



# Bandwidth and Network Optimization

This section explains the following topics:

- [Overview, on page 1](#)
- [Scenario: Use CS-SR Policies to Reserve Bandwidth, on page 15](#)

## Overview

### Objective

Network operators need a toolset to help automate bandwidth optimization, steer traffic with little operator intervention, and ensure that critical links always have sufficient bandwidth to avoid congestion.

### Challenge

For service providers, managing bandwidth problems used to be a reactive and manual process. Pressure to solve it is huge. Network congestion leads to poor end-customer experiences. Congested links, high latency, and other network impairments lead to a poor perception of the services carried across your network or result in an inability to meet the service level agreements (SLAs) you have with your customers. In the worst-case scenario, your network issues lead to SLA or contract violations and the loss of your brand equity.

### Solution

Using LCM and Circuit Style policies, SPs can now specify business-critical links with the intention to reserve bandwidth for these links. Identifying critical links and the operator's intention enables automatic optimization of the network in real time.

Cisco Crosswork Network Controller offers both:

- Local Congestion Mitigation (LCM) is a tactical solution for bandwidth management and congestion mitigation. It is best applied when you are attempting to solve congestion issues directly, on the devices themselves, without a full-scale traffic matrix or advanced planning.
- Circuit-Style Segment Routing (CS-SR) is a strategic traffic engineering solution that permits you to reserve bandwidth in advance for critical links, avoiding congestion issues entirely for these high-priority links.

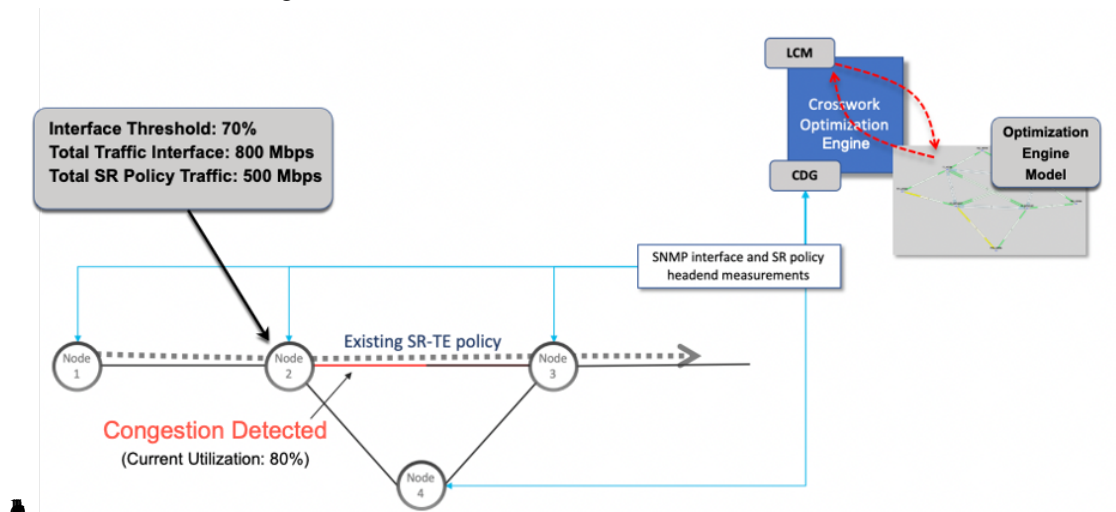
## Local Congestion Mitigation (LCM)

Instead of optimizing for bandwidth resource in the network by rerouting traffic in the entire network (end-to-end path optimization), LCM checks the capacity locally, in and around the congested area, at an interface level and reroutes traffic between the endpoints of the congested interface (local interface-level optimization). Focusing on an issue locally eliminates the need for simulating edge-to-edge traffic flows in the network through a full traffic matrix, which is both cumbersome to create and is less scalable as node counts continue to increase.

When congestion is detected in the network, LCM provides recommendations to divert the minimum amount of traffic away from the congested interface. LCM performs the collection of SR-TE policy and interface counters through SNMP. It estimates the amount of traffic that may be diverted and, if the user approves, performs the mitigation through the deployment of Tactical Traffic Engineering (TTE) SR-TE policies. Mitigating congestion locally does not require the use of the full Segment Routing Traffic Matrix (SR-TM). TTE SR-TE policies are created at the device on only either side of the congested link, with the shortest paths possible that do not congest interfaces elsewhere.

### How Does LCM Work?

1. First, network operators create domains that define "local" portions of the network. A domain can be the entire network, but more commonly a domain will match one or geographical areas or groups of device interfaces. In this example, we have defined a domain with four devices and all their interfaces. We also assume that all the links in this domain are 1Gbps.
2. Operator specifies a threshold defining what "congestion" means for a particular domain. In this example, the operator has set the domain's congestion threshold to 70%. The congestion threshold you decide on may vary. For guidance on how to determine what's congestion threshold is best for your network and its domain architecture, see [Cisco's Local Congestion Mitigation \(LCM\) White Paper](#).
3. LCM first analyzes the Optimization Engine Model (a realtime representation of the physical network, its topology and its traffic) on a regular cadence. After a congestion check interval, LCM detects congestion when Node 2 utilization goes above the 70% utilization



- 4.
5. LCM calculates how much traffic is eligible to divert. LCM will follow these rules and restrictions in its recommendations:

LCM only diverts traffic that is not already routed by an existing SR policy (for example: unlabeled, IGP-routed, or carried via FlexAlgo-0 SIDs). The traffic within an SR policy will not be included in LCM calculation and will continue to travel over the original programmed path.

LCM computes diversion-eligible traffic by taking the interface traffic statistics that account for all traffic on the interface and subtracting the sum of traffic statistics for all SR-TE policies that flow over the interface.

*Total interface traffic – SR policy traffic = Eligible traffic that can be optimized*

This process must account for any ECMP splitting of SR policies to ensure the proper accounting of SR policy traffic. In this example, the total traffic on congested Node 2 is 800 Mbps. The total traffic of all SR policies routed over Node 2 is 500 Mbps.

The total traffic that LCM can divert in this example is 240 Mbps. That is: 800 Mbps – 560 Mbps = 240 Mbps

6. LCM calculates the amount of traffic that must be sent over alternate paths by subtracting the threshold-equivalent traffic from the total traffic on the interface. In this example, the amount to be diverted is 100 Mbps:

$800 \text{ Mbps} - 640 \text{ Mbps (70\% threshold)} = 100 \text{ Mbps}$

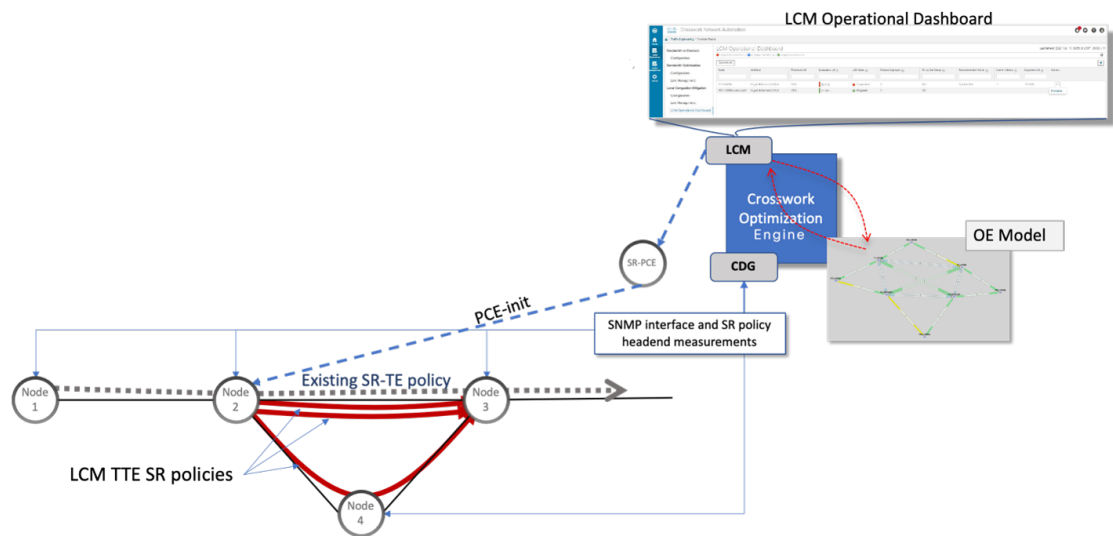
LCM must route 100 Mbps of 300 Mbps (eligible traffic) to another path.

7. LCM determines how many TTE SR policies are needed and their paths. The ratio of how much LCM eligible traffic can stay on the shortest path to the amount that must be rerouted, will determine the number of TTE SR policies that are needed on the shortest versus alternate paths, respectively.

In this example, LCM needs to divert one-third of the total eligible traffic (100 Mbps out of 300 Mbps) away from the congested link. Assuming a perfect ECMP, LCM estimates that three tactical SR-TE policies are required to create this traffic split: one tactical SR-TE policy will take the diversion path and two tactical SR-TE policies will take the original path. There is sufficient capacity in the path between Node 2 and Node 4. Therefore, LCM recommends three TTE SR policies (each expected to route approximately 100 Mbps) to be deployed from Node 2 to Node 3 via SR-PCE:

- 2 TTE SR policies to take a direct path to Node 3 (200 Mbps)
- 1 TTE SR policy takes a path via Node 4 (100 Mbps)

These recommendations will be listed in the **LCM Operational Dashboard**.



Assuming you deploy these TTE SR policies, LCM continues to monitor the deployed TTE policies and will recommend modifications or deletions as needed in the LCM **Operational Dashboard**. TTE SR policy removal recommendations will occur if the mitigated interface would not be congested if these policies were removed (minus a hold margin). This helps to avoid unnecessary TTE SR policy churn throughout the LCM operation.

### Circuit-Style Policies

**Circuit-Style Segment Routing Policies** (CS-SR, or CS policies) are connection-oriented transport services that you can use to implement what are sometimes referred to as "circuit emulations" or "private lines". Combining segment-routing architecture's adjacency SIDs with stateful PCEP path computation, CS policies provide:

- Persistent, dedicated, bi-directional, co-routed transport paths with predictable latencies and other performance metrics in both directions.
- Guaranteed bandwidth commitments for traffic-engineered services using these paths.
- End-to-end path protection to ensure there is no impact on Service Level Agreements.
- Automatic monitoring, maintenance and restoration of path integrity.
- Flexible operations, administration and management of Circuit-Style paths.
- A software-defined replacement for older CEM infrastructure, such as SONET/SDH.

### How Do Circuit-Style Policies Work?

Initial configuration of CS policies follows these steps:

1. Crosswork Network Controller and its applications discover and map the network topology.
2. Crosswork users enable CS policy support, specifying the base bandwidth to be allocated to CS policies as a whole, and a threshold percentage of bandwidth usage which, when exceeded on any CS-calculated path, will generate an alarm. So, for example, on a 1 GB link with 20 percent of bandwidth reserved for Circuit Style use, CS policies can use up to 200 Mbps of that link. Note, however, that if the bandwidth

minimum threshold is set to the default of 80 percent, alarms will be generated as soon as 160 Mbps of the link is used.

3. Network operators create a CS policy for each set of nodes for which they want to establish a guaranteed path. The policy specifies the two nodes to be linked by the main path, the bandwidth to be reserved, and the backup path. To ensure bandwidth and path failures can be accommodated, the configuration must include bi-directionality, path protection, and performance-management liveness-detection settings.
4. When the operator commits the CS policy, the device-resident Path Computation Client (PCC) will request the Crosswork-resident PCE server to compute candidate Working and Protected paths that conform to the CS policy's bandwidth and other constraints (using a single PCEP request message).
5. The PCC computes both paths and deducts the CS policy-guaranteed bandwidth for them from the total available bandwidth allocated when CS policy support was enabled.
6. Crosswork replies to the PCC with the primary Working and Protected path lists and commits to, or "delegates", them. The topology map displays the current Active and Protected paths between the two nodes, using the colors configured when the CS policy was configured, and labels the two endpoint nodes so they can be identified as CS policy endpoints.

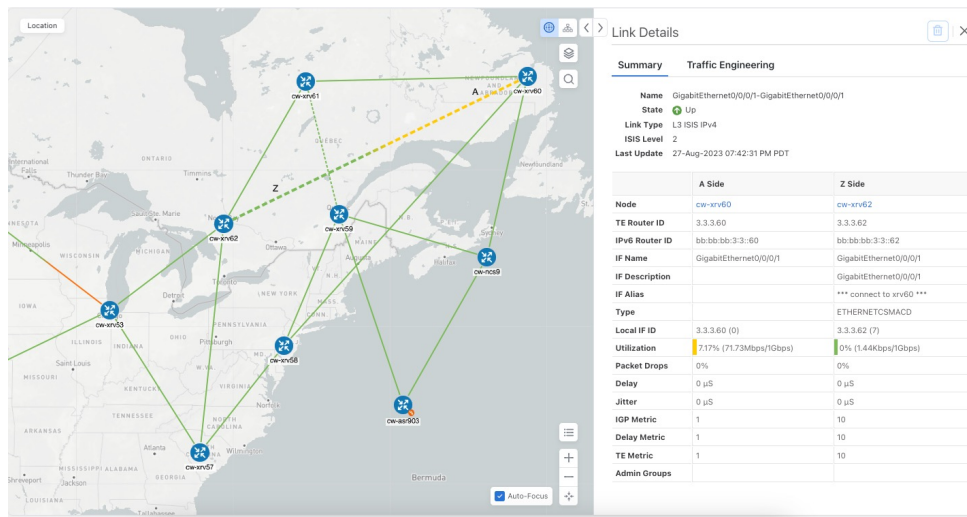
After the initial configuration:

1. Crosswork monitors the delegated path and the active CS policies. It updates the available and reservable bandwidth in the network in near real time.
2. Crosswork generates threshold-crossing alarms when bandwidth usage or additional CS policy requirements exceed the configured reserved bandwidth or bandwidth usage threshold.
3. If delegated paths fail for any reason, Crosswork recomputes paths as needed.

## Scenario: Use LCM to Reroute Traffic on an Overused Link

In this scenario, we will enable Local Congestion Mitigation (LCM) and observe its congestion mitigation recommendations. LCM will recommend that we deploy Tactical Traffic Engineering Segment Routing (TTE SR) policies on a device's interfaces when usage exceeds a defined threshold. We will preview the recommended TTE SR policies before committing them.

This example uses the following topology:



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

We will enable LCM with a configuration that results in the link between **cw-xrv60** and **cw-xrv60** becoming over-used. We will then review the mitigation solutions Crosswork calculates. In this example, it is left to the operator whether to apply the solution or not.

## LCM Scenario: Assumptions and Prerequisites

The following sections list high-level requirements that must be met to ensure proper LCM operation.

### Congestion Evaluation Requirements

LCM requires traffic statistics from the following:

- Interface traffic measurements
- Headend SR-TE policy traffic measurements

To ensure LCM is receiving these traffic statistics:

- Enable SNMP on the devices whose traffic you want to monitor, including the headend device. For more on this task, see [Configuring SNMP Support](#). Note that gNMI is also an option for collecting traffic measurements.
- Ensure that the SNMP-enabled devices are all reachable from the Crosswork Data Gateway. For more on this task, see [Check Connectivity to the Destination](#).
- Configure the headend device to use strict SID labels for SR policies. To perform this task:
  1. Enable segment routing on the headend device and configure the segment routing global block (SRGB) and the segment routing local block (SRLB) ranges. For example:

```
segment-routing
mpls
  global-block 16000 23999
  node-msd 16
```

```
!
srlb 15000 15999
```

2. Configure the SR policy candidate paths to use strict SID labels. You can use either explicit paths or dynamic paths with constraints. For example:

```
segment-routing
traffic-eng
policy COLOR-100-TO-10.0.0.1
color 100 end-point ipv4 10.0.0.1
candidate-paths
preference 100
explicit segment-list SL1
!
preference 200
dynamic
constraints
affinity include-any RED BLUE
sid-algorithm strict-spf
!
!
!
!
!
!
segment-list SL1
index 10 mpls label 16001 node 10.0.0.2 strict
index 20 mpls label 16002 node 10.0.0.3 strict
index 30 mpls label 16003 node 10.0.0.4 strict
!
```

3. Configure the SR policy headend behavior using the binding SID and the autoroute announce option. For example:

```
!segment-routing
traffic-eng
pcc
profile 1
autoroute
include ipv4 all
force-sr-include
!
!
!
!
```

### Congestion Mitigation Requirements

The headend device must support PCE-initiated SR-TE policies with autoroute steering. However, LCM will not work if the headend is a Cisco NCS device and there is L2VPN traffic in the network.

Devices should be configured with `force-sr-include` to enable traffic steering into SR-TE policies with autoroute. For example:

```
segment-routing traffic-eng pcc profile ID autoroute force-sr-include
```

The `ID` parameter in this command identifies the PCC profile associated with the SR-TE policy that PCE has provisioned. The ID value can be any integer from 1 to 65535, but it must match the profile ID that PCE uses to instantiate the policy. If not, the policy will not be activated. For example, if PCE provisions a policy with profile ID 10, you must configure `segment-routing traffic-eng pcc profile 10 autoroute`

`force-sr-include` on the headend router to enable autoroute announcement for that policy. For more information, see the [Segment Routing Configuration Guide, Cisco IOS XE 17 \(Cisco ASR 920 Series\), COE-PCE Initiated SR Policy with OSPF and IS-IS SR-TE Autoroute Announce](#).



**Note** The ID that is configured under the PCC profile, must match the Profile ID option set in the LCM Configuration page.

The headend device must support Equal Cost Multi-Path (ECMP) across multiple parallel SR-TE policies. To verify that a device can support SR-TE policies using ECMP, check that the device has the following:

- Segment Routing is enabled and configured, with a Segment Routing Global Block (SRGB) that matches the SRGB of the SR-TE policy headend and tailend routers. Use the `show segment-routing mpls state` command to verify the SRGB configuration on the device.
- BGP-LS is enabled and configured to advertise and receive link-state information from the SR-TE policy headend and tailend routers. Use the `show bgp link-state link-state` command to verify the BGP-LS status and the `show bgp link-state link-state database` command to verify the link-state information on the device.
- ECMP is enabled and configured to load-balance traffic across multiple equal-cost paths based on flows. Use the `show ip route` command to verify the ECMP routes and the `show ip cef` command to verify the ECMP load-balancing algorithm on the device.

If all these conditions are met, then the device can support an SR-TE policy using ECMP.

### Related Topics

For more information and examples on how to configure and verify SR-TE policies, see:

- [Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#)
- [Segment Routing Configuration Guide, Cisco IOS XE 17 | Access and Edge Routers](#)

## LCM Scenario: Workflow

Workflow steps	Detailed procedure links
Step 1. Enable LCM and configure the global utilization thresholds	<a href="#">Step 1: Enable LCM and Configure the Utilization Thresholds, on page 9</a>
Step 2. View link congestion on the map	<a href="#">Step 2: View Link Congestion on the Map, on page 11</a>
Step 3. View TTE SR policy recommendations in the LCM Operational Dashboard	<a href="#">Step 3: View TTE SR Policy Recommendations in the LCM Operational Dashboard, on page 11</a>
Step 4. Validate the TTE SR policy deployment	<a href="#">Step 4: Validate TTE SR Policy Deployment, on page 13</a>
Step 5. Remove the TTE SR policies upon LCM recommendation	<a href="#">Step 5: Remove TTE SR policies on LCM Recommendation, on page 14</a>



## Step 1: Enable LCM and Configure the Utilization Thresholds

To enable LCM and configure the global utilization threshold:

**Step 1** Go to **Services & Traffic Engineering > Local Congestion Mitigation > Domain-ID** and click **Configure**.

**Step 2** Toggle the **Enable** switch to **True**, and enter the global utilization threshold you want to set. In this case, we set the threshold at 80%, and select the **Interfaces to Monitor > All Interfaces** option. In the **Advanced** tab, Operation mode is set to **Manual**. Manual mode allows you to view recommended TTE policies prior and decide whether or not to deploy them. To see information about other options for each configuration setting, hover the mouse over **i** (help icon).

**Figure 1: Basic LCM Configuration**

Configuration

Basic  Advanced

<p><b>Enable</b> ⓘ</p> <p>False <input type="checkbox"/> True <input checked="" type="checkbox"/></p>	<p><b>Color</b> * ⓘ</p> <p>2000</p> <p>Range: 1 to 4294967294</p>	<p><b>Utilization Threshold</b> * ⓘ</p> <p>80</p> <p>Range: 0 to 100</p>
<p><b>Utilization Hold Margin</b> * ⓘ</p> <p>5</p> <p>Range: 0 to Utilization Threshold</p>	<p><b>Delete Tactical SR Policies when Disabled</b> ⓘ</p> <p>False <input type="checkbox"/> True <input checked="" type="checkbox"/></p>	<p><b>Profile ID</b> * ⓘ</p> <p>0</p> <p>Range: 0 to 65534</p>
<p><b>Congestion Check Interval</b> * ⓘ</p> <p>900 seconds</p> <p>Range: 60 to 86400 seconds</p>	<p><b>Max LCM Policies per Set</b> * ⓘ</p> <p>8</p> <p>Range: 1 to 8</p>	<p><b>Interfaces to Monitor</b> ⓘ</p> <p><input type="radio"/> Selected Interfaces <input checked="" type="radio"/> All Interfaces</p>
<p><b>Description</b> ⓘ</p> <p>LCM Startup Config</p>		

## Step 1: Enable LCM and Configure the Utilization Thresholds

Figure 2: Advanced LCM Configuration (Manual Mode)

Configuration

Basic **Advanced**

Auto Repair Solution ⓘ

False  True

Stay in Area ⓘ

False  True

Adjacency Hop Type ⓘ

Unprotected

Operation Mode ⓘ

Manual  Automated

Optimization Objective ⓘ

Minimize the IGP metric

Deployment Timeout \* ⓘ

180

Range: 10 to 300

Congestion Check Suspension Interval \* ⓘ

600

Range: 600 to 3600

Over-Provisioning Factor \* ⓘ

Range: 0.0 to 100.0

Uneven ECMP Traffic Threshold \* ⓘ

Range: 0.0 to 100.0

Throttle Mode Threshold \* ⓘ

5

Range: 0 to 10

Step 3 Click **Commit Changes**.

**Note** After committing the configuration changes, LCM will display *recommendations* on the **LCM Operational Dashboard** if congestion occurs on any monitored interfaces. LCM will *not* commit or deploy new TTE policies automatically. Later, you will be able to preview the recommended TTE policies and decide whether or not to commit and deploy them onto your network.

Step 4 You can also define individual interface thresholds. Go to the **Customized Interface Thresholds** page (**Traffic Engineering > Local Congestion Mitigation > Domain-ID > ... > Interface Thresholds**).

See the following example and note the defined threshold for cw-xrv60 with interface GigabitEthernet0/0/0/1 is 16%.

**Note** The utilization thresholds used in this example are extremely low and are best used for lab environments.

Figure 3: Customized Interface Thresholds

Customized Interface Thresholds

Interfaces to Monitor: Selected Interfaces - LCM monitors only the interfaces with custom thresholds.

**+ Create**   |  Edit Mode: OFF

Node	Interface	Threshold (%)	Select for
cw-xrv60	GigabitEthernet0/0/0/1	16	<input type="checkbox"/>

## Step 2: View Link Congestion on the Map

The link between **cw-xrv60** and **cw-xrv62** is now congested. Let's see that on the map.

**Step 1** Go to **Services & Traffic Engineering > Traffic Engineering**.

**Step 2** Click on the link to view link details, including utilization information. Usage has surpassed the custom LCM threshold defined at 16% for node **cw-xrv60** with interface GigabitEthernet0/0/0/1.

	A Side	Z Side
Node	cw-xrv60	cw-xrv62
TE Router ID	3.3.3.60	3.3.3.62
IPv6 Router ID	bb:bb:bb:3:3::60	bb:bb:bb:3:3::62
IF Name	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
IF Description		GigabitEthernet0/0/0/1
IF Alias		*** connect to xrv60 ***
Type		ETHERNETCSMACD
Local IF ID	3.3.3.60 (0)	3.3.3.62 (7)
Utilization	38.35% (383.5Mbps/1Gbps)	0% (1.44Kbps/1Gbps)
Packet Drops	0%	0%
Delay	0 μs	
Jitter	0 μs	
IGP Metric	1	
Delay Metric	1	
TE Metric	1	
Admin Groups		

	A Side
Node	cw-xrv60
TE Router ID	3.3.3.60
IPv6 Router ID	bb:bb:bb:3:3::60
IF Name	GigabitEthernet0/0/0/1
IF Description	
IF Alias	
Type	
Local IF ID	3.3.3.60 (0)
Utilization	38.35% (383.5Mbps/1Gbps)

## Step 3: View TTE SR Policy Recommendations in the LCM Operational Dashboard

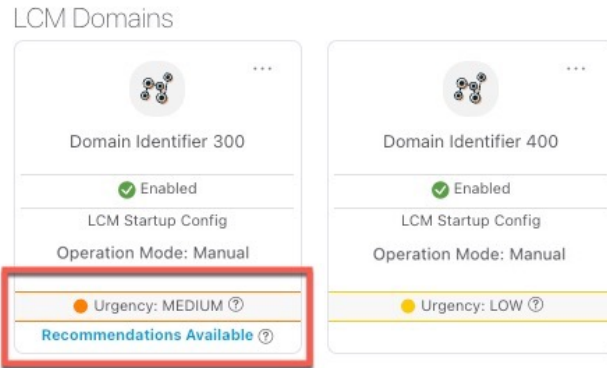
LCM has detected the congestion and computed tactical policies to mitigate the congestion, which we can preview and then decide whether or not to commit them.

Note that, in this scenario, the congested device is healthy, reachable and in sync with Crosswork. The actions we take and policies we implement will be different if, in addition to congestion, the device is down, unreachable or out of sync.

**Step 1** Go to **Services & Traffic Engineering > Local Congestion Mitigation**.

### Step 3: View TTE SR Policy Recommendations in the LCM Operational Dashboard

When congestion is detected, the domain displays the urgency type and recommendations that are available. Click the question mark icons to display more information about the urgency type and when the most recent recommendation was given.



**Step 2** Open the Operational Dashboard (**Services & Traffic Engineering > Local Congestion Mitigation > Domain-ID > ... > Operational Dashboard**).


The dashboard shows that cw-xrv60 utilization has surpassed 16% and is now at 38.5%. In the **Recommended Action** column, LCM recommends the deployment of TTE policy solution sets (**Recommended Action - Update Set**) to address the congestion on the interface.

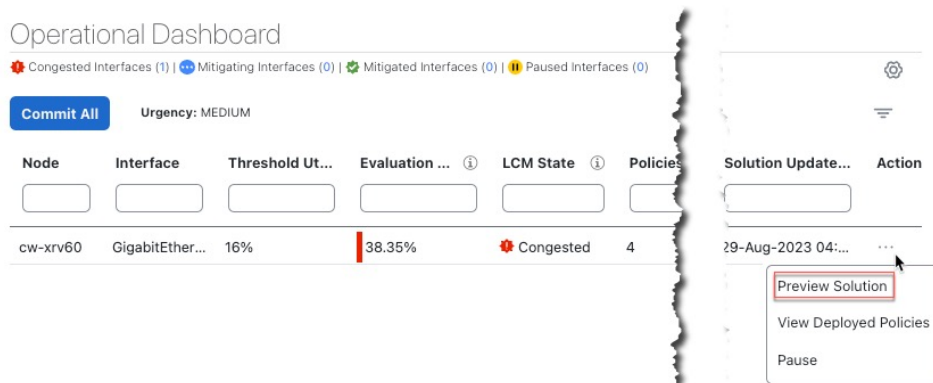
Operational Dashboard

Congested Interfaces (1) | Mitigating Interfaces (0) | Mitigated Interfaces (0) | Paused Interfaces (0)

Commit All Urgency: MEDIUM

Node	Interface	Threshold Ut...	Evaluation ...	LCM State	Policies De...	Policy Set ...	Recommende...	Commit ...	Expected Util...	Solution Update...
cw-xrv60	GigabitEther...	16%	38.35%	Congested	4	DEGRADED	Update Set	None	14%	29-Aug-2023 04:...

**Step 3** Before committing TTE policies, you can preview the deployment of each TTE policy solution set. Click  in the **Actions** column and choose **Preview Solution**.



The resulting window displays the node, interface, and the recommended action for each TTE policy. From the Preview window, you can select the individual TTE policies, and view different aspects and information as you would normally do in the topology map. You can expand each policy to view individual segments. After reviewing the potential implications on your network, you can decide whether or not to deploy the bypass policies that LCM recommends.

The following figure shows the recommended TTE policies for node cw-xrv60.

Preview Recommended TTE Policies

Node cw-xrv60  
Interface GigabitEthernet0/0/0/1

Candidate Path

Headend	Endpoint	Color	Recommended Action
<input checked="" type="checkbox"/> cw-xrv60	cw-xrv62	2000	UPDATE

Seg...	Segment Type	Label	Algo	IP	No...	Interf...
0	Node SID	16562	1	3.3.3.62	cw...	

Se...	Segme...	La...	Algo	IP	N...	Interf...	Sti...
0	IGP ...	24...	0	12.1.14...	cw...	GigabitEthe	
1	Nod...	165...	1	3.3.3.57	cw...		Stri...
2	Nod...	165...	1	3.3.3.62	cw...		Stri...

[Back To LCM Dashboard](#)

**Step 4** After you are done viewing the recommended TTE policies on the map, go back to the **Operational Dashboard** and click **Commit All**. The LCM State column changes to **Mitigating**.

All LCM recommendations per domain must be committed in order to mitigate congestion and produce the expected utilization as shown in the **Operational Dashboard**. The mitigating solution is based on *all* LCM recommendations being committed because of dependencies between solution sets.

LCM Domain Identifier: 300  
Operational State: Enabled Description: LCM Startup Config Mode: Manual

Operational Dashboard

Interface Thresholds

Configuration

[Commit All](#) Urgency: LOW

Node	Interface	Threshold Util...	Evaluation UL...	LCM State	Policies Depl...	Policy Set S...	Recommended...	Commit St...
cw-xrv60	GigabitEther...	16%	31.01%	Mitigating	2	-	No Change	CONFIRMED

## Step 4: Validate TTE SR Policy Deployment

To validate the TTE SR policy deployment, follow the steps given below:

**Step 1** With the **Operational Dashboard** displayed, click the at the top right of the user interface to open the **Alarms** window, then select the **Events** tab. You can use these two tabs to monitor LCM alarms and events. The **Events** shows you events for the LCM recommendations, the commit actions, as well as any exceptions.


Crosswork will report network events that are detected based on the policies and features you have enabled. For example, if a link drop causes an SR-TE policy to go down, or if LCM detects congestion, an event is displayed in the UI.

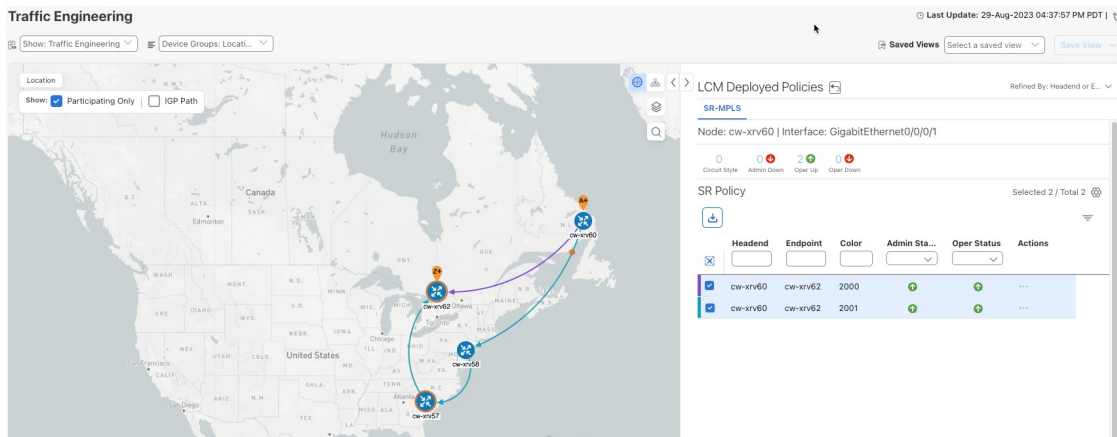
**Step 2** Return to the **Operational Dashboard** to see that the LCM state changes to **Mitigated** for all TTE policy solution sets.

**Note** The LCM state change can take up to twice as much time as the SNMP cadence.

## Step 5: Remove TTE SR policies on LCM Recommendation

## Step 3


Confirm the TTE policy deployment by viewing the topology map. Click  in the **Actions** column and choose **View Deployed Policies**. The deployed policies are displayed in focus within the topology map. All other policies are dimmed.

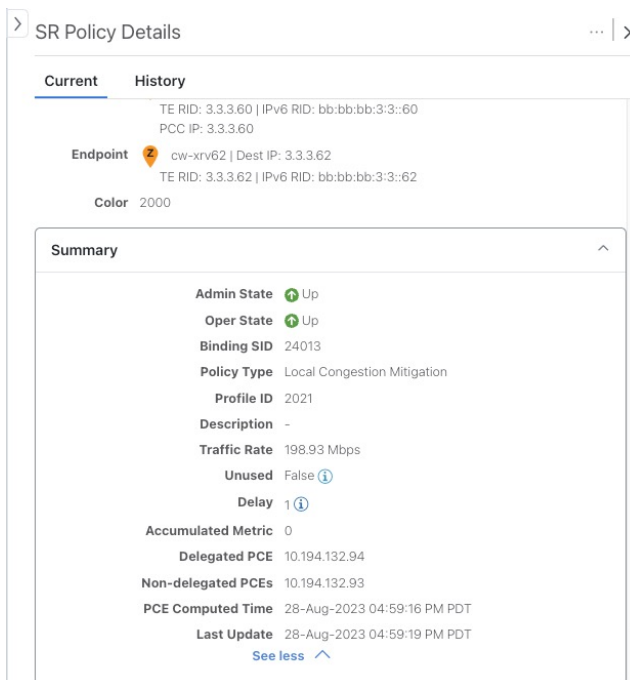


The screenshot shows the Traffic Engineering interface. On the left, a map of the United States displays several network nodes (cw-xrv60, cw-xrv62, cw-xrv58, cw-xrv57) connected by lines. On the right, the 'LCM Deployed Policies' panel is open, showing a table of SR Policies. The table has columns for Headend, Endpoint, Color, Admin Sta..., Oper Status, and Actions. Two policies are listed:

Headend	Endpoint	Color	Admin Sta...	Oper Status	Actions
cw-xrv60	cw-xrv62	2000		Up	...
cw-xrv60	cw-xrv62	2001		Up	...

## Step 4

View the SR policy details. From the **Actions** column of one of the deployed policies, click  and choose **View Details**. Note that the **Policy Type** is **Local Congestion Mitigation**.



The screenshot shows the 'SR Policy Details' view. It includes a 'Current' tab and a 'History' tab. The 'Current' tab displays the following information:

- TE RID: 3.3.3.60 | IPv6 RID: bb:bb:bb:3:3:60
- PCC IP: 3.3.3.60
- Endpoint: cw-xrv62 | Dest IP: 3.3.3.62
- TE RID: 3.3.3.62 | IPv6 RID: bb:bb:bb:3:3:62
- Color: 2000


The 'Summary' section provides additional details:

- Admin State: Up
- Oper State: Up
- Binding SID: 24013
- Policy Type: Local Congestion Mitigation
- Profile ID: 2021
- Description: -
- Traffic Rate: 198.93 Mbps
- Unused: False
- Delay: 1
- Accumulated Metric: 0
- Delegated PCE: 10.194.132.94
- Non-delegated PCEs: 10.194.132.93
- PCE Computed Time: 28-Aug-2023 04:59:16 PM PDT
- Last Update: 28-Aug-2023 04:59:19 PM PDT

## Step 5: Remove TTE SR policies on LCM Recommendation

After some time, the deployed TTE SR policies may no longer be needed. This occurs if utilization continues to stay under threshold without the LCM-initiated TTE policies. If this is the case, LCM generates new recommended actions to delete the TTE SR policy sets.

To remove the TTE SR policies upon LCM recommendation, follow the steps given below:

- Step 1** If needed: Display the topology map and click  in the **Actions** column. Choose **View Deployed Policies**.
- Step 2** Click **Commit All** to remove the previously deployed TTE SR policies.
- Step 3** Confirm the removal by viewing the topology map and SR Policy table.

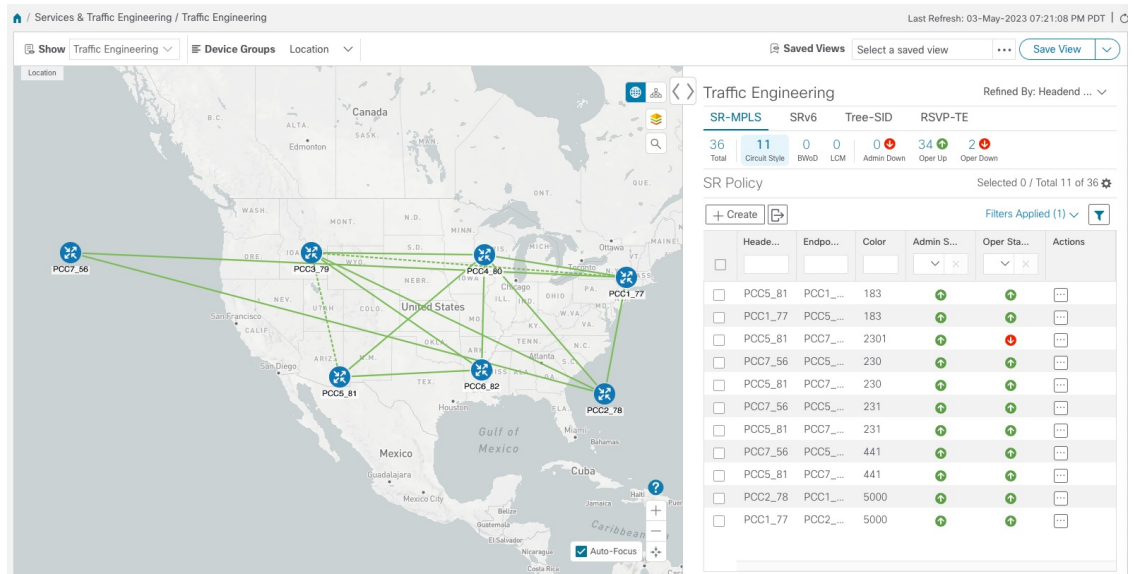
## LCM Scenario: Summary and Conclusion

In this scenario, we observed how to leverage LCM to alleviate traffic congestion in the network. LCM takes the manual tracking and calculation out of your hands but at the same time gives you control as to whether to implement the congestion mitigation recommendations, or not. You can preview the recommendations and see how the potential deployment will take effect in your network before you deploy them. As traffic changes, LCM tracks the deployed TTE SR policies and decides whether or not they are still needed. If not, LCM recommends deleting them.

## Scenario: Use CS-SR Policies to Reserve Bandwidth

In this scenario, we enable Circuit-Style Segment Routing Traffic Engineering (CS-SR, or CS SR-TE) policies and set bandwidth-reservation parameters, then configure a CS-SR policy and visualize it on the topology map. We will inspect the policy's details, including its computed Active (working) and Protected (protect) paths.

The examples in this scenario use the following topology:



The screenshot displays the Traffic Engineering interface. On the left, a topology map shows a network of nodes (PCCs) connected by links. The nodes are labeled with IDs such as PCC7\_56, PCC3\_79, PCC4\_80, PCC1\_77, PCC5\_81, PCC6\_82, and PCC2\_78. On the right, the SR Policy table is visible, showing a list of policies with columns for Name, Endpoints, Color, Admin Status, Oper Status, and Actions.

SR Policy	SRv6	Tree-SID	RSVP-TE
36 Total	11 Circuit Style	0 BwD	0 LCM
		0 Admin Down	34 Oper Up
			2 Oper Down

SR Policy	Headend	Endpoint	Color	Admin S...	Oper Sta...	Actions
<input type="checkbox"/>	PCC5_81	PCC1_...	183			...
<input type="checkbox"/>	PCC1_77	PCC5_...	183			...
<input type="checkbox"/>	PCC5_81	PCC7_...	2301			...
<input type="checkbox"/>	PCC7_56	PCC5_...	230			...
<input type="checkbox"/>	PCC5_81	PCC7_...	230			...
<input type="checkbox"/>	PCC7_56	PCC5_...	231			...
<input type="checkbox"/>	PCC5_81	PCC7_...	231			...
<input type="checkbox"/>	PCC7_56	PCC5_...	441			...
<input type="checkbox"/>	PCC5_81	PCC7_...	441			...
<input type="checkbox"/>	PCC2_78	PCC1_...	5000			...
<input type="checkbox"/>	PCC1_77	PCC2_...	5000			...

We will observe what happens when the Active bandwidth-reserved path between the NCS1 and NCS3 nodes fails. We will then re-optimize the failed path.

## CS-SR Scenario: Assumptions and Prerequisites

The following sections provide a list of high-level requirements for proper CS-SR operation, including requirements and constraints on the policy attribute values set in each CS-SR policy, and the processing logic followed during path reversions.

In addition to the constraints discussed in the following sections:

- The Crosswork Circuit Style Manager (CSM) feature pack is a feature of the Crosswork Network Automation Essential Suite. All licensed features are available during the 90-day trial period. After the trial period, you must have a license for Crosswork Optimization Engine to continue using CSM.
- Circuit-Style policy configuration was introduced with Crosswork Network Controller (CNC) 5.0. To use it, you must have version 7.9.1 (or later) of the Cisco IOS-XR Path Computation Client (PCC) installed on your devices. If you have been using a previous version of CNC with IOS-XR version 7.7.1 or earlier, please upgrade to version 7.9.1 or later before attempting to configure CS-SR policies.
- When using CSM with Crosswork Network Controller, the UI navigation starts from **Traffic Engineering & Services**. When using CSM with Crosswork Optimization Engine, the navigation starts from **Traffic Engineering**.

### CS Policy Attribute Constraints

In this scenario, we will build a CS policy between node NCS1 and node NCS 3. The policy will use the following settings and constraints:

- **PolicyName:** NCS1-NCS3
- **Headend Device:** NCS1
- **Headend IP Address:** 192.168.20.4
- **Tailend Device:** NCS3
- **Tailend IP Address:** 192.168.20.14
- **Color-choice:** 1000
- **Bandwidth:** 10000
- **path-protection:** Enabled
- **disjoint-path:** Enabled
- **disjoint-path forward-path type:** Link
- **disjoint-path forward-path group-id:** 531
- **disjoint-path reverse-path type:** Link
- **disjoint-path reverse-path group-id:** 5311
- **performance-measurement :** Enabled.
- **performance-measurement profile-type:** Liveness
- **performance-measurement liveness-detection:** Enabled
- **performance-measurement profile:** CS-active



- **working-path**: Enabled
- **working-path preference**: 100
- **working-path dynamic-path**: Enabled
- **working-path dynamic-path pce**: Enabled
- **working-path dynamic-path metric type**: **igp**
- **working-path dynamic-path bidirectional-association-choice**: Enabled
- **working-path dynamic-path bidirectional-association-id**: 230
- **working path dynamic constraints segments**: Enabled
- **working-path constraints segments protection**: **unprotected-only**
- **protect-path**: Enabled
- **protect-path preference**: 100
- **protect-path dynamic-path**: Enabled
- **protect-path dynamic-path pce**: Enabled
- **protect-path dynamic-path metric type**: **igp**
- **protect-path dynamic-path bidirectional-association-choice**: Enabled
- **protect-path dynamic-path bidirectional-association-id**: 231
- **protect-path dynamic constraints segments**: Enabled
- **protect-path constraints segments protection**: **unprotected-only**
- **restore-path**: Enabled
- **restore-path preference**: 100
- **restore-path dynamic-path**: Enabled
- **restore-path dynamic-path pce**: Enabled
- **restore-path dynamic-path metric type**: **igp**
- **restore-path dynamic-path bidirectional-association-choice**: Enabled
- **restore-path dynamic-path bidirectional-association-id**: 232
- **restore-path dynamic constraints segments**: Enabled
- **restore-path constraints segments protection**: **unprotected-only**

The following table shows all of the options you can choose from when building a policy. It is important to understand that the attributes described in the table act as constraints. Each of them corresponds to elements of the configuration that Cisco Crosswork uses to govern how Circuit-Style path hops are computed. Each value is effectively a path computation or optimization constraint, since they either specify a required property of a path or exclude possible choices for that path.

There are dependencies that must be met as well as combinations that are not allowed. The system will warn you when these sorts of issues arise. We encourage you to experiment to learn how to provision services in your network that match the types of services you want to deliver.

**Table 1: Supported Circuit Style SR-TE Policy Attribute Values and Constraints**

Attribute	Description
Policy Path Protection	The path protection constraint is required for both sides of a Circuit Style SR-TE policy.
Bandwidth Constraint	<p>The bandwidth constraint is required and must be the same on both sides of a Circuit Style SR-TE policy. Bandwidth changes can be made to existing policies, with these effects:</p> <ul style="list-style-type: none"> <li>• Once you configure the new bandwidth on both sides, Crosswork will evaluate the path. This <b>will not</b> result in a recomputed path.</li> <li>• If the new bandwidth is higher, Crosswork checks the existing path to ensure sufficient resources. If all currently delegated paths can accommodate the new bandwidth, Crosswork returns the same path with the new bandwidth value, indicating to the path computation client (PCC) that it was successful. If any of the current paths cannot accommodate the new bandwidth, it returns the old bandwidth value indicating that it was unsuccessful. This evaluation will not be retried unless the bandwidth is changed again.</li> <li>• If the bandwidth is lower, Crosswork returns the same path with the new bandwidth value to indicate to the PCC that it was successful.</li> </ul> <p>The user interface shows both the requested and reserved bandwidth under each candidate path when you view the policy details. These values can differ if the requested bandwidth is increased but there is insufficient available CS pool bandwidth along one or more of the paths.</p>
Candidate Paths and Roles	<p>The <code>Working</code> path is defined as the highest preference Candidate Path (CP).</p> <p>The <code>Protect</code> path is defined as the CP with the second highest preference.</p> <p>The <code>Restore</code> path is defined with the lowest preference CP. The headend must have <code>backup-ineligible</code> configured.</p> <p>CPs of the same role in each direction must have the same CP preference.</p>
Bi-Directional	<p>All paths must be configured as co-routed.</p> <p>Paths with the same role on both sides must have the same globally unique bi-directional association ID.</p>

Attribute	Description
Disjointness	<p>Working and Protect paths on the same PCC must be configured with a disjointness constraint using the same disjoint association ID and disjointness type.</p> <p>The disjointness association ID for a Working and Protect path pair in one direction must be unique when compared with the corresponding pair in the opposite direction.</p> <p>Only the <code>Node</code> and <code>Link</code> disjoint types are supported. The disjoint type used must be the same in both directions of the same policy.</p> <p>The Restore path must not have a disjointness constraint set.</p> <p>Crosswork follows strict fallback behavior for all Working and Protect path disjointness computations. This means that, if node type disjointness is configured but no path is available, Crosswork makes no automatic attempt to compute a less restrictive link type disjoint path.</p>
Metric Type	<p>Only the <code>TE</code>, <code>IGP</code> and <code>Latency</code> metric types are supported. The metric type used must match across Working, Protect and Restore paths in both directions.</p>
Segment Constraints	<p>All Working, Protect and Restore paths must have the following segment constraints:</p> <ul style="list-style-type: none"> <li>• <code>protection unprotected-only</code></li> <li>• <code>adjacency-sid-only</code></li> </ul> <p>To ensure persistence through link failures, configure static adjacency SIDs on all interfaces that might be used by Circuit Style policies.</p>
Supported Policy Changes	<p>The following constraints may be changed for an operationally "up" Circuit Style SR-TE policy that has been previously delegated:</p> <ul style="list-style-type: none"> <li>• Metric type</li> <li>• Disjoint type</li> <li>• MSD</li> <li>• Affinities</li> </ul> <p>Once configuration changes are made in a consistent manner across all CPs and both PCCs (for example: the new metric type is the same for all CPs and both sides), Crosswork will initiate a recompute, which can result in new Working, Protect and Restore paths.</p> <p>During any transitory period in which configurations are not in sync between paths on the same PCC or between PCCs, no path updates are sent to the PCCs.</p>

Attribute	Description
Path Computation	<p>Crosswork computes paths for circuit style policies only after a complete bi-directional, path-protected set of candidate paths has been delegated, including Working and Protect paths on both sides.</p> <p>Crosswork computes the Restore path only after the Working and Protect paths are down. The SR Circuit Style Manager feature pack configuration interface provides a configurable delay timer to control how long after Restore paths are delegated from both sides to wait before the path is computed. This delay allows topology and SR policy state changes to fully propagate to Crosswork, in cases where these changes triggered the Restore path delegation.</p> <p>Path computation is supported for Intra/Inter area/level and Intra/Inter IGP Domain (same AS).</p>
Reversion Behavior	<p>Reversion behavior is controlled by the configuration of the WTR lock timer option under the Protect and Revert paths (it is not relevant for the Working path):</p> <ul style="list-style-type: none"> <li>• No lock configuration: Revert after a default 5-minute lock</li> <li>• Lock with no duration specified: No reversion</li> <li>• Lock duration &lt;value&gt;: Revert after the specified number of seconds</li> </ul>

### Unsupported CS Policy Options

The following table lists the CS policy options, attributes and constraints that are not supported in this version of CSM.

**Table 2: Unsupported Circuit Style SR-TE Policy Options**

Attribute	Description
Unsupported Configurations	<p>The following configurations are not supported:</p> <ul style="list-style-type: none"> <li>• Metric-bounds</li> <li>• SID-Algo constraints</li> <li>• Partial recovery is not supported with 7.8.x.</li> <li>• State-sync configuration between PCEs of a high-availability pair. These are not required with Circuit Style SR-TE policies. Use of this feature may result in degraded performance.</li> <li>• Multiple Circuit Style SR-TE policies between the same nodes with the same color but different endpoint IPs.</li> </ul>

Attribute	Description
Unsupported Policy Changes	<p>The following configuration changes to a previously delegated and operationally "up" Circuit Style SR-TE policy are not supported:</p> <ul style="list-style-type: none"> <li>• CP preference</li> <li>• Disjoint Association ID</li> <li>• Bi-directional Association ID</li> </ul> <p>To change these configurations for an existing policy, you must first shut down the policy on both sides, make the change (complying with restrictions as detailed above in terms of consistency) and then "no shut" the policy.</p>
Unsupported Path Computation	Automatic re-optimization is not supported for any paths based on changes in topology, LSP state, or any periodic event. Path computation is not supported for Inter-AS.

### Path Reversion Logic

Path reversion depends on the initial state of the Working, Protect and Revert paths and the events affecting each path. The scenarios in the following table provide examples of typical reversion behavior.

**Table 3: Path Reversion Scenarios**

Initial State	Events	Behavior
Working path is down, Protect path is up/active	Working path comes back up	<ol style="list-style-type: none"> <li>1. Working path recovers to up/standby state.</li> <li>2. Each PCC moves the Working path to active after the WTR timer expires.</li> <li>3. Protect path moves to up/standby.</li> </ol>
Working path is down, Protect path is down, Revert path is up/active	Working path comes back up, then Protect path comes back up	<ol style="list-style-type: none"> <li>1. Working path recovers and goes to up/active state</li> <li>2. Revert path is removed</li> <li>3. Protect path recovers and goes to up/standby</li> </ol>

Initial State	Events	Behavior
Working path is down, Protect path is down, Revert path is up/active	Protect path comes back up, then Working path comes back up	<p>On side A: The Working path failure is local (the first Adj SID in the SegList is <b>invalid</b>):</p> <ol style="list-style-type: none"> <li>1. Protect path recovers and goes to up/active.</li> <li>2. Recover path is removed.</li> <li>3. Working path recovers and goes to up/standby.</li> <li>4. Each PCC moves the Working path to active after the WTR timer expires, Protect path goes to up/standby.</li> </ol> <p>On side Z: Working path failure is remote (first Adj SID in SegList is <b>valid</b>):</p> <ol style="list-style-type: none"> <li>1. Protect path recovers but is not brought up, Revert path remains up/active.</li> <li>2. Working path recovers and goes up/active.</li> <li>3. Revert path is removed.</li> <li>4. Protect path goes to up/standby.</li> </ol>

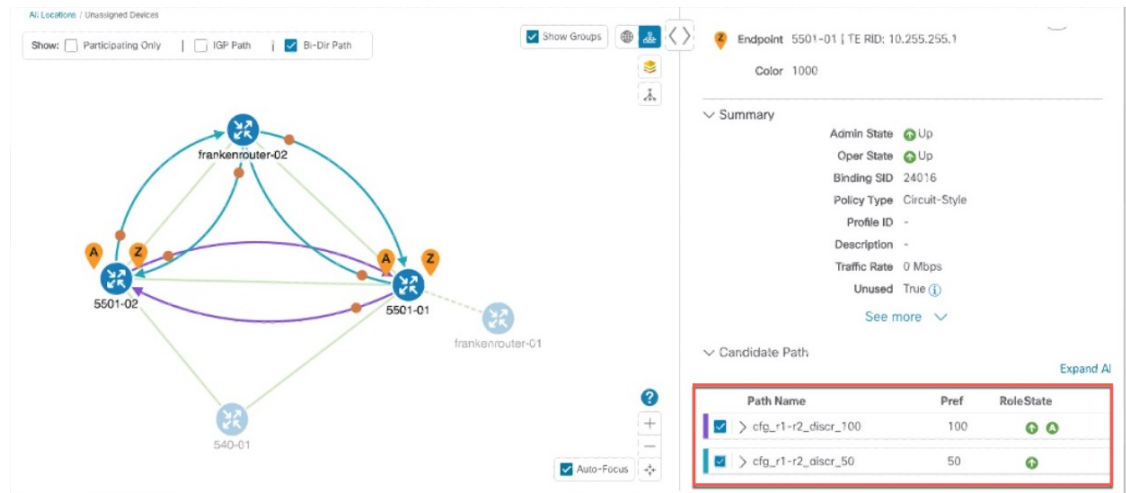
### What Happens When Path Failures Occur?

Cisco Crosswork computes paths for CS policies only after a complete bidirectional, path-protected set of candidate paths has been delegated. A path can be considered to have "failed" due to a variety of reasons, including transient changes in workloads caused by congestion elsewhere in the network, or any condition that causes the path not to meet bandwidth expectations. Irrespective of the cause, there are three types of paths used during these kinds of failures. Crosswork activates them as needed, according to their preference settings:

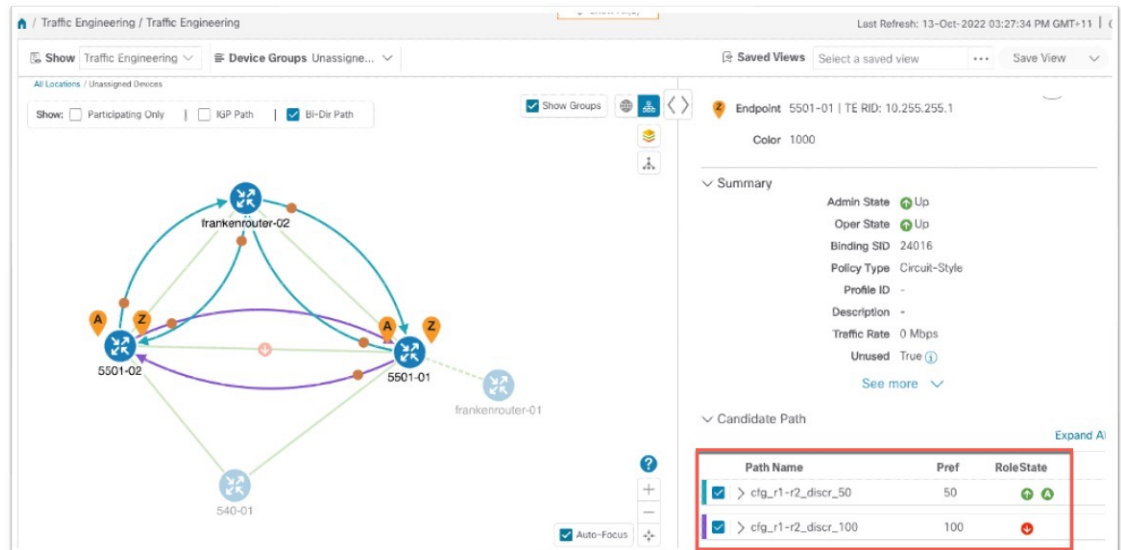
- **Working**—This is the path with the highest preference value. Crosswork always tries to keep the operational (Oper Up) path with the *highest* preference as the *Active* path.
- **Protected**—This is the path with the second highest preference. If the Working path goes down, the Protected path (with the lower preference value) is activated. After the Working path recovers, the Protected path remains active until the default lock duration expires, then the Working path is activated.
- **Restore**—This is the path with the lowest preference path. Crosswork computes the Restore path only when the Working and Protected paths are both down. You can control how long after Restore paths are delegated to wait before the path is computed. This delay allows topology and policy state changes to fully propagate through the network and gives Crosswork a chance to gather and analyze telemetry to determine network health.

To address failures effectively and switch from the Working to the Protected path, be sure to configure Performance Measurement (PM) as part of your CS policy. For more information, see [Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 35](#).

The following image shows that the Working and Protected paths of an example CS policy are operational. The *active* path is indicated by the "A" icon shown next to that path in the **State** column in the **Candidate Path** list.

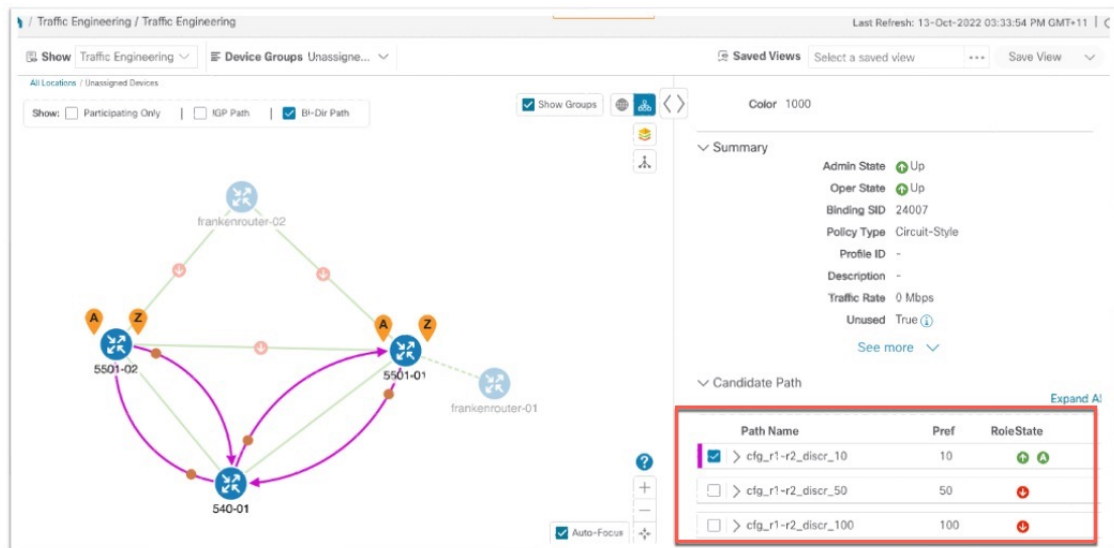


If the Working path performance falls below expectations, the Protected path becomes Active immediately (usually, under 50 milliseconds).



When the Working path comes back up, the Protected path resumes the Protected role again and the Working path (with preference 100) becomes Active again.

If both the Working and Protected paths go down, Crosswork calculates a Restore path and makes it the active path. Note that the Restore path has the lowest preference value of 10. The Restore path only appears in this particular case. If either the Working or Protected paths become operational again, Crosswork will activate them, and the Restore path will disappear from the topology map and from the Candidate Path list.



## CS-SR Scenario: Workflow

Workflow steps	Detailed procedure links
1. Enable the SR Circuit Style Manager (CSM) feature pack.	<a href="#">Step 1: Enable Circuit Style Manager, on page 25.</a>
2-4. Configure Circuit Style SR-TE policies on the devices.  <b>Note</b> If you haven't enabled the feature pack, the Circuit Style SR-TE policies you configure will appear operationally down.	You can configure Circuit Style SR-TE policies using any of the following methods: <ul style="list-style-type: none"> <li>• On the device, using the CLI. See <a href="#">Step 2: Configure Circuit Style SR-TE Policies Using Device CLI, on page 30</a></li> <li>• Using the user interface. See <a href="#">Step 3: Configure Circuit Style SR-TE Policies Using Add, on page 33</a></li> <li>• Import a JSON or XML file. See <a href="#">Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 35</a></li> </ul>
5. Verify that the Circuit Style SR-TE policy appears in the SR Policy table and on the topology map.	See <a href="#">Step 5: View Circuit Style SR-TE Policies on the Topology Map, on page 38</a>
6. Verify that the reserved bandwidth pool settings you defined in Step 1 are configured properly.	See <a href="#">Step 6: Verify Circuit Style SR-TE Policy Bandwidth Utilization, on page 42.</a>
7. Trigger path re-computation after path failures.	See <a href="#">Step 7: Trigger Circuit Style SR-TE Path Recomputation, on page 43.</a>



## Step 1: Enable Circuit Style Manager

In order to manage and visualize Circuit Style SR-TE policies on the topology map, we must first enable SR Circuit Style Manager (CSM) and set bandwidth reservation settings. As soon as you define these settings, CSM computes the best bidirectional failover paths between the two nodes, while observing the requested CSM bandwidth and threshold settings, and the constraints defined in the Circuit Style SR-TE policy. The following steps show how to do this.

CSM tries to ensure that the total reserved bandwidth on all interfaces remains at or below the network-wide resource pool. When the total usage on all interfaces exceeds the threshold value you set, CSM generates a threshold-crossing alarm.

To help you estimate Circuit Style SR-TE bandwidth pool and threshold settings that are reasonable for your organization's implementation, this topic provides two examples showing how CSM handles policies that exceed either the bandwidth pool size or both the pool size and alarm threshold. For the purposes of this scenario, you can enter either one of these examples, or choose settings less likely to be exceeded in a practical implementation.

After enabling CSM, you will need to create Circuit Style SR-TE policy configurations. You can use any of the following methods to create Circuit Style SR-TE policies. In this scenario, we will create the same policy each time, but we will go through each method in order, so that you can decide which methods will best meet your needs:

- [Step 2: Configure Circuit Style SR-TE Policies Using Device CLI, on page 30](#)
- [Step 3: Configure Circuit Style SR-TE Policies Using Add, on page 33](#)
- [Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 35](#)

- Step 1** From the main menu, choose **Services & Traffic Engineering > Circuit Style SR-TE > Configuration > Basic**.
- Step 2** Toggle the **Enable** switch to **True**.

Circuit Style SR-TE

The screenshot shows the configuration page for Circuit Style SR-TE. It has two tabs: 'Basic' and 'Advanced'. Under the 'Basic' tab, there are three main configuration areas:

- Enable:** A toggle switch currently set to 'True' (indicated by a blue circle).
- Link CS BW Pool Size:** A text input field containing '10' with a percentage sign, and a range indicator '0 to 100%' below it.
- Link CS BW Min Threshold:** A text input field containing '80' with a percentage sign, and a range indicator '0 to 100%' below it.

At the bottom of the configuration area, there are three buttons: 'Commit Changes' (highlighted in blue), 'Get Default Values', and 'Discard Changes'.

- Step 3** Enter the required bandwidth pool size and threshold information, as explained in the table below. See also the examples below, and choose one of them to enter.

Field	Description
Link CS BW Pool Size	The percentage of each link's bandwidth reservable for Circuit Style SR-TE policies.
Link CS BW Min Threshold	The Link CS BW Pool utilization percentage beyond which Crosswork will generate a threshold-crossing event notification.

**Step 4** Click **Commit Changes** to save the Basic configuration.

**Step 5** (Optional): Click the **Advanced** tab to display additional CS-SR configuration values.

Circuit Style SR-TE

Configuration

Basic **Advanced**

Validation Interval \* Ⓞ Sec  
10  
5 to 3600 seconds

Timeout \* Ⓞ Sec  
300  
30 to 600 seconds

Restore Delegation Delay \* Ⓞ Sec  
5  
1 to 60 seconds

Debug Optimizer

Debug Optimizer Ⓞ  
False  True

Debug Optimization Max Files \* Ⓞ  
30  
0 to 1024

**Commit Changes** **Get Default Values** **Discard Changes**

a) Change the values on the **Advanced** tab as explained in the table below.

Field	Description
Validation Interval	This is the interval that CSM will wait before the bandwidth that is reserved for an un-delegated policy is returned to the Circuit Style SR-TE policy bandwidth Pool.
Timeout	The duration CSM will wait for the delegation request, before generating a threshold-crossing alarm.
Restore Delegation Delay	The duration CSM will pause before processing a restore path delegation.
Debug Optimizer	Toggle the switch to <b>True</b> to turn on the Debug Optimizer for all CS-SR policies. The Debug Optimizer will write log files to the Crosswork file system whenever it calculates routes, up to the maximum number of files you specify.
Debug Optimization Max Files	Enter the maximum number of log files the Debug Optimizer will write. Once the maximum is reached, the Optimizer will overwrite existing files.

b) When you are finished entering Advanced configuration values, click **Commit Changes** to save the configuration.

## Example

### Example: Bandwidth Utilization Surpasses Defined Threshold

In this example, we assume the reserved bandwidth settings are as follows:

- Bandwidth Pool Size: 10%
- Bandwidth Pool Threshold: 1%

Our two nodes have 10 Gbps Ethernet interfaces, so the bandwidth pool size with these settings is 1Gbps and the alarm threshold is 100 Mbps.

1. We create a CS policy connecting node 5501-02 to node 5501-01 (r02 - r01), with a bandwidth of 100 Mbps.

Link Details 🗑️ ✕

Summary **Traffic Engineering**

**General** SR-MPLS SRv6 Tree-SID RSVP-TE

	A Side	Z Side
Node	5501-02	5501-01
IF Name	TenGigE0/0/0/0	TenGigE0/0/0/0
FA Affi...		
FA Top...		
∨ Circuit...		
Pool ...	1000 Mbps	1000 Mbps
Used	10 Mbps	10 Mbps
Avail...	990 Mbps	990 Mbps

2. Later, the requested bandwidth for the policy increases to 500 Mbps. The updated CS policy is created and operational (Oper State Up).

Link Details 🗑️ | ✕

Summary **Traffic Engineering**

**General** SR-MPLS SRv6 Tree-SID RSVP-TE

	A Side	Z Side
Node	5501-02	5501-01
IF Name	TenGigE0/0/0/0	TenGigE0/0/0/0
FA Affi...		
FA Top...		
∨ Circuit...		
Pool ...	1000 Mbps	1000 Mbps
Used	500 Mbps	500 Mbps
Avail...	500 Mbps	500 Mbps

3. Since the bandwidth utilization of 500 Mbps with the updated policy is greater than the configured bandwidth threshold (100 Mbps), Crosswork triggers alerts.

Optima CSM App	⚠️ Warning	Bandwidth pool allocation (500.000) exceeds pool threshold (100.00) for frankenrouter-02   TenGigE0/0/0/21
Optima CSM App	⚠️ Warning	Bandwidth pool allocation (500.000) exceeds pool threshold (100.00) for frankenrouter-02   TenGigE0/0/0/20
Optima CSM App	⚠️ Warning	Bandwidth pool allocation (500.000) exceeds pool threshold (100.00) for 5501-02   TenGigE0/0/0/2
Optima CSM App	⚠️ Warning	Bandwidth pool allocation (500.000) exceeds pool threshold (100.00) for 5501-02   TenGigE0/0/0/0
Optima CSM App	⚠️ Warning	Bandwidth pool allocation (500.000) exceeds pool threshold (100.00) for 5501-01   TenGigE0/0/1/0/1
Optima CSM App	⚠️ Warning	Bandwidth pool allocation (500.000) exceeds pool threshold (100.00) for 5501-01   TenGigE0/0/0/0

### Example: Bandwidth Pool Size and Usage Exceeded

In this example, we assume the reserved bandwidth settings are as follows:

- Bandwidth Pool Size: 10%
- Bandwidth Pool Threshold: 10%

The bandwidth pool size for the 10 Gbps Ethernet interfaces is 1Gbps and the alarm threshold is 100 Mbps.

1. An existing CS-SR policy from node 5501-02 to node 5501-01 (*r02- r01*) uses a bandwidth of 500 Mbps.
2. Later, a new policy requiring a bandwidth of 750 Mbps with a path from node 5501-02 to node 5501-01 to 5501-2 (*r02- r01- r2*) is requested. Since the existing policy and this new policy together exceed the bandwidth pool size and alarm threshold of 1 Gbps (750 Mbps + 500 Mbps = 1250 Mbps), the following behaviors occur:
  - The new CS-SR policy *r02- r01- r2* is created but not operational (Oper State Down).

Endpoint 5501-01 | TE RID: 10.255.255.1

Color 2000

---

Summary

- Admin State ↑ Up
- Oper State ↓ Down
- Binding SID 0
- Policy Type Circuit-Style
- Profile ID -
- Description -
- Traffic Rate 0 Mbps
- Unused True i

[See more](#) v

---

Candidate Path

Path Name	Pref	RoleState
<input checked="" type="checkbox"/> > cfg_r1-r2-2_discr_100	100	<span style="color: red;">↓</span> <span style="color: green;">A</span>
<input type="checkbox"/> > cfg_r1-r2-2_discr_50	50	<span style="color: red;">↓</span>

- Alerts are triggered.

Source	Severity	Description
Optima CSM App	<span style="color: blue;">⚠</span> Warning	Unable to compute path for 10.255.255.1 <-> 10.255.255.2   color 2000 due to CsmUpdateStatus.NO_PATH
SR Policy [10.255.255.2#10.255.255.1]	<span style="color: blue;">⚠</span> Warning	Policy 'srte_c_2000_ep_10.255.255.1' has operational status as DOWN.
SR Policy [10.255.255.1#10.255.255.2]	<span style="color: blue;">⚠</span> Warning	Policy 'srte_c_2000_ep_10.255.255.2' has operational status as DOWN.

3. Later, the CS-SR policy *r02- r01- r2* is updated and only requires 10 Mbps. The following behaviors occur:

- Since the total bandwidth required for the two policies (10 Mbps + 500 Mbps = 510 Mbps) now requires less than the bandwidth pool size (1Gbps), CS-SR policy *r02- r01- r2* becomes operational (Oper State Up).

## Step 2: Configure Circuit Style SR-TE Policies Using Device CLI

Endpoint 5501-01 | TE RID: 10.255.255.1

Color 2000

Summary

Admin State ↑ Up  
 Oper State ↑ Up  
 Binding SID 24005  
 Policy Type Circuit-Style  
 Profile ID -  
 Description -  
 Traffic Rate 0 Mbps  
 Unused True i  
[See more](#) v

Candidate Path

Path Name	Pref	RoleState
<input type="checkbox"/> > cfg_r1-r2-2_discr_50	50	<span style="color: green;">↑</span>
<input checked="" type="checkbox"/> > cfg_r1-r2-2_discr_100	100	<span style="color: green;">↑</span> <span style="color: green;">A</span>

- Since the bandwidth utilization (10 Mbps) with the updated policy is below the configured bandwidth threshold (1 Gbps), alerts are cleared.

Source	Severity	Description
SR Policy [10.255.255.1#10.255.255.1]	<span style="color: green;">✔</span> Clear	Policy 'srte_c_2000_ep_10.255.255.2' has operational status back to UP.
SR Policy [10.255.255.2#10.255.255.1]	<span style="color: green;">✔</span> Clear	Policy 'srte_c_2000_ep_10.255.255.1' has operational status back to UP.

## Step 2: Configure Circuit Style SR-TE Policies Using Device CLI

Prior to Cisco Crosswork, most network engineers created Circuit Style SR-TE policies directly on the devices themselves, using the appropriate network operating system CLI commands. This step of the scenario covers direct CLI policy configuration for a Cisco device. We present it only because this is a legitimate way to create these policies, and so you can see how the configuration implemented using this method matches the configuration for the other, Crosswork-native methods presented in this scenario.

Crosswork Network Controller's topology discovery will automatically recognize CS policy configurations implemented directly on devices, and will help you visualize them on the topology map. However, this method has some important drawbacks. To start with, you will need to be familiar with the CLI commands required to configure Circuit Style SR-TE policies properly. More importantly, Crosswork can *discover* Circuit Style SR-TE policies configured directly on a device, but cannot change or delete them. We encourage you to use instead the **Add** or **Import** methods, which allow you to manage and change your configuration using Crosswork. For help using these methods, skip this step and go on to [Step 3: Configure Circuit Style SR-TE Policies Using Add, on page 33](#) or to [Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 35](#).

A Circuit Style SR-TE policy configuration must include the destination endpoint, the amount of requested bandwidth, and the bidirectional attribute. See [CS-SR Scenario: Assumptions and Prerequisites, on page 16](#) for additional requirements and notable constraints.

When configuring Circuit Style SR-TE policies directly on Cisco devices, make sure the configuration includes a Performance Measurement (PM) Liveness profile. A PM Liveness profile enables proper detection of candidate path liveness and effective path protection. Path Computation Clients (PCCs) do not validate past the first SID, so without PM Liveness, the path protection will not occur if the failure in the Circuit Style SR-TE policy candidate path occurs after the first hop in the segment list. Crosswork supports software-based and hardware-offload PM Liveness configuration methods. For more background on PM Liveness profiles and methods, see [Configuring SR Policy Liveness Monitoring](#).

**Step 1** Use your preferred method to access the head-end device console and log in.

**Step 2** If applicable, enable the hardware module on the device for PM configuration.

**Example:**

```
hw-module profile offload 4
reload location all
```

**Step 3** Configure the Performance Measurement (PM) Liveness profile on the device. The following example uses a hardware-offload configuration.

**Example:**

```
performance-measurement
  liveness-profile sr-policy name CS-active-path
    probe
      tx-interval 3300
  !
  npu-offload enable    !! Required for hardware Offload only
  !
  !
  liveness-profile sr-policy name CS-protected-path
    probe
      tx-interval 3300
  !

npu-offload enable    !! Required for hardware Offload only
!
!
!
```

**Step 4** Configure the Circuit Style SR-TE policy. All configuration entries shown are required in order for the Crosswork CSM feature pack to manage the policy. Entry values that you must change appropriately for your network (or for your PM Liveness profile) are shown in *italics*. See [CS-SR Scenario: Assumptions and Prerequisites, on page 16](#) for additional requirements and notable constraints.

**Example:**

```
segment-routing
  traffic-eng
    policy NCS1-NCS3

    performance-measurement
      liveness-detection
        liveness-profile backup name CS-protected    !! Name must match liveness profile defined for
        Protect path
```

```

    liveness-profile name CS-active                !! Name must match liveness profile defined for
Active path
!
!
bandwidth 10000
color 1000 end-point ipv4 192.168.20.4
path-protection
! Path protection is required on both ends of the candidate-paths
! Defining the Working path. Must have the highest CP preference
preference 100
  dynamic
    pcep
    !
    metric
      type igp
    !
  !
  constraints
    segments
      protection unprotected-only
      adjacency-sid-only
    !
    disjoint-path group-id 3 type node
  !
  bidirectional
    co-routed
    association-id 230
!
! Defining the Protect path. Must have second highest CP preference.
preference 50
  dynamic
    pcep
    !
    metric
      type igp
    !
  !
  constraints
    segments
      protection unprotected-only
      adjacency-sid-only
    !
    disjoint-path group-id 3 type node
  !
  bidirectional
    co-routed
    association-id 231
! Defining the restore path. It must have both the lowest CP preference and backup-ineligible
setting
preference 10
  dynamic
    pcep
    !
    metric
      type igp
    !
  !
  backup-ineligible
  !

  constraints
    segments
      protection unprotected-only
      adjacency-sid-only

```




```
!
!
bidirectional
  co-routed
  association-id 232
!
!
!
!
!
!
!
```

### Step 3: Configure Circuit Style SR-TE Policies Using Add

You can create a Circuit Style SR-TE policy between any two nodes using the Crosswork Network Controller **Add** function. This method is the simplest for users who want to be able to use Crosswork to edit or delete the Circuit Style SR-TE policies they create.

This method doesn't completely eliminate the need to be familiar with the CLI command attributes needed to configure Circuit Style SR-TE policies properly. If you prefer a faster method that can also help you to standardize these policies across your network, skip this step and use the method in [Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 35](#).

- Step 1** From the main menu, choose **Services & Traffic Engineering > Provisioning (NSO)**.
- Step 2** In the **Services/Policies** column on the left, select **SR-TE > Circuit-Style Policy**. Crosswork displays the **Create SR-TE > Circuit Style Policy** window.
- Step 3** Click . Crosswork displays the **Create SR-TE > Circuit Style Policy** window.
- Step 4** In this scenario, we will use the name **NCS1-NCS3**. Enter that name in the **Name** field, then click **Continue**.
- Step 5** Begin by making the following entries in the respective fields on the **Create SR-TE > Circuit Style Policy**:
- **Name:** **NCS1-NCS3**
  - **Color-choice:** **1000**
  - **Bandwidth:** **10000**
  - **path-protection:** Check the checkbox.
- Note** The color-choice and bandwidth values shown here are examples only. If you decide to follow this example in your network, be sure to use a color-choice value that is not already in use, and a bandwidth value that is available within the percentage you are dedicating to CS policies.
- Step 6** Continue the scenario by entering the Circuit Style SR-TE policy constraints and specifications shown in the table below. The user interface for the **Add** function groups policy fields into related categories. Click on the field group name or the > icon at the right to expand a category and display its dependent fields.

You will need to change the device names and IP addresses you enter to match actual devices on your network.

**Table 4: Example: Circuit Style SR-TE Policy Using Add**

Expand this:	To specify this:
head-end	<ul style="list-style-type: none"> <li>• <b>Device:</b> Enter <b>NCS1</b>.</li> <li>• <b>Ip-address:</b> Enter <b>192.168.20.4</b>.</li> </ul>
tail-end	<ul style="list-style-type: none"> <li>• <b>Device:</b> Enter <b>NCS3</b>.</li> <li>• <b>Ip-address:</b> Enter <b>192.168.20.14</b>.</li> </ul>
disjoint-path	Click <b>Enable disjoint-path</b> .
disjoint-path > forward-path	<ul style="list-style-type: none"> <li>• <b>Type:</b> Select <b>Link</b>.</li> <li>• <b>group-id:</b> Enter <b>531</b>.</li> </ul>
disjoint-path > reverse-path	<ul style="list-style-type: none"> <li>• <b>Type:</b> Select <b>Link</b>.</li> <li>• <b>group-id:</b> Enter <b>5311</b>.</li> </ul>
performance-measurement	Click <b>Enable performance-measurement</b> .
performance-measurement > Profile-type	Click <b>liveness</b> .
performance-measurement > Profile-type > liveness-detection	Click <b>Enable liveness-detection</b> . Then: <ul style="list-style-type: none"> <li>• <b>Profile:</b> Enter <b>CS-active</b>.</li> <li>• <b>Backup:</b> Enter <b>CS-protected</b>.</li> </ul>
working-path	Click <b>Enable working-path</b> . Then select <b>dynamic-path</b> .
working path > dynamic	Click <b>Enable dynamic-path</b> . Then: <ul style="list-style-type: none"> <li>• <b>pce:</b> Check the checkbox.</li> <li>• <b>Metric-type:</b> Select <b>igp</b></li> <li>• <b>Bidirectional-association-choice:</b> Select <b>bidirectional-association-id</b> and enter <b>230</b> in the field.</li> </ul>
working path > dynamic > constraints > segments	Click <b>Enable segments</b> . Then in the <b>Protection</b> field, select <b>unprotected-only</b> .
protect-path	Click <b>Enable protect-path</b> . Then select <b>dynamic-path</b> .

Expand this:	To specify this:
protect-path > dynamic	Click <b>Enable dynamic</b> . Then: <ul style="list-style-type: none"> <li>• <b>pce</b>: Check the checkbox.</li> <li>• <b>Metric-type</b>: Select <b>igp</b></li> <li>• <b>Bidirectional-association-choice</b>: Select <b>bidirectional-association-id</b> and enter <b>231</b> in the field.</li> </ul>
protect-path > dynamic > constraints > segments	Click <b>Enable segments</b> . Then in the <b>Protection</b> , field, select <b>unprotected-only</b> .
restore-path	Click <b>Enable restore-path</b> . Then select <b>dynamic-path</b> .
restore-path > dynamic	Click <b>Enable dynamic-path</b> . Then: <ul style="list-style-type: none"> <li>• <b>pce</b>: Check the checkbox.</li> <li>• <b>Metric-type</b>: Select <b>igp</b></li> <li>• <b>Bidirectional-association-choice</b>: Select <b>bidirectional-association-id</b> and enter <b>232</b> in the field.</li> </ul>
restore-path > dynamic > constraints > segments	Click <b>Enable segments</b> . Then in the <b>Protection</b> field, select <b>unprotected-only</b> .

**Step 7** When you are finished, click **Dry Run** to validate your changes and save them. Crosswork will display your changes in a popup window.

If you want to configure a service that has requirements that do not match those we describe in this example, contact Cisco Customer Experience.

**Step 8** When you are ready to activate the policy, click **Commit Changes**.

## Step 4: Configure Circuit Style SR-TE Policies Using Import

If your organization has already implemented Circuit Style SR-TE policies and wants to roll them out on more network devices, the easiest way to do so is using Crosswork Network Controller's **Import** function. You can use **Import** to download a policy template file from Crosswork. The template file will be in JSON or XML format. You can save the template under a new name, insert the policy values of your choice, and then import the modified file.

As well as being fast, using the **Import** function is a good way to standardize Circuit Style SR-TE policies across your network. You can set the same template files to establish CS-SR policies between multiple pairs of devices, varying only the endpoint names and addresses, and any other values as appropriate for each circuit.

**Step 1** From the main menu, choose **Services & Traffic Engineering > Provisioning (NSO)**.

**Step 2** In the **Services/Policies** column on the left, select **SR-TE > Circuit-Style Policy**.

- Step 3** Click [📄](#). Then click the **Download sample JSON and XML files (.zip)** link. The downloaded ZIP file contains templates for all the Crosswork service types, including Circuit-Style, in JSON and XML formats.
- Step 4** Unzip `samplePayload.zip` and locate the `CS-Policy.json` and `CS-Policy.xml` template files.
- Step 5** Using the [JSON](#) or [XML](#) file editor of your choice, open the `CS-Policy` template file and save it under the name **cs1-cs4**.
- Step 6** If you are using the JSON template file, edit it so that it looks like the example below. If you are using the XML template, go on to the next step.

**Example:****CS-SR Policy in JSON**

```
{
  "name": "NCS1-NCS3",
  "head-end": {
    "device": "NCS1",
    "ip-address": "192.168.20.4"
  },
  "tail-end": {
    "device": "NCS3",
    "ip-address": "192.168.20.14"
  },
  "color": 1000,
  "bandwidth": 10000,
  "disjoint-path": {
    "forward-path": {
      "type": "Link",
      "group-id": 531
    },
    "reverse-path": {
      "type": "Link",
      "group-id": 5311
    }
  },
  "performance-measurement": {
    "profile-type": "liveness", {
      "profile": "CS-active",
      "backup": "CS-protected"
    }
  },
  "path-protection": {},
  "working-path": {
    "dynamic": {
      "constraints": {
        "segments": {
          "protection": "unprotected-only"
        }
      },
      "pce": {},
      "metric-type": "igp",
      "bidirectional-association-id": 230
    }
  },
  "protect-path": {
    "dynamic": {
      "constraints": {
        "segments": {
          "protection": "unprotected-only"
        }
      },
      "pce": {},
      "metric-type": "igp",

```

```

        "bidirectional-association-id": 231
    },
    "revertive": true
},
"restore-path": {
  "dynamic": {
    "constraints": {
      "segments": {
        "protection": "unprotected-only"
      }
    },
    "pce": {},
    "metric-type": "igp",
    "bidirectional-association-id": 232
  }
}
}
}

```

**Step 7** If you are using the XML template file, edit it so that it looks like the example below.

**Example:**

**CS-SR Policy in XML**

```

<config xmlns="http://tail-f.com/ns/config/1.0">
  <cs-sr-te-policy xmlns="http://cisco.com/ns/nso/cfp/cisco-cs-sr-te-cfp">
    <name>NCS1-NCS3</name>
    <head-end>
      <device>cs1</device>
      <ip-address>192.168.20.4</ip-address>
    </head-end>
    <tail-end>
      <device>cs4</device>
      <ip-address>192.168.20.14</ip-address>
    </tail-end>
    <color>1000</color>
    <bandwidth>10000</bandwidth>
    <disjoint-path>
      <forward-path>
        <type>Link</type>
        <group-id>531</group-id>
      </forward-path>
      <reverse-path>
        <type>Link</type>
        <group-id>5311</group-id>
      </reverse-path>
    </disjoint-path>
    <performance-measurement>
      <profile-type>liveness
        <profile>CS-active</profile>
        <backup>CS-protected</backup>
      </profile-type>
    </performance-measurement>
    <path-protection></path-protection>
    <working-path>
      <dynamic>
        <constraints>
          <segments>{
            <protection>unprotected-only</protection>
          </segments>{
        </constraints>{
          <pce></pce>
          <metric-type>igp</metric-type>
          <bidirectional-association-id>230</bidirectional-association-id>
        </dynamic>
      </working-path>
    </path-protection>
  </cs-sr-te-policy>
</config>

```


## Step 5: View Circuit Style SR-TE Policies on the Topology Map

```

</working-path>
<protect-path>
  <dynamic>
    <constraints>
      <segments>
        <protection>unprotected-only</protection>
      </segments>
    </constraints>
  </dynamic>
</protect-path>
<restore-path>
  <dynamic>
    <constraints>
      <segments>
        <protection>unprotected-only</protection>
      </segments>
    </constraints>
  </dynamic>
</restore-path>
</cs-sr-te-policy>
</config>

```

**Step 8** When you have finished editing the file and saved your changes, navigate to **Services & Traffic Engineering > Provisioning > SR-TE > Circuit-Style Policy** again.

**Step 9** Click  again. In the **File Name** field, enter the path to and file name of your modified template file, or click **Browse** to locate and select it. Then click **Import**.

## Step 5: View Circuit Style SR-TE Policies on the Topology Map

Next, we'll use Crosswork to visualize the NCS1-NCS3 Circuit Style SR-TE policy and isolate it on the map. To make this step more realistic and demonstrate how to focus on just one policy, the scenario assumes that we have multiple active Circuit Style SR-TE policies, not just the policy we created. We'll also view the Circuit Style SR-TE policy details, including endpoints, bandwidth constraints, IGP metrics, and candidate (Active/Working and Protect) paths.

**Step 1** From the main menu, choose **Services & Traffic Engineering > Traffic Engineering > SR-MPLS**. Then click **Circuit Style**.

Traffic Engineering Refined By: Headend or E... ▾

SR-MPLS	SRv6	Tree-SID	RSVP-TE
90 Total	6 Circuit Style	2 BWoD	0 LCM
		0 ↓ Admin Down	31 ↑ Oper Up
			59 ↓ Oper Down

The **SR Policy** table lists all of the Circuit Style SR-TE policies.

**Step 2** From the **Actions** column, click **Circuit Style SR-TE > View Details** for one of the Circuit Style SR-TE policies.

**Note** You cannot edit or remove Circuit Style SR-TE policy configurations that have been created directly on the device.

The screenshot shows the Traffic Engineering interface. On the left is a topology map of the San Francisco Bay Area with nodes like xrv9k-14, xrv9k-16, xrv9k-15, and xrv9k-17. A path is highlighted in purple. On the right is the SR Policy list:

SR-MPLS	SRv6	Tree-SID	RSVP-TE
90	6	2	0
Total	Circuit Style	BWd	LCM
0	0	0	0
	Admin Down	Oper Up	Oper Down
31	59		

Below the summary is the SR Policy list table:

Head...	Endp...	Color	Admin...	Oper St...	Actions
<input checked="" type="checkbox"/>	xrv9k-16	xrv9k-15	11056	+	+
<input type="checkbox"/>	xrv9k-15	xrv9k-16	11056	+	+
<input type="checkbox"/>	xrv9k-16	xrv9k-15	4294...	+	+
<input checked="" type="checkbox"/>	xrv9k-15	xrv9k-16	4294...	+	+
<input checked="" type="checkbox"/>	xrv9k-...	xrv9k-12	5600	+	+
<input checked="" type="checkbox"/>	xrv9k-12	xrv9k-...	5600	+	+

The **Circuit Style Policy Details** window is displayed in the side panel. By default, the Active path is displayed in the topology map and shows the bidirectional paths (Bi-Dir Path checkbox is checked) on the topology map. The Candidate Path list displays the Active (path that currently takes traffic) and Protected paths.

The screenshot shows the Circuit Style Policy Details window. On the left is a topology map of the Fremont area with nodes xrv9k-23 and xrv9k-25. A path is highlighted in purple. On the right is the details panel:

**Current**

- Headend:** xrv9k-25 | TE RID: 192.168... | PCC IP: 192.168... | Source IP: 192.168...
- Endpoint:** xrv9k-23 | TE RID: 192.168... | Dest IP: 192.168... | Color: 6905

**Performance Metrics**

- Traffic Rate: 0 Mbps avg.

**Summary**

**Candidate Path**

Path Name	Pref	Role	State
<input checked="" type="checkbox"/> cfg_srte_c_6905_ep_192.16...	100	+	+
<input type="checkbox"/> cfg_srte_c_6905_ep_192.16...	50	+	+

**Note** The Bandwidth Constraint value can differ from the bandwidth you requested if the value was increased and insufficient resources existed to satisfy demand on all Active and Protected candidate paths.

**Step 3** View Candidate path configuration details.

a) The **Circuit Style Policy Details** window allows you to drill down to view more information about the candidate paths. The operational (Oper State Up) candidate path with the highest preference will always be the Active path. In this example, the Protected path (with preference 50) is currently the Active path and is displayed on the topology map. Notice that it is designated with a green "A" icon under State to clearly indicate it is currently the operational Active path. Click **Expand All** to view more information about both paths.

## Step 5: View Circuit Style SR-TE Policies on the Topology Map

The screenshot shows a network topology map on the left and a 'Circuit Style Policy Details' panel on the right. The map displays three paths between two nodes labeled 'avw-25' and 'avw-26'. The paths are color-coded: a purple link (highest preference), a blue link (second preference), and a pink link (third preference). The right panel shows the details for the selected path (the pink one, which is highlighted with a red box in the image). The details include:

Path Name	Pref	Role	State
<input type="checkbox"/> cfg_srte_c_6905_ep_192.168.0.23...	100		<span style="color: red;">●</span>
<input checked="" type="checkbox"/> cfg_srte_c_6905_ep_192.168.0.23...	90		<span style="color: green;">●</span>
<input type="checkbox"/> cfg_srte_c_6905_ep_192.168.0.23...	50		<span style="color: green;">●</span>

The details for the selected path (Pref 90) are:

- Path Name: `cfg_srte_c_6905_ep_192.168.0.23_discoz_100`
- Oper State: ● Down
- Metric Type: IGP
- Bandwidth: Requested: 9.006 Mbps, Reserved: 0 Mbps
- Bi-Dir Association ID: 5906
- Disjoint Group: ID: 453, Association Source: 0.0.0.0, Type: Node-disjoint
- PCE Initiated: false
- Affinity: Exclude-Any: -, Include-Any: -, Include-All: -
- Segment Type: Unprotected
- SID Algorithm: -

- Note**
- First preference paths are shown as purple links.
  - Second preference paths are shown as blue links.
  - Third preference paths are shown as pink links.

If the Circuit Style SR-TE policy configuration was done through the UI, you have the option to view the Circuit Style SR-TE policy configuration. To see the configuration, click the link next to **Config ID**. For example:



Circuit Style Policy Details

Current History

Path Name	Pref	Role	State
<input checked="" type="checkbox"/> cfg_srte_c_6905_ep_192.168....	100		<span style="color: green;">↑</span> <span style="color: green;">A</span>

**Path Name** cfg\_srte\_c\_6905\_ep\_192.168.0.25\_disc

**Oper State** ↑ Up | A Active

**Metric Type** IGP

**Bandwidth** Requested: 9.006 Mbps  
Reserved: 0 Mbps

**Bi-Dir Association ID** 5906

**Config ID** [CS-CS-SR-WP-601-head-end-internal](#)


**Disjoint Group** ID: 567  
Association Source: 0.0.0.0  
Type: Node-disjoint

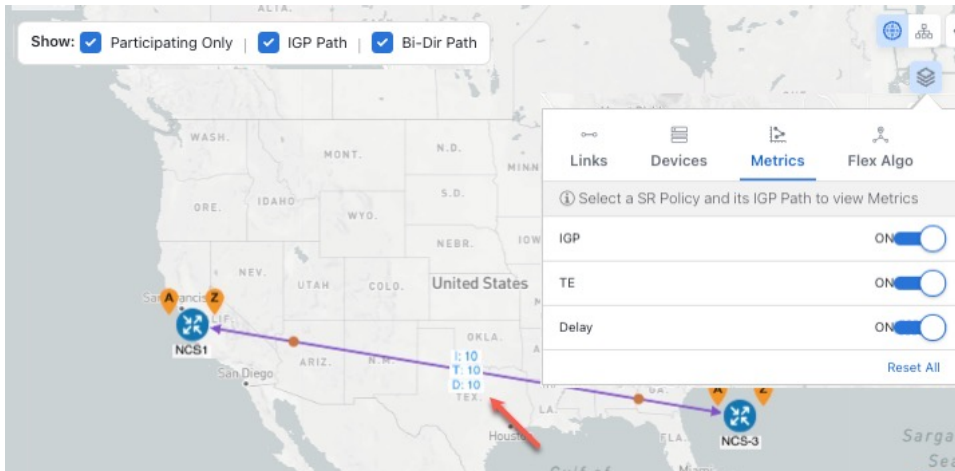
**PCE Initiated** false

**Affinity** Exclude-Any: -  
Include-Any: -  
Include-All: -

**Segment Type** Unprotected

**SID Algorithm** -

**Step 4** To view the physical path and metrics between endpoints of the selected policies, click  to turn applicable metrics on and check the **IGP Path** checkbox.



The screenshot shows a map of the United States with a path highlighted between two nodes, NCS1 and NCS-3. A 'Metrics' panel is overlaid on the right side of the map. The panel has tabs for 'Links', 'Devices', 'Metrics', and 'Flex Algo'. Under the 'Metrics' tab, there are three checkboxes: 'IGP Path' (checked), 'TE' (checked), and 'Delay' (checked). A red arrow points to the 'IGP Path' checkbox. At the top of the map, there are filters: 'Show:  Participating Only |  IGP Path |  Bi-Dir Path'.

## Step 6: Verify Circuit Style SR-TE Policy Bandwidth Utilization

Let's verify that the reserved bandwidth pool settings we defined when enabling Circuit Style SR-TE (see [Step 1: Enable Circuit Style Manager, on page 25](#)) are configured properly. We can also check how much bandwidth is either in use or still available.

- Step 1** From the main menu, choose **Services & Traffic Engineering > Traffic Engineering > SR-MPLS**. Then, under the **SR-MPLS** column, click **Circuit Style**. The **SR Policy** table lists all CS SR policies.
- Step 2** In the **SR Policy** table, check the check box next to the participating device whose details you want to see.
- Step 3** On the topology map, click on a participating Circuit Style SR-TE policy node to display the **Device Details** for that node.
- Step 4** On the **Device Details** page, click the **Links** tab to display the list of CS-SR and other links on the participating node. Then click on the link whose details you want to see. The **Link Details** list displays a **Summary** of the link information.
- Step 5** On the **Link Details** page, click on the **Traffic Engineering** tab, then the **General** tab. The **Link Details** list displays detailed information for the link.

Under **Circuit Style Bandwidth Pool**, you can see the reserved bandwidth pool size, the amount of bandwidth currently being used, and the amount of bandwidth (of the total allocated to Circuit Style SR-TE policies) is still available.

In this example, the reserved bandwidth pool size is displayed as 800 Mbps for NCS-3 and NCS1. The configured settings were earlier defined as 80% for the bandwidth pool size. Since the interfaces on this circuit are both 1 Gbps, we can confirm that Circuit Style SR-TE has correctly allocated 80 percent of bandwidth for these two interfaces.

### Link Details



Link Details		
Summary		
Traffic Engineering		
General		
SR-MPLS		
SRv6		
Tree-SID		
RSVP-TE		
	A Side	Z Side
Node	NCS-3	NCS1
IF Name	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/0
FA Affinities		
FA Topologies		
∨ Circuit Style Bandwidth Pool		
Pool Size	800 Mbps	800 Mbps
Used	4 Mbps	4 Mbps
Available	796 Mbps	796 Mbps

## Step 7: Trigger Circuit Style SR-TE Path Recomputation

Circuit-Style policies are static in nature, meaning once the paths are computed, Crosswork will not re-compute them automatically. Changes in your network topology or operational status may affect the previously computed Working and Protected paths to the extent that you want Crosswork to re-compute and optimize them for the new situation. In this step, we see a demonstration of how to re-optimize for paths to accommodate these types of changes.

For more details on the logic CSM employs in these cases, see [What Happens When Path Failures Occur?](#), on page 22.

**Step 1** From the main menu, choose **Services & Traffic Engineering > Traffic Engineering > SR-MPLS** and click **Circuit Style**.



**Step 2** The SR Policy table displays the status of each of the Active CS-SR policies. One of them is Operationally down.

**Step 3** From the **Actions** column next to the CS-SR TE policies whose Operational State is **Down**, click **\*\*\* > View Details**.

Crosswork displays the **Circuit Style Policy Details** window in the side panel. By default, the topology map shows the Active path and the bidirectional paths on the topology map (for these to appear, the **Bi-Dir Path** checkbox in the topology map's **Show** panel must be checked). The **Candidate Path** list at the bottom of the side panel displays the Active (Working) and Protected paths.

In the Summary panel, click the **See more** link to get a closer look at the type of Summary details available. The Candidate Path list displays the Active and Protected paths.

**Step 4** To have Crosswork re-optimize these paths: Click **\*\*\*** at the top of the **Circuit Style Policy Details** panel and select **Re-optimize**. Click **Yes** when prompted to confirm your selection.

## Summary and Conclusion

In this scenario, we observed how to use Circuit Style Segment Routing policies to reserve bandwidth for high-priority services and traffic in the network. CS-SR removes the need to manually track and calculate high-priority traffic paths, but still gives you control over how those paths are calculated and optimize bandwidth usage on each path. You can use these policies to ensure that available bandwidth is dedicated for these services. As traffic changes, Circuit Style policies warn you when your dedicated "circuit" paths fail, and allows you to re-optimize them as needed.

