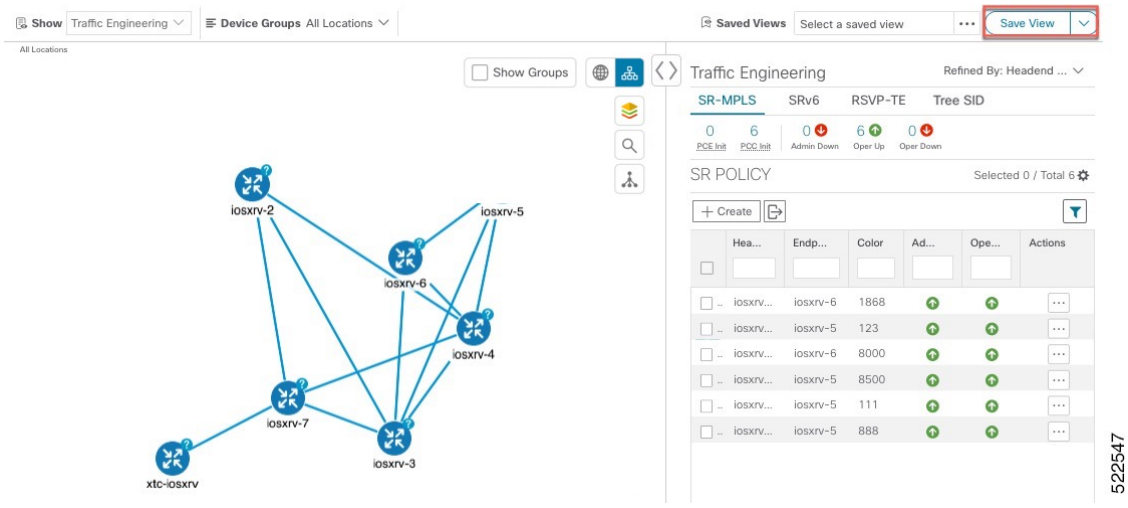


Step 5 Customize and save a logical view of the topology.

a) Click ⚯ to display the logical view of selected SR-MPLS policies.
b) Arrange the nodes to your preference.
c) To save the topology layout (*not SR-MPLS policy selection*), clear all selected SR-MPLS policies, and click **Save View**.

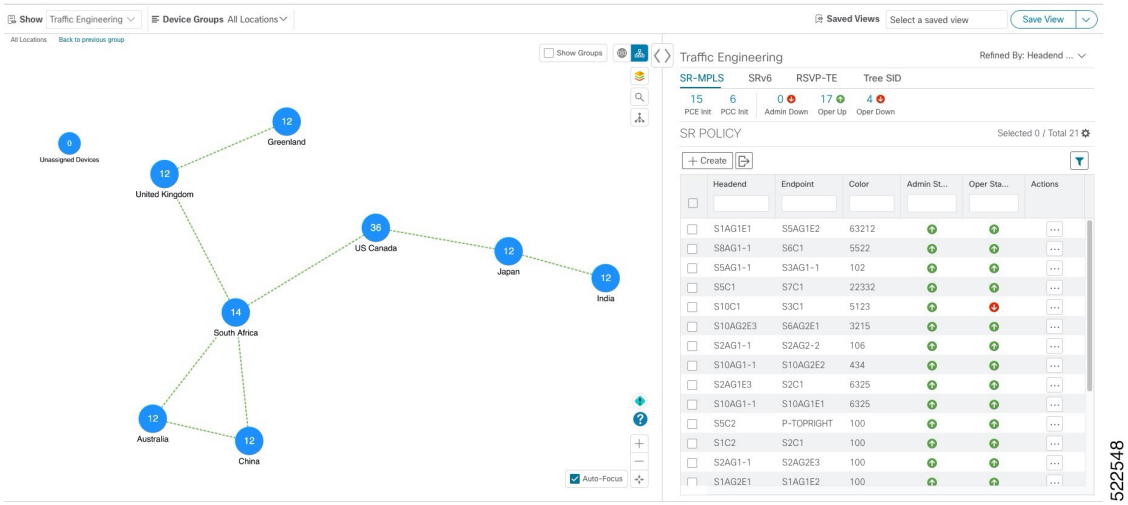
Example:

Figure 3: Logical Map (Save Without SR-MPLS Policies Selected)

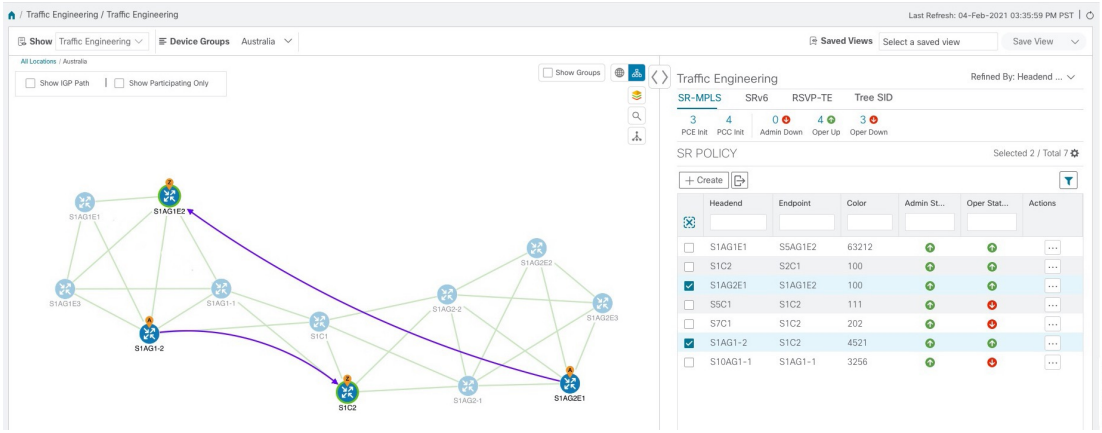


Step 6 Close (⨉) the current view to return to the **SR Policy** table.

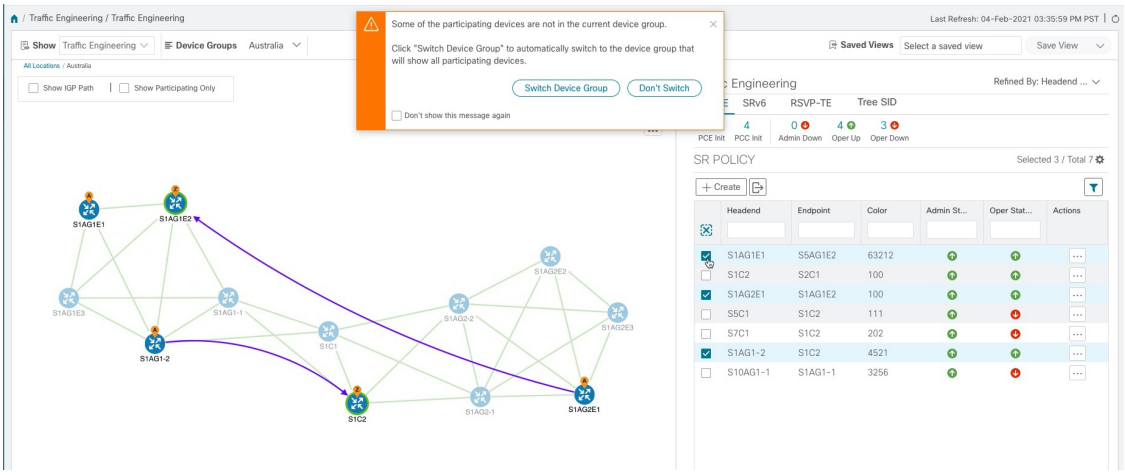
Step 7 To understand how device groups are displayed with the selection of SR-MPLS policies, uncheck any SR-MPLS policies that might be selected and check **Show Groups**.



Step 8 Selecting a specific group from the **Device Groups** drop-down list, will only display that group in the map. In this example, **Australia** is selected and the associated SR-MPLS policy is selected and displayed.

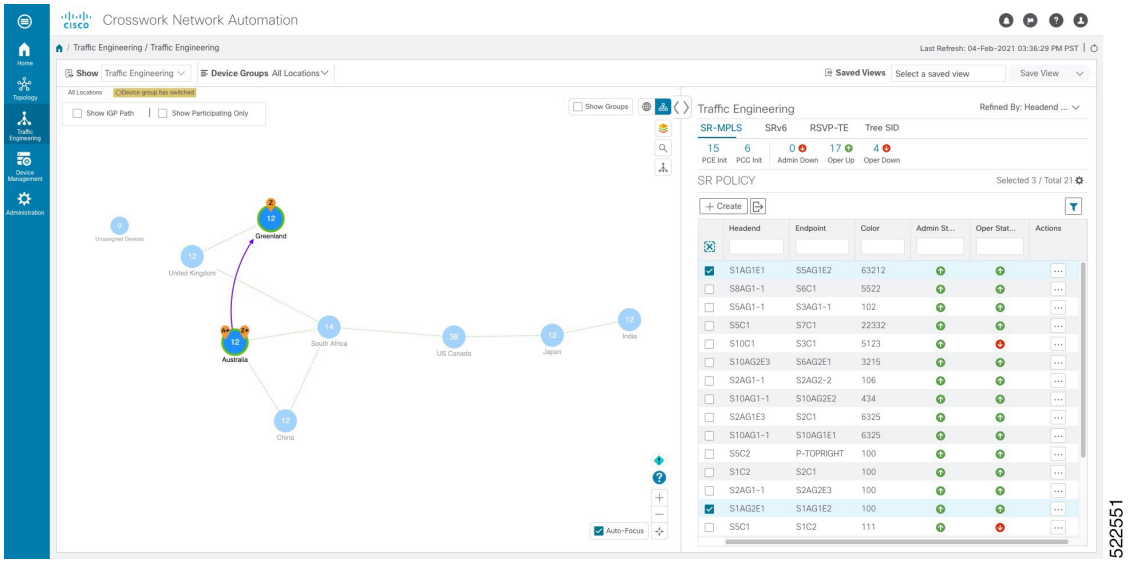


Step 9 If you select a policy where participating devices are not part of the selected group, then a dialog appears giving you an option to switch the group view. This is the default behavior. If this window does not appear, then the administrator has configured the display to automatically switch view or stay in the current view. For more information, see Configure How Device Groups Are Displayed for Traffic Engineering.



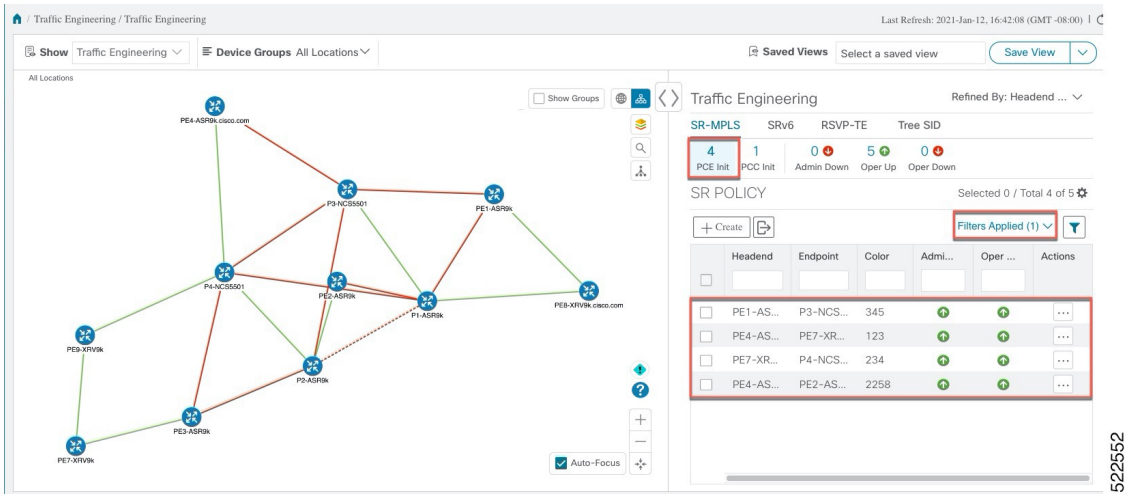
Step 10 If you select **Switch Device Group**, then the group will change and you will see all participating devices for the SR-MPLS policies you have selected.

To go back to the previous group view, click **Back** (this link appears later in the yellow text area indicated in the following figure).



Step 11 You can also use the Mini Dashboard to drill down and focus on certain SR-TE policies.

To filter the SR Policy table to show only PCE-initiated policies, click the value for PCE Init from the SR-MPLS Mini Dashboard. Note that the **Filters Applied** text appears.



Step 12 To remove filter criteria, click **Filters Applied** > **Clear All Filters**. You can also select individual filters if more than one filter has been applied.

Find Multiple Candidate Paths (MCPs)

Visualizing MCPs gives you insight into which paths might be a better alternative to the currently active one. If you determine to do so, you can then manually configure the device and change which path becomes active.

Important Notes

- Only PCC-initialized SR-TE policies with MCPs are supported.
- Crosswork Optimization Engine does not distinguish dynamic paths versus explicit paths. The Policy Type field value displays as 'Unknown'.
- You can view active explicit paths, but not inactive candidate explicit paths in the UI.

Before you begin

A policy must be configured with MCPs on devices before visualizing them on the Traffic Engineering topology map. This configuration can be done manually or within Crosswork Network Controller.

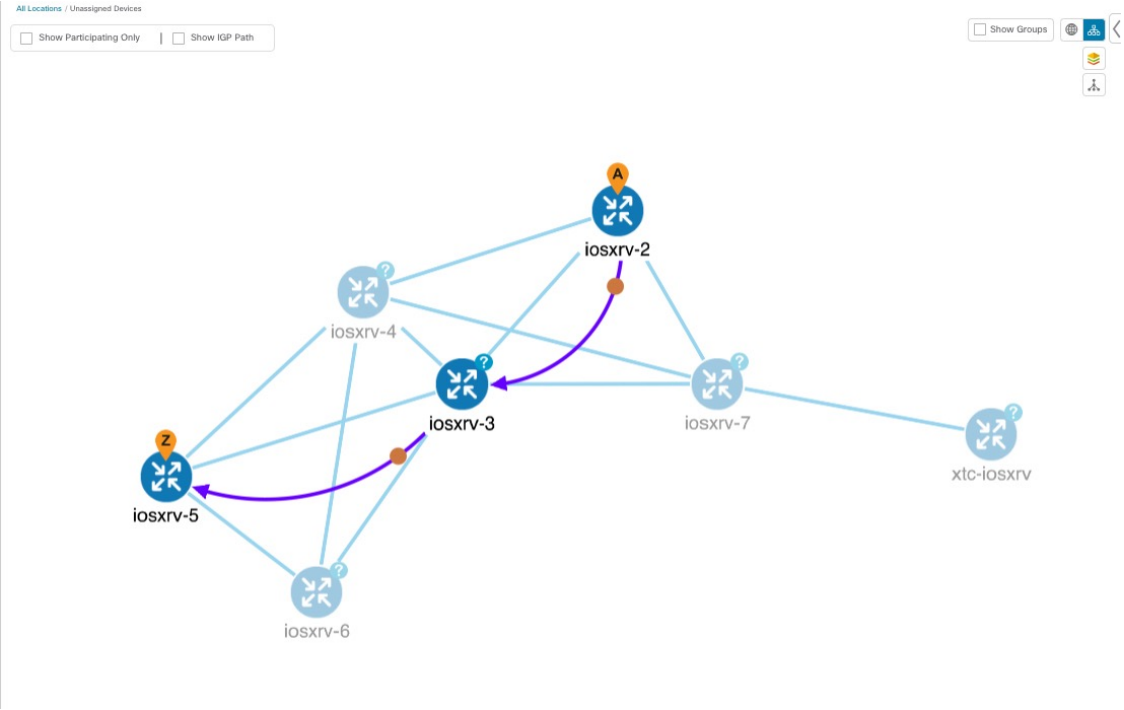
Step 1 From the main menu, choose **Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** or **SRv6** tab.

Step 2 Navigate to the active SR-TE policy that has MCPs configured and view it on the topology map.

a) Check the check box next to the SR-TE policy that has MCPs configured.

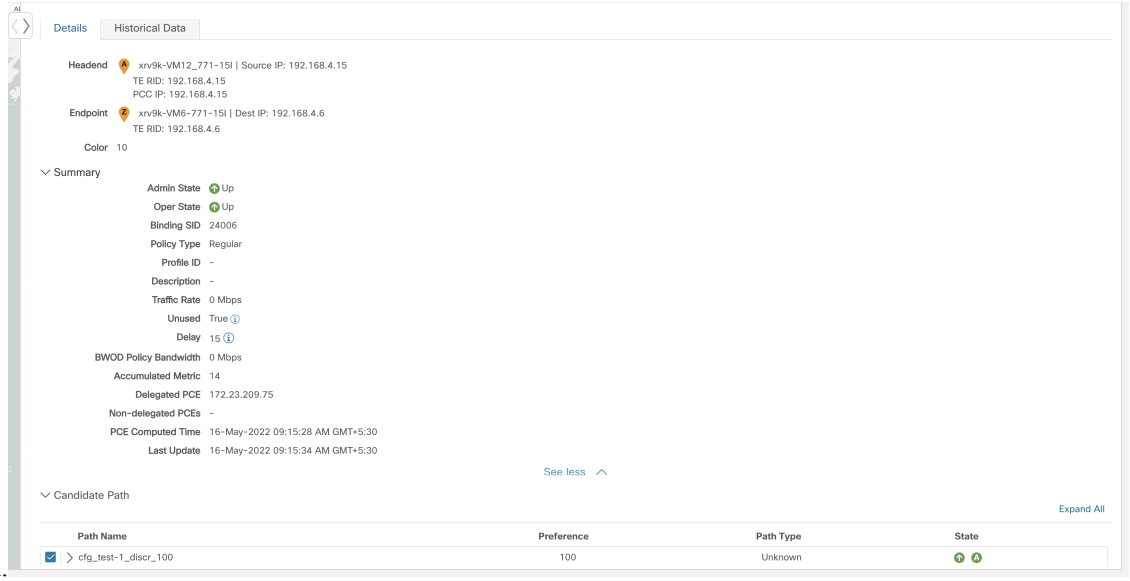
b) View the SR-TE policy that is highlighted on the topology map.

In this example, you see that the active path is going from **iosxrv-2 > iosxrv-3 > iosxrv-5**.



Step 3 View the list of candidate paths.

a) From the SR-TE Policy table **Actions** column, click ... > **View Details**. A list of candidate paths appear along with policy details in the **SR Policy Details** window. The green A in the state column indicates the active path.

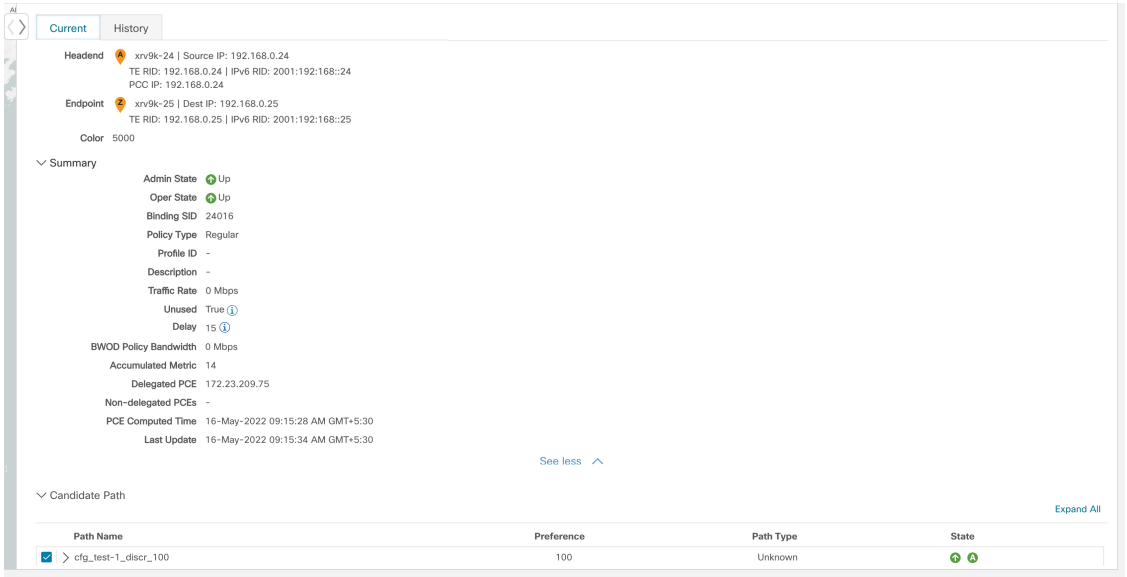


Step 4 You can expand individual paths or click **Expand All** to view details of each path. As you hover each segment, the segment is highlighted on the map.

Step 5 Visualize the candidate path on the topology map.

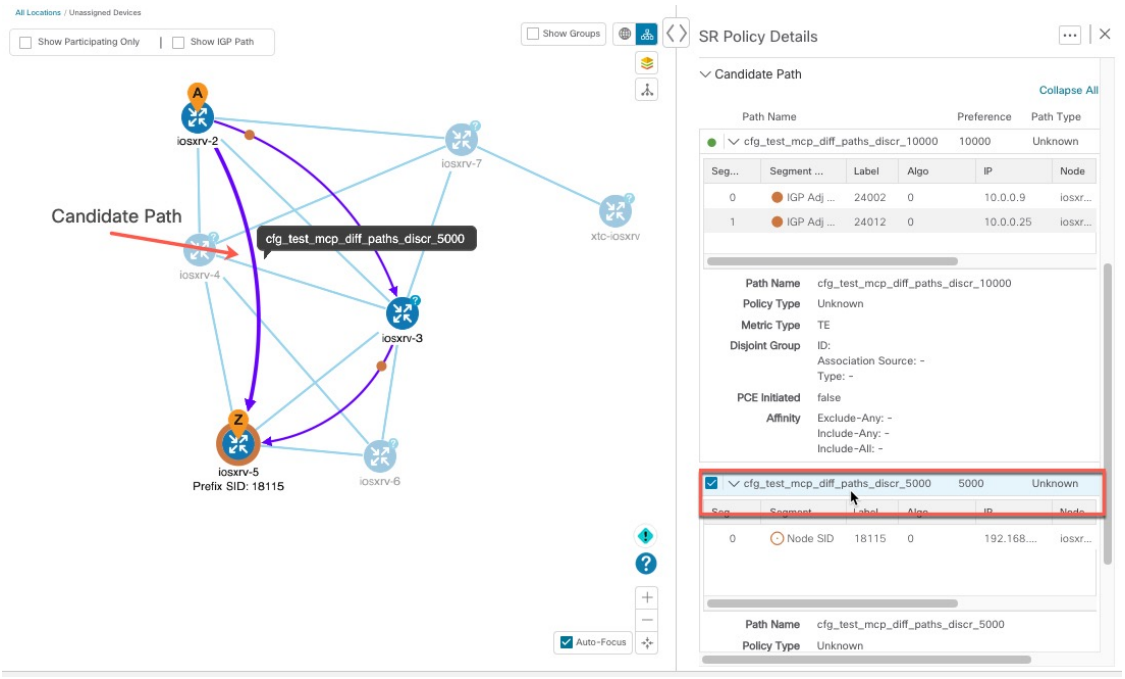
a) Check the check box next to any candidate path.

Note You will not be able to select or view explicit candidate paths.



b) From the **Candidate Path** area, hover your mouse over the candidate path name. The candidate path is highlighted on the topology map.

In this example, you see that the alternate path goes directly from **iosxrv-2 > iosxrv-5**.



Visualize Underlying Paths Associated with a Defined Binding-Segment ID (B-SID) Label

Crosswork Optimization Engine allows you to visualize the underlying path of a B-SID hop that you have manually configured on a device or configured using Crosswork Network Controller. In this example, we have assigned **15700** as a B-SID label on an SR-MPLS policy hop.

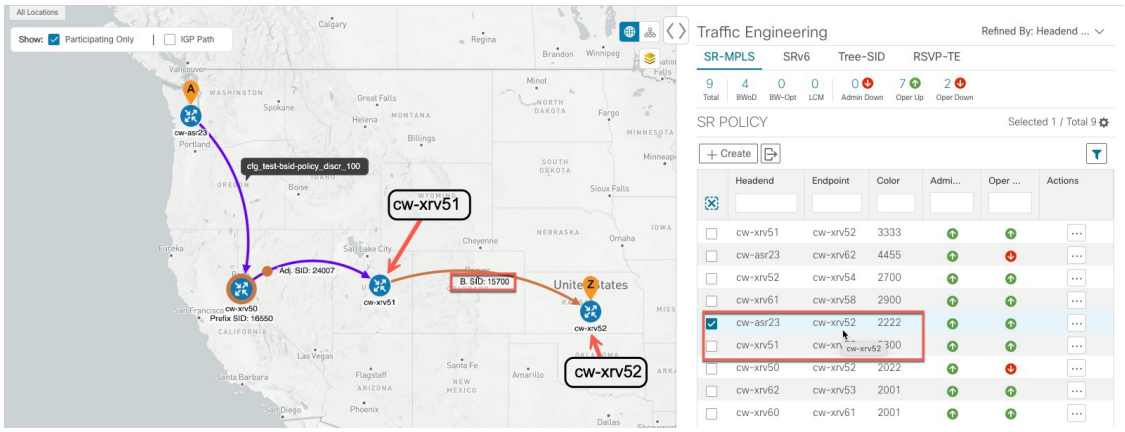
To view the B-SID underlying path for an SR-MPLS or SRv6 policy, do the following:

Step 1 From the main menu, choose **Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** or **SRv6** tab.

Step 2 Check the check box next to the SR-MPLS policy that contains a hop assigned with a B-SID label and hover your mouse over any part of the SR-MPLS row to see the B-SID name. The B-SID path is highlighted in ***orange*** on the topology map.

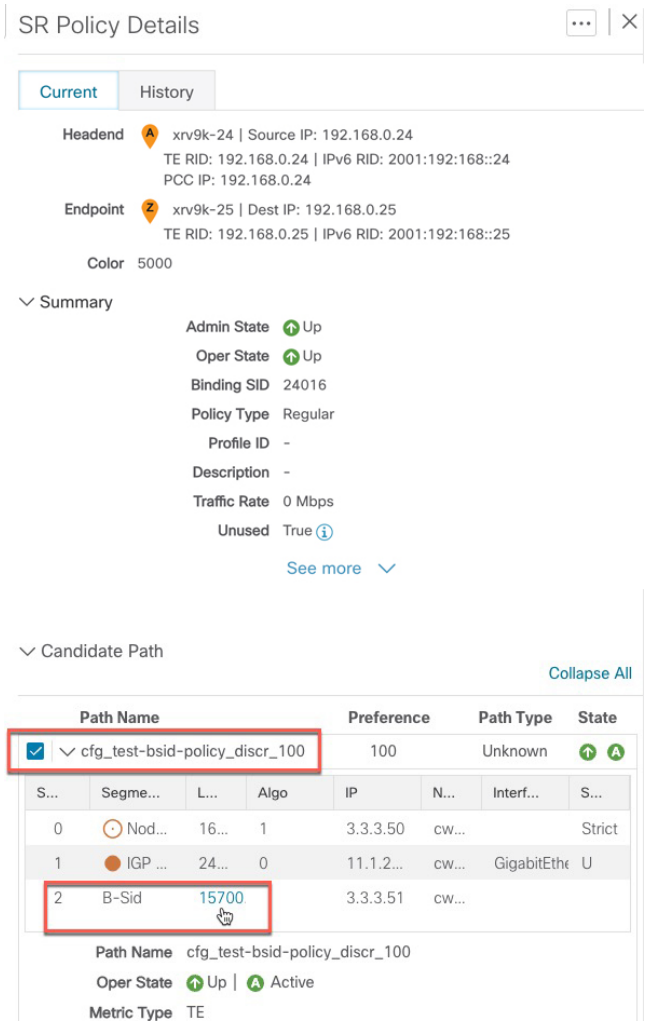
In this example, you see that the B-SID path is going from **cw-xrv51** to **cw-xrv52**.

Note Click image examples to zoom in for a closer look.

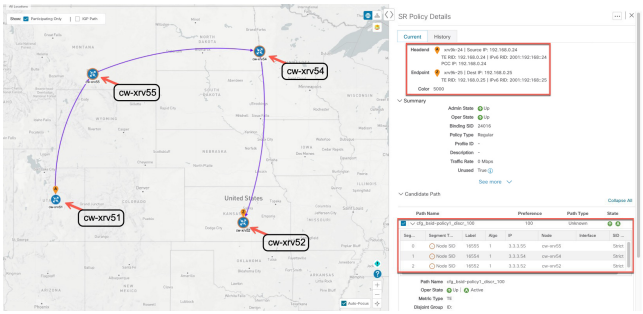


Step 3 From the **Actions** column, click ··· > **View Details**.

Step 4 From the **SR Policy Details** window, expand the active path name and click the ***B-SID label***. In this example, the B-SID label is **15700**.



Step 5 In the **SR Policy Details** window for the underlying path, expand the active path name to view more details. In this example, you see the underlying path actually goes from **cw-xrv51** > **cw-xrv55** > **cw-xrv54** > **cw-xrv52**.



Visualize Native SR Paths

Visualizing the native path will help you in OAM (Operations, Administration and Maintenance) activities to monitor label-switched paths (LSPs) and quickly isolate forwarding problems to assist with fault detection and troubleshooting in the network. Since this feature uses multipaths, all ECMP paths are shown between the source and destination. You can visualize only SR-MPLS policies.

Before you begin

Confirm that device requirements are met. See Visualize Native Path Device Prerequisites, on page 17.

To create a path query, do the following:

Step 1 From the main menu, choose **Traffic Engineering** > **Path Query.**

Step 2 On the Query Path Dashboard, click **New Query.**

Step 3 Under the New Path Query, select the required values and click **Get Paths.**

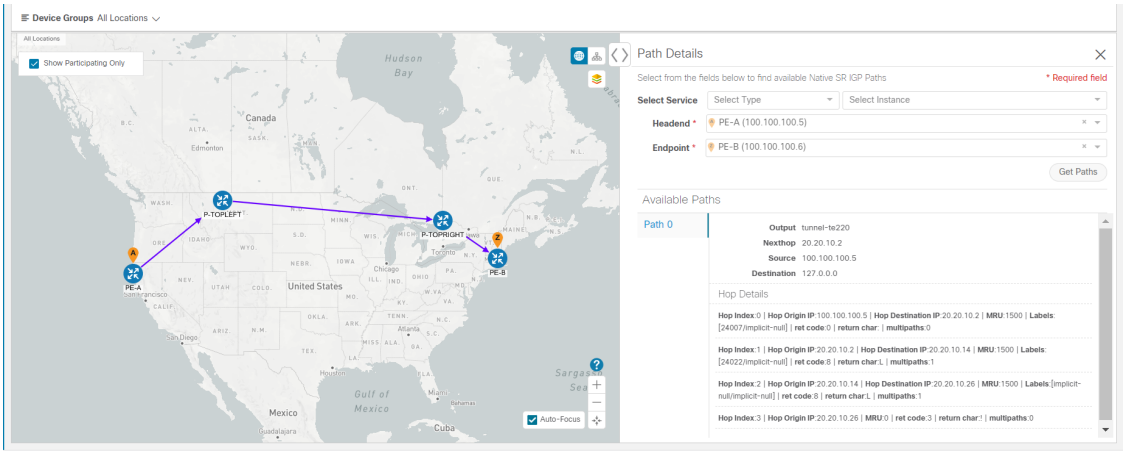
Step 4 Click **View Result** to view the query result.

Step 5 (Optional) On the result pop-up click, **View Past Result.** Check the query ID to view the available results.

Example:

In the below example, you can view the available paths : **Path 0**

Figure 4: Path Details



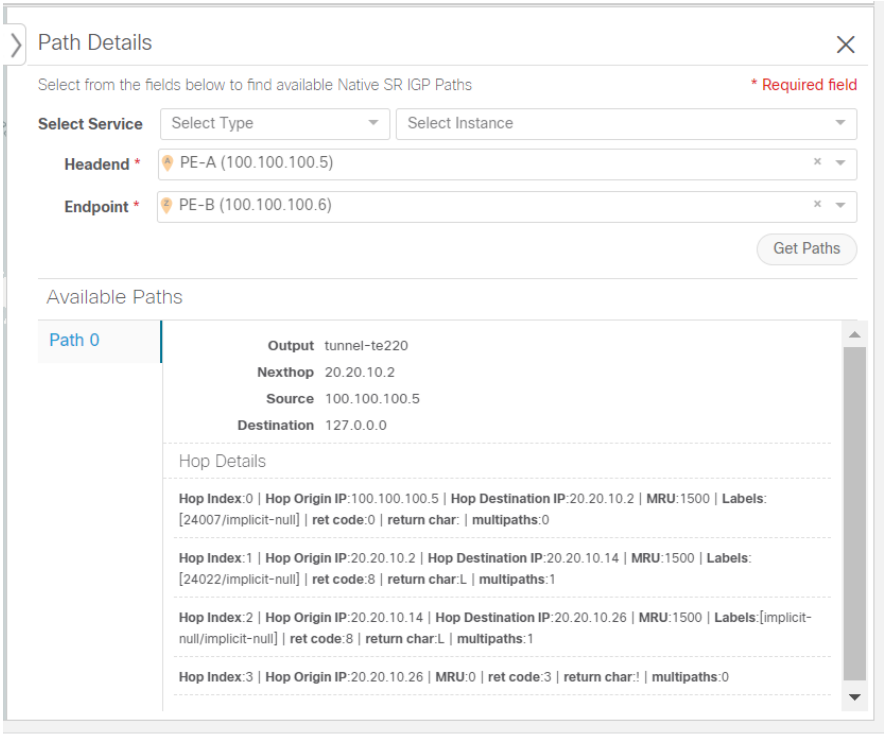
Step 6 From the **Actions** column, click **View Details**.

If you have not provided the longitude and latitude information for your devices, the path is visualized in the logical view.

Step 7 From the available paths, click **Path 0** to expand and view the active path.

Example:

Figure 5: Path Details



Visualize Native Path Device Prerequisites

Confirm the following device software and configurations are met prior to visualizing native paths.

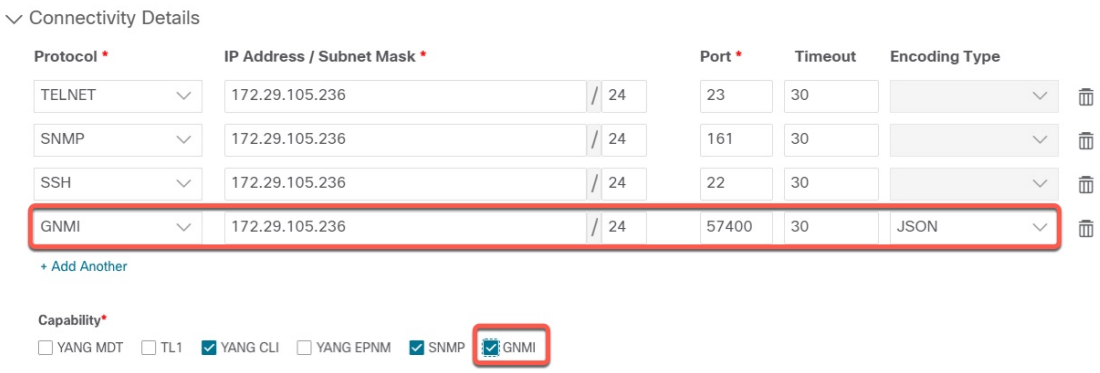
1. Devices should be running Cisco IOS XR 7.3.2 or higher. Run `show version` command to verify it.
2. Devices should have GRPC enabled.
   a. Run `show grpc` to confirm GRPC configuration. You should see something similar to this:

```
tpa
vrf default
address-family ipv4
default-route mgmt
!
address-family ipv6
default-route mgmt
!
!
!

or

linux networking
vrf default
address-family ipv4
default-route software-forwarding
!
address-family ipv6
default-route software-forwarding
!
!
!
```

Note

- `address-family` is only required in an IPv4 topology.
- To enable GRPC with a secure connection, you must upload security certificates to connect to the device.

3. Devices should have GNMI capability enabled and configured.
   a. From **Device Management**, click on a device and view device details ( ).
   b. Confirm that GNMI capability and connectivity details are configured.



Note Based on the type of devices, the following device encoding type are available:

- JSON
- BYTES
- PROTO
- ASCII
- JSON IETF

4. Devices should have the CDG router static address. Static route should be added from the device to the southbound CDG IP address. For example:

```
RP/0/RP0/CPU0:xrvr-7.3.2#config

RP/0/RP0/CPU0:xrvr-7.3.2(config)#router static

RP/0/RP0/CPU0:xrvr-7.3.2(config-static)#address-family ipv4 unicast <CDG Southbound
interface IP: eg. 172.24.97.110> <Device Gateway eg: 172.29.105.1>

RP/0/RP0/CPU0:xrvr-7.3.2(config-static)#commit
```

Configure TE Link Affinities

If you have any affinities you wish to account for when provisioning an SR policy, Tree-SID, or RSVP-TE tunnel, then you must define them on the Cisco Crosswork UI. Affinity names defined on devices are not collected by Cisco Crosswork. The affinity mapping is only used for visualization. For this reason, you should collect affinities on the device, then define affinity mapping in Cisco Crosswork UI with the same name and bits that are used on the device. Crosswork Optimization Engine will only send bit information to SR-PCE during provisioning. If an affinity mapping is not defined in the UI, then the affinity name is displayed as "UNKNOWN".

The affinity configuration on interfaces simply turns on some bits. It is a 32-bit value, with each bit position (0 - 31) representing a link attribute. Affinity mappings can be colors representing a certain type of service profile (for example: low delay, high bandwidth, and so on). This makes it easier to refer to link attributes.

See SR, Tree-SID, or RSVP-TE configuration documentation for your specific device to view descriptions and supported configuration commands (for example: Segment Routing Configuration Guide for Cisco ASR 9000 Series Router)

The following example shows the affinity configuration (`affinity-map`) on a device:

```
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
  !
 !
!
```

Step 1 From the main menu choose **Administration** > **Settings** > **System Settings > Traffic Engineering > Affinity > TE Link Affinities**. You can also define affinities while creating an SR-TE policy, Tree-SID, or RSVP-TE tunnel by clicking **Manage Mapping**.

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

Step 3 Enter the name and the bit it will be assigned. For example (using the above configuration):

Example:

Step 4 Click **Save** to save the mapping.

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.

Create Explicit SR-MPLS Policies

This task creates SR-MPLS policies using an explicit (fixed) path consisting of a list of prefix or adjacency Segment IDs (SID list), each representing a node or link along on the path.

Tip If you plan to use affinities, collect affinity information from your devices and then map them in Cisco Crosswork before creating an explicit SR-MPLS policy. For more information, see Configure TE Link Affinities, on page 18.

Step 1 From the main menu, choose **Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** tab.

Step 2 From the **SR Policies** table, click **+ Create**. If you are using Crosswork Network Controller, select either **PCE init** or **PCC init**.

Step 3 Enter or select the required SR-MPLS policy values. Hover the mouse pointer over ⓘ to view a description of the field.

Tip If you have set up device groups, you can select the device group from the **Device Groups** drop-down menu. Then navigate and zoom in on the topology map to click the device for headend or endpoint selection.

Step 4 Under Policy Path, click **Explicit Path** and enter a path name.

Step 5 Add segments that will be part of the SR-MPLS policy path.

Step 6 Click **Preview** and confirm that the policy you created matched your intent.

Step 7 If you want to commit the policy path, click **Provision** to activate the policy on the network or exit to abort the configuration process.

Step 8 Validate the SR-MPLS policy creation:

a. Confirm that the new SR-MPLS policy appears in the SR Policy table. You can also click the check box next to the policy to see it highlighted in the map.

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

b. View and confirm the new SR-MPLS policy details. From the **SR Policy** table, click ··· and select **View**.

Note On a setup with high node, policy, or interface counts, a timeout may occur during policy deployment. To configure timeout options, see Configure TE Timeout Settings.

Create Dynamic SR-MPLS Policies Based on Optimization Intent

This task creates an SR-MPLS policy with a dynamic path. SR-PCE computes a path for the policy based on metrics and path constraints (affinities or disjointness) defined by the user. A user can select from three available metrics to minimize in path computation: IGP, TE, or latency. The SR-PCE will automatically re-optimize the path as necessary based on topology changes. In the event of a link or interface failing, the network will find an alternate path that meets all the criteria specified in the policy and raise an alarm. The alarm is also raised in case no path is found, the packets are then dropped.

Tip If you plan to use affinities, collect affinity information from your devices and then map them in Cisco Crosswork before creating a dynamic SR-MPLS policy. For more information, see Configure TE Link Affinities, on page 18 or Configure Flexible Algorithm Affinities.

Before you begin

If you have affinities configured on your devices, define an affinity mapping using the Cisco Crosswork UI prior to provisioning an SR-MPLS policy (see Configure TE Link Affinities, on page 18).

Step 1 From the main menu, choose **Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** tab.

Step 2 From the **SR Policy** table, click **+ Create**. If you are using Crosswork Optimization Engine within Crosswork Network Controller, select either **PCE Init** or **PCC Init**.

Step 3 Under **Policy Details**, enter or select the required SR-MPLS policy values. Hover the mouse pointer over ⓘ to view a description of each field.

Tip If you have set up device groups, you can select the device group from the **Device Groups** drop-down menu. Then navigate and zoom in on the topology map to click the device for headend or endpoint selection.

Step 4 Under **Policy Path**, click **Dynamic Path** and enter a path name.

Step 5 Under **Optimization Objective**, select the metric you want to minimize.

Step 6 Define any applicable constraints and disjointness.

Note
- Affinity constraints and disjointness cannot be configured on the same SR-MPLS policy. Also, there cannot be more than two SR-MPLS policies in the same disjoint group or subgroup. The configuration will not be allowed during Preview.
- If there are existing SR-MPLS policies belonging to a disjoint group that you define here, all SR-MPLS policies that belong to that same disjoint group are shown during Preview.

Step 7 Under **Segments**, select whether or not protected segments should be used when available.

Step 8 If applicable, enter a SID contraint in the **SID Algorithm** field. Cisco Crosswork will try to find a path with this SID. If a path with the SID constraint cannot be found, the provisioned policy will remain operationally down until the conditions are met.

Note
- Flexible Algorithm: The values correspond to the Flexible Algorithm that are defined on the device and the 128-255 range is enforced by Cisco IOS XR.
- Algorithm 0: This is a Shortest Path First (SPF) algorithm based on link metric. This shortest path algorithm is computed by the Interior gateway protocol (IGP).
- Algorithm 1: This is a Strict Shortest Path First (SSPF) algorithm based on link metric. The algorithm 1 is identical to algorithm 0 but requires that all nodes along the path honor the SPF routing decision. Local policy does not alter the forwarding decision. For example, a packet is not forwarded through locally engineered path.

Step 9 Click **Preview**. The path is highlighted on the map.

Step 10 If you want to commit the policy path, click **Provision**.

Step 11 Validate the SR-MPLS policy creation:

a. Confirm that the new SR-MPLS policy appears in the SR Policy table. You can also click the check box next to the policy to see it highlighted in the map.

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

b. View and confirm the new SR-MPLS policy details. From the **SR Policy** table, click ··· and select **View**.

Note On a scaled setup with high node, policy, or interface counts, a timeout may occur during policy deployment. To configure timeout options, see Configure TE Timeout Settings.

Modify SR-MPLS Policies

To view, modify, or delete an SR-MPLS policy, do the following:

Step 1 From the main menu, choose **Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** tab.

Step 2 From the SR Policy table, locate the SR-MPLS policy you are interested in and click ···.

Step 3 Choose **View** or **Edit/Delete**.

Note
- You can only modify or delete SR-MPLS policies that have been created with the UI.
- After updating the SR-MPLS policy details, you can preview the changes on the map before saving it.