Bandwidth and Network Optimization

This section explains the following topics:

Overview

Objective

Tactically optimize the network in real time during periods of congestion, and strategically reserve bandwidth for business-critical links to avoid congestion entirely.

Challenge

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. 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.

Solution

Cisco Crosswork Network Controller provides two means for meeting this challenge:

- 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)

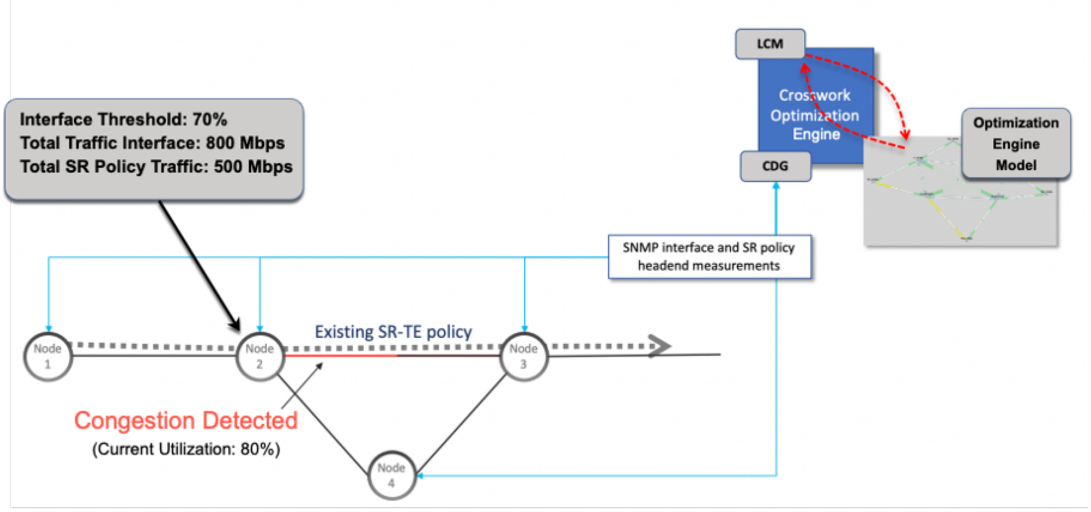
Instead of optimizing for bandwidth resource in the network by rerouting traffic in the entire network (end-to-end path optimization), LCM checks the capacity locally, in and around the congested area, at an interface level and reroutes traffic between the endpoints of the congested interface (local 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. LCM first analyzes the Optimization Engine Model (a realtime topology and traffic representation of the physical network) on a regular cadence.

2. In this example, after a congestion check interval, LCM detects congestion when Node 2 utilization goes above the 70% utilization threshold.


LCM
Crosswork Optimization Engine
CDG
Optimization Engine Model
Interface Threshold: 70%
Total Traffic Interface: 800 Mbps
Total SR Policy Traffic: 500 Mbps
SNMP interface and SR policy headend measurements
Existing SR-TE policy
Node 1
Node 2
Node 3
Node 4
Congestion Detected
(Current Utilization: 80%)

3. LCM calculates how much traffic is eligible to divert.

   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.

   Eligible traffic is computed 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 300 Mbps: 800 Mbps – 500 Mbps = 300 Mbps

4. 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 Mbps – 700 Mbps (70% threshold) = 100 Mbps

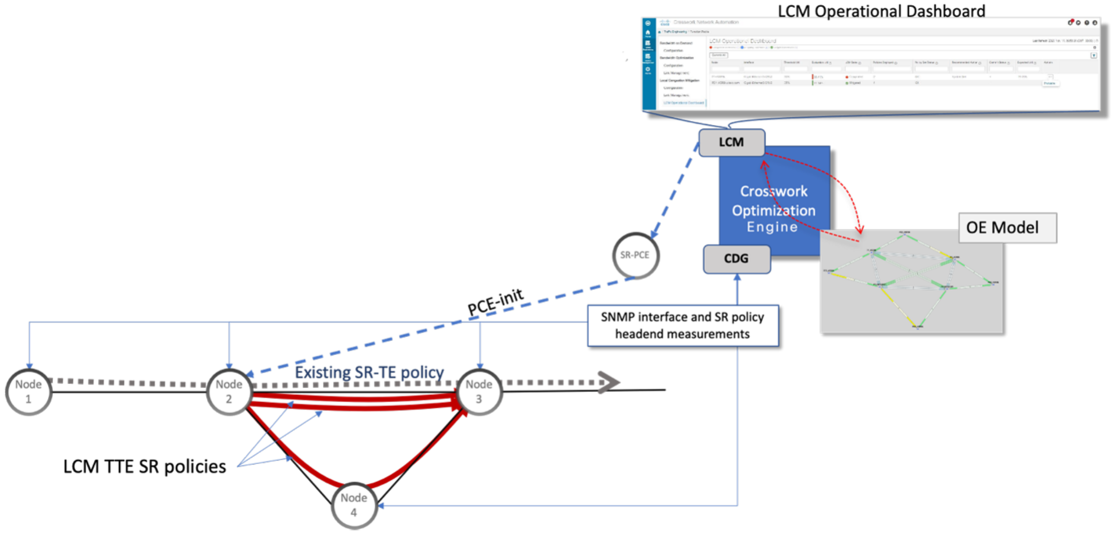
   LCM must route 100 Mbps of 300 Mbps (eligible traffic) to another path.

5. 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**.


LCM Operational Dashboard
LCM
Crosswork Optimization Engine
CDG
OE Model
SR-PCE
PCE-init
SNMP interface and SR policy headend measurements
Existing SR-TE policy
Node 1
Node 2
Node 3
Node 4
LCM TTE SR policies

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.

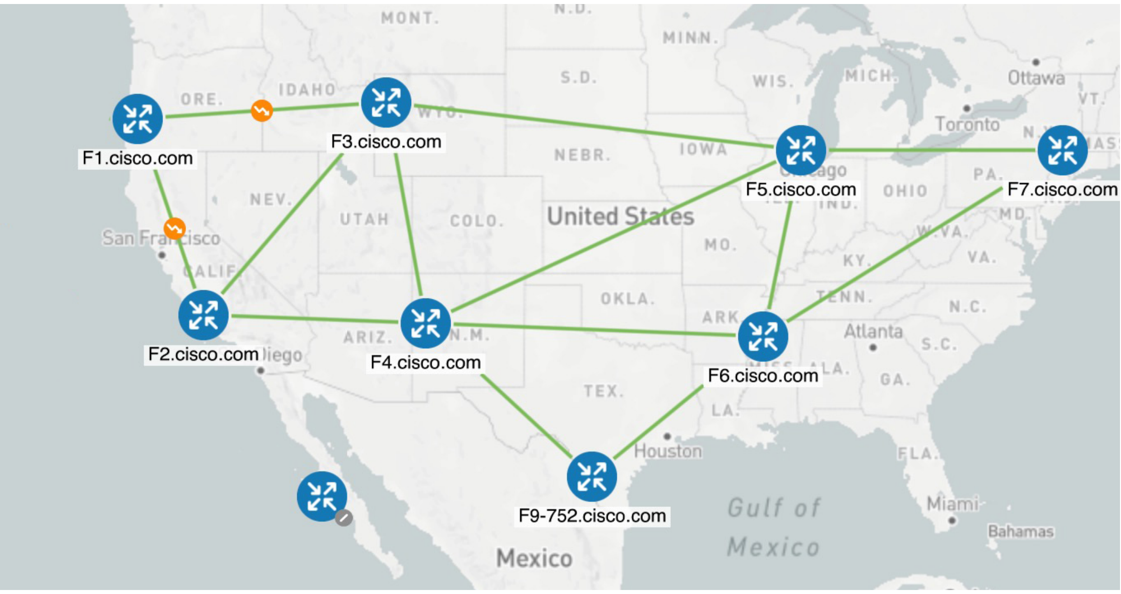
After the initial configuration:

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 6 – Use Local Congestion Mitigation (LCM) to reroute traffic on an over-utilized link

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

This example uses the following topology:



We will enable LCM with a configuration that results in the link between **F3.cisco.com** and **F5.cisco.com** becoming over-utilized. We will then review the mitigation solutions Crosswork calculates. In this example, it is left to the operator to choose to apply the solution.

Assumptions and Prerequisites

The following is a non-exhaustive list of high-level requirements for proper LCM operation:

Congestion Evaluation

LCM requires traffic statistics from the following:

- SNMP interface traffic measurements
- SNMP headend SR-TE policy traffic measurements

Congestion Mitigation

The headend device must support PCE-initiated SR-TE policies with autoroute steering.

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 headend device must support Equal Cost Multi-Path (ECMP) across multiple parallel SR-TE policies.

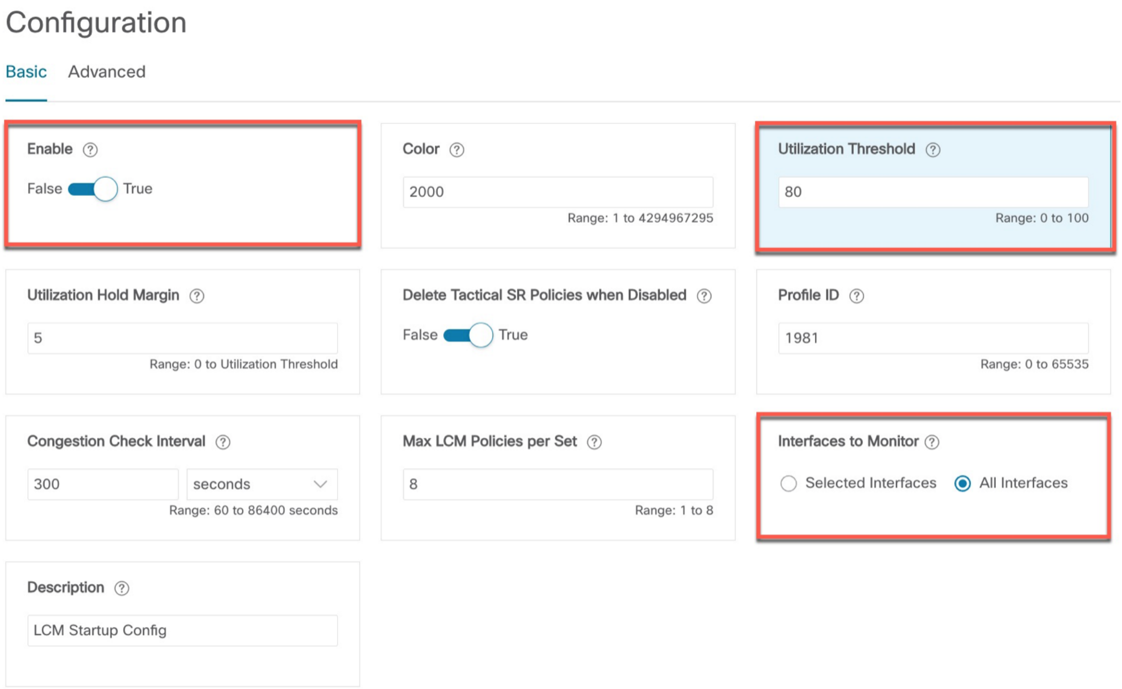
For more information, contact your Cisco Account representative.

Step 1 Enable LCM and configure the global 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 **Configuration**.

Step 2 Toggle the Enable switch to True, and enter the global utilization threshold you want to set. In this case, the threshold is set at 80%, and the **Interfaces to Monitor** > **All Interfaces** option is selected. To see information about other configuration options, hover the mouse over **?** (help icon).



Configuration

Basic | Advanced

Enable: False ● True

Color: 2000 (Range: 1 to 4294967295)

Utilization Threshold: 80 (Range: 0 to 100)

Utilization Hold Margin: 5 (Range: 0 to Utilization Threshold)

Delete Tactical SR Policies when Disabled: False ● True

Profile ID: 1981 (Range: 0 to 65535)

Congestion Check Interval: 300 seconds (Range: 60 to 86400 seconds)

Max LCM Policies per Set: 8 (Range: 1 to 8)

Interfaces to Monitor: ○ Selected Interfaces ● All Interfaces

Description: LCM Startup Config

Step 3 Click **Commit Changes**.

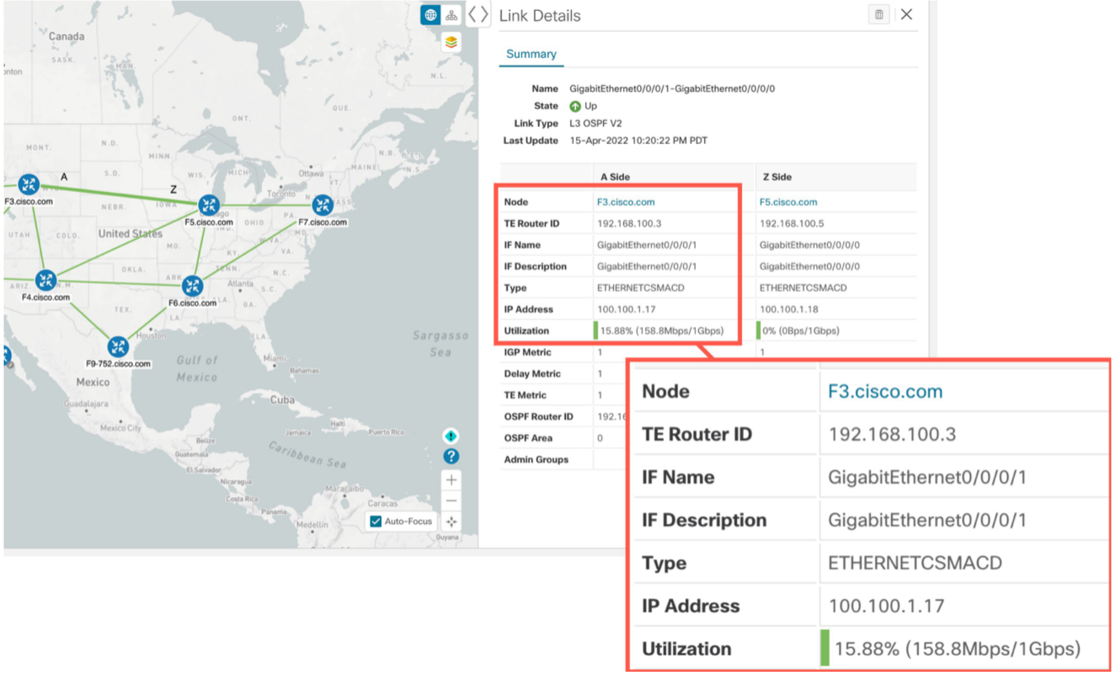
Note After committing the configuration changes, LCM will display *recommendations* on the **LCM Operational Dashboard** if congestion occurs on any monitored interfaces. LCM will *not* commit or deploy new TTE policies automatically. Later, you will be able to preview the recommended TTE policies and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

Step 2 View link congestion on the map

The link between **F3.cisco.com** and **F5.cisco.com** 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. Note that utilization on the P4-NCS5501 interfaces has surpassed the custom LCM threshold defined at 13%.



Link Details

Summary

Name GigabitEthernet0/0/0/1-GigabitEthernet0/0/0/0
State Up
Link Type L3 OSPF V2
Last Update 15-Apr-2022 10:20:22 PM PDT

	A Side	Z Side
Node	F3.cisco.com	F5.cisco.com
TE Router ID	192.168.100.3	192.168.100.5
IF Name	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/0
IF Description	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/0
Type	ETHERNETCSMACD	ETHERNETCSMACD
IP Address	100.100.1.17	100.100.1.18
Utilization	15.88% (158.8Mbps/1Gbps)	0% (0Bps/1Gbps)
IGP Metric	1	1
Delay Metric	1	
TE Metric	1	
OSPF Router ID	192.16	
OSPF Area	0	
Admin Groups		

Node	F3.cisco.com
TE Router ID	192.168.100.3
IF Name	GigabitEthernet0/0/0/1
IF Description	GigabitEthernet0/0/0/1
Type	ETHERNETCSMACD
IP Address	100.100.1.17
Utilization	15.88% (158.8Mbps/1Gbps)

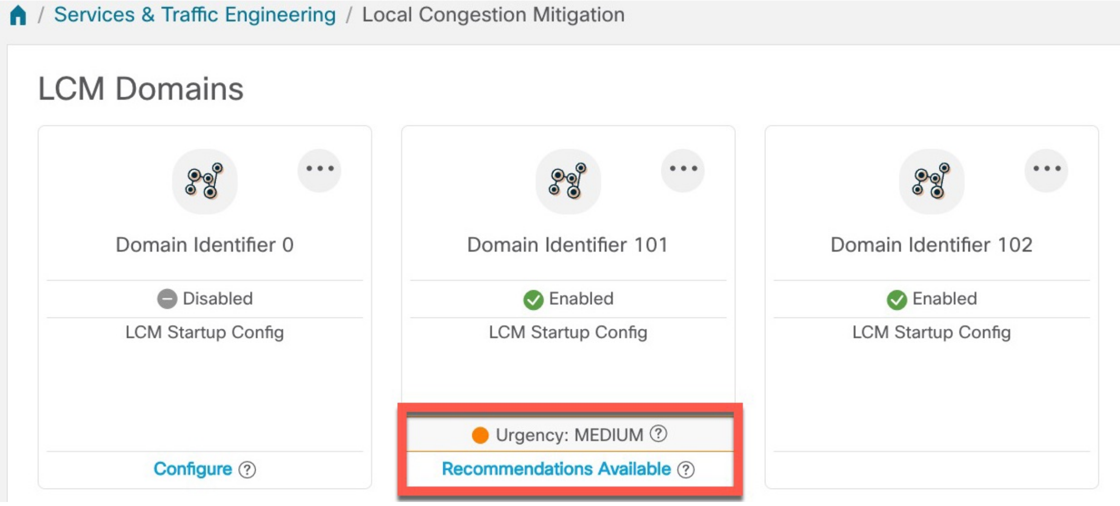
Step 3 Implement LCM recommendations

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**.

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.



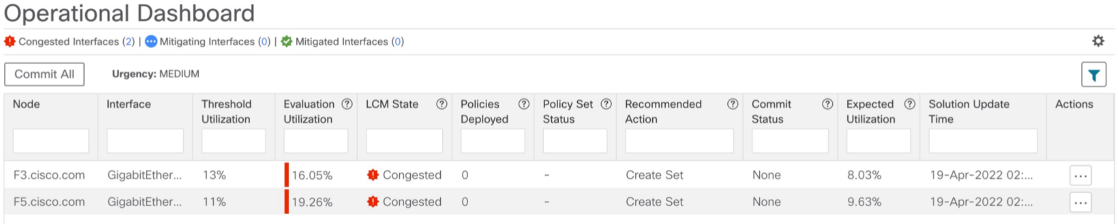
Services & Traffic Engineering / Local Congestion Mitigation

LCM Domains

Domain Identifier 0	Domain Identifier 101	Domain Identifier 102
Disabled	Enabled	Enabled
LCM Startup Config	LCM Startup Config	LCM Startup Config
	Urgency: MEDIUM	
Configure	Recommendations Available	

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

The dashboard shows that F3.cisco.com utilization has surpassed 13% and is now at 16.05%. It also shows that F5.cisco.com utilization has also surpassed the 11% threshold and is now 19.26%. In the Recommended Action column, LCM recommends the deployment of TTE policy solution sets (Create Set) to address the congestion on the interface. The Expected Utilization column shows the expected utilization of each of the interfaces after the recommended action is committed.



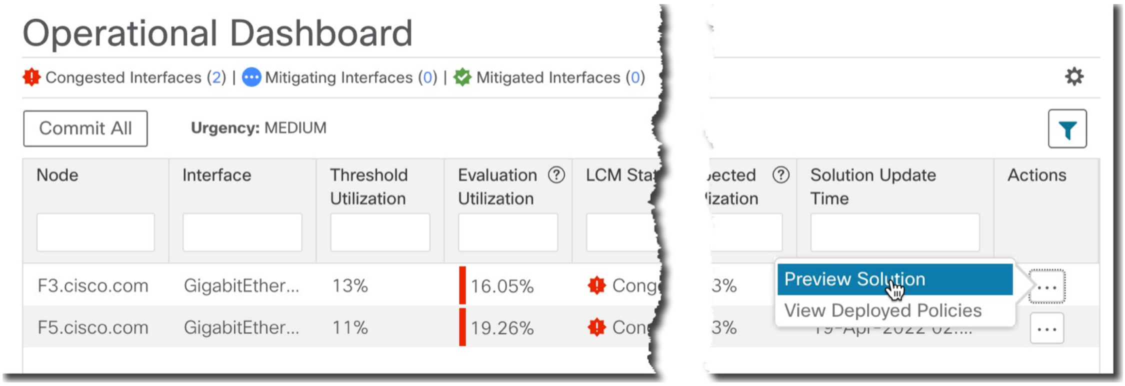
Operational Dashboard

Congested Interfaces (2) | Mitigating Interfaces (0) | Mitigated Interfaces (0)

Commit All   **Urgency:** MEDIUM

Node	Interface	Threshold Utilization	Evaluation Utilization	LCM State	Policies Deployed	Policy Set Status	Recommended Action	Commit Status	Expected Utilization	Solution Update Time	Actions
F3.cisco.com	GigabitEther...	13%	16.05%	Congested	0	-	Create Set	None	8.03%	19-Apr-2022 02:...	...
F5.cisco.com	GigabitEther...	11%	19.26%	Congested	0	-	Create Set	None	9.63%	19-Apr-2022 02:...	...

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.



Operational Dashboard

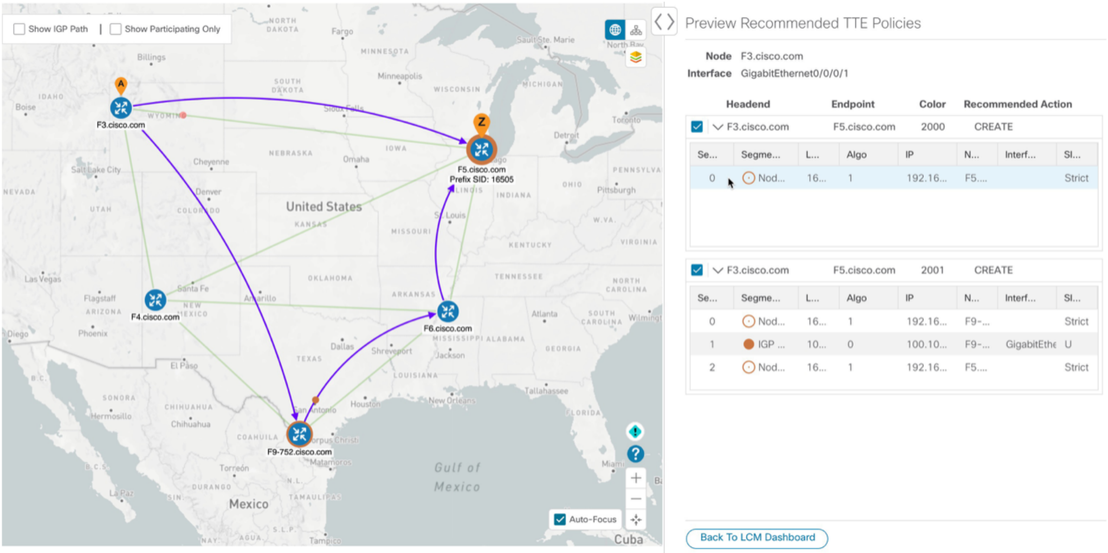
Congested Interfaces (2) | Mitigating Interfaces (0) | Mitigated Interfaces (0)

Commit All   **Urgency:** MEDIUM

Node	Interface	Threshold Utilization	Evaluation Utilization	LCM Stat	ected ization	Solution Update Time	Actions
F3.cisco.com	GigabitEther...	13%	16.05%	Cong	3%		...
F5.cisco.com	GigabitEther...	11%	19.26%	Con	3%	19-Apr-2022 02:...	...

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 F3.cisco.com and interface GigabitEthernet0/0/0/1. The top path shows the node SID (orange outline), headend and endpoint (A and Z) because the mouse pointer hovers over that segment.



Preview Recommended TTE Policies

Node F3.cisco.com
Interface GigabitEthernet0/0/0/1

	Headend	Endpoint	Color	Recommended Action
☑	F3.cisco.com	F5.cisco.com	2000	CREATE

Se...	Segme...	L...	Algo	IP	N...	Interf...	Sl...
0	○ Nod...	16...	1	192.16...	F5....		Strict

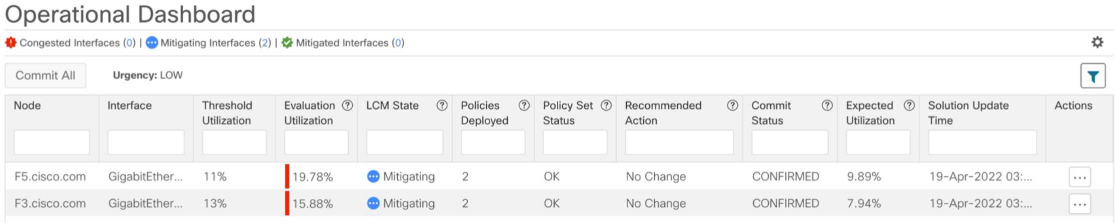
	Headend	Endpoint	Color	Recommended Action
☑	F3.cisco.com	F5.cisco.com	2001	CREATE

Se...	Segme...	L...	Algo	IP	N...	Interf...	Sl...
0	○ Nod...	16...	1	192.16...	F9-...		Strict
1	● IGP ...	10...	0	100.10...	F9-...	GigabitEthe	U
2	○ Nod...	16...	1	192.16...	F5....		Strict

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.



Operational Dashboard

Congested Interfaces (0) | Mitigating Interfaces (2) | Mitigated Interfaces (0)

Commit All   **Urgency:** LOW

Node	Interface	Threshold Utilization	Evaluation Utilization	LCM State	Policies Deployed	Policy Set Status	Recommended Action	Commit Status	Expected Utilization	Solution Update Time	Actions
F5.cisco.com	GigabitEther...	11%	19.78%	Mitigating	2	OK	No Change	CONFIRMED	9.89%	19-Apr-2022 03:...	...
F3.cisco.com	GigabitEther...	13%	15.88%	Mitigating	2	OK	No Change	CONFIRMED	7.94%	19-Apr-2022 03:...	...

Step 4 Validate the TTE SR policy deployment

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

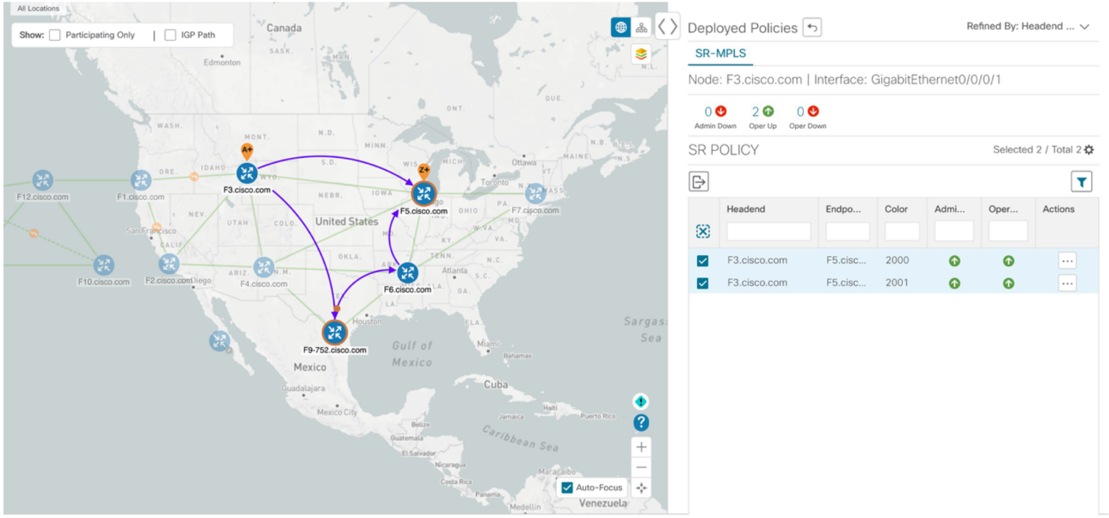
Step 1 Click **bell icon> Events** tab to open the Events window in which you can monitor LCM events. You see events for the LCM recommendations, the commit actions, as well as any exceptions.

Crosswork Optimization Engine 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 will take up to 2 times longer than the SNMP cadence.

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.



Deployed Policies

Refined By: Headend ...

SR-MPLS

Node: F3.cisco.com | Interface: GigabitEthernet0/0/0/1

0 Admin Down | 2 Oper Up | 0 Oper Down

SR POLICY Selected 2 / Total 2

	Headend	Endpo...	Color	Admi...	Oper...	Actions
☑	F3.cisco.com	F5.cisc...	2000	⬆	⬆	⋯
☑	F3.cisco.com	F5.cisc...	2001	⬆	⬆	⋯

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**.

Step 5 Remove the TTE SR policies upon LCM recommendation

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

Step 1 After some time, the deployed TTE SR policies may no longer be needed. This occurs if the utilization will continue to stay under the threshold without the LCM-initiated TTE policies. If this is the case, LCM generates new recommended actions to delete the TTE SR policy sets.

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.

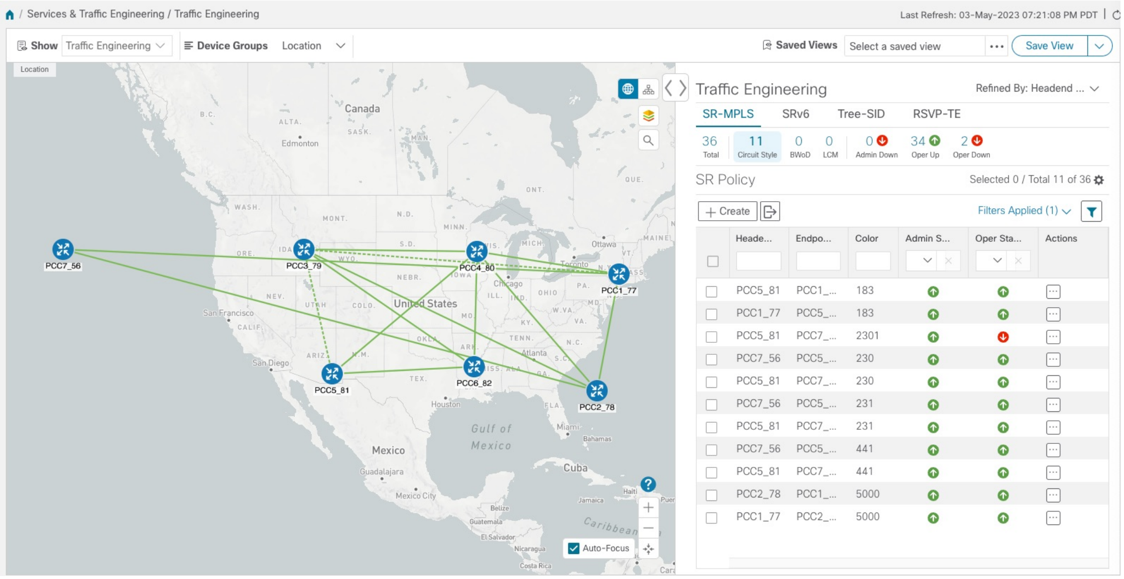
Summary and Conclusion

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 7 – Use Circuit-Style SR Policies to Reserve Bandwidth

In this scenario, we enable CS-SR 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:



□	Heade...	Endpo...	Color	Admin S...	Oper Sta...	Actions
□	PCC5_81	PCC1_...	183	↑	↑	⋯
□	PCC1_77	PCC5_...	183	↑	↑	⋯
□	PCC5_81	PCC7_...	2301	↑	↓	⋯
□	PCC7_56	PCC5_...	230	↑	↑	⋯
□	PCC5_81	PCC7_...	230	↑	↑	⋯
□	PCC7_56	PCC5_...	231	↑	↑	⋯
□	PCC5_81	PCC7_...	231	↑	↑	⋯
□	PCC7_56	PCC5_...	441	↑	↑	⋯
□	PCC5_81	PCC7_...	441	↑	↑	⋯
□	PCC2_78	PCC1_...	5000	↑	↑	⋯
□	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.

Assumptions and Prerequisites

The following sections provide a non-exhaustive list of high-level requirements for proper CS-SR operation, including requirements and constraints on the policy attribute values set in each Circuit Style SR-TE 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.

Attribute	Description
Bandwidth Constraint	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: • Once you configure the new bandwidth on both sides, Crosswork will evaluate the path. This **will not** result in a recomputed path. • 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. • If the bandwidth is lower, Crosswork returns the same path with the new bandwidth value to indicate to the PCC that it was successful. 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.
Candidate Paths and Roles	The `Working` path is defined as the highest preference Candidate Path (CP). The `Protect` path is defined as the CP with the second highest preference. The `Restore` path is defined with the lowest preference CP. The headend must have `backup-ineligible` configured. CPs of the same role in each direction must have the same CP preference.
Bi-Directional	All paths must be configured as co-routed. Paths with the same role on both sides must have the same globally unique bi-directional association ID.
Disjointness	Working and Protect paths on the same PCC must be configured with a disjointness constraint using the same disjoint association ID and disjointness type. 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. Only the `Node` and `Link` disjoint types are supported. The disjoint type used must be the same in both directions of the same policy. The Restore path must not have a disjointness constraint set. 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.

Attribute	Description
Metric Type	Only the `TE`, `IGP` and `Latency` metric types are supported. The metric type used must match across Working, Protect and Restore paths in both directions.
Segment Constraints	All Working, Protect and Restore paths must have the following segment constraints: • `protection unprotected-only` • `adjacency-sid-only` To ensure persistence through link failures, configure static adjacency SIDs on all interfaces that might be used by Circuit Style policies.
Supported Policy Changes	The following constraints may be changed for an operationally "up" Circuit Style SR-TE policy that has been previously delegated: • Metric type • Disjoint type • MSD • Affinities 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. 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.
Path Computation	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. 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. Path computation is supported for Intra/Inter area/level and Intra/Inter IGP Domain (same AS).
Reversion Behavior	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): • No lock configuration: Revert after a default 5-minute lock • Lock with no duration specified: No reversion • Lock duration <value>: Revert after the specified number of seconds

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	The following configurations are not supported: • Metric-bounds • SID-Algo constraints • Partial recovery is not supported with 7.8.x. • 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. • Multiple Circuit Style SR-TE policies between the same nodes with the same color but different endpoint IPs.
Unsupported Policy Changes	The following configuration changes to a previously delegated and operationally "up" Circuit Style SR-TE policy are not supported: • CP preference • Disjoint Association ID • Bi-directional Association ID 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.
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	1. Working path recovers to up/standby state. 2. Each PCC moves the Working path to active after the WTR timer expires. 3. Protect path moves to up/standby.

Initial State	Events	Behavior
Working path is down, Protect path is down, Revert path is up/active	Working path comes back up, then Protect path comes back up	1. Working path recovers and goes to up/active state 2. Revert path is removed 3. Protect path recovers and goes to up/standby
Working path is down, Protect path is down, Revert path is up/active	Protect path comes back up, then Working path comes back up	On side A: The Working path failure is local (the first Adj SID in the SegList is **invalid**): 1. Protect path recovers and goes to up/active. 2. Recover path is removed. 3. Working path recovers and goes to up/standby. 4. Each PCC moves the Working path to active after the WTR timer expires, Protect path goes to up/standby. On side Z: Working path failure is remote (first Adj SID in SegList is **valid**): 1. Protect path recovers but is not brought up, Revert path remains up/active. 2. Working path recovers and goes up/active. 3. Revert path is removed. 4. Protect path goes to up/standby.

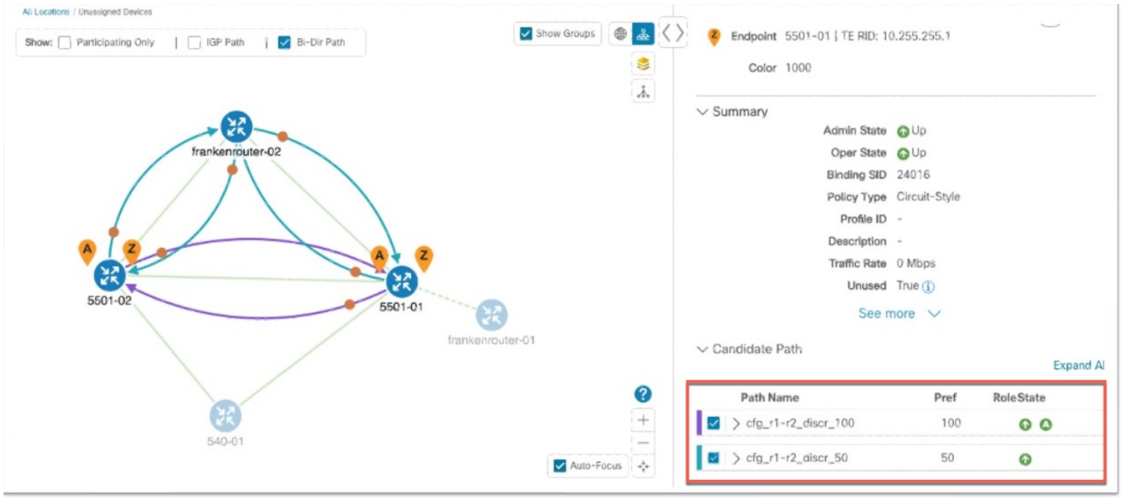
What Happens When Path Failures Occur?

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 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 30.

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.


All Locations / Unassigned Devices
Show: ☐ Participating Only | ☐ IGP Path | ☑ Bi-Dir Path
☑ Show Groups
frankenrouter-02
A
Z
5501-02
A
Z
5501-01
frankenrouter-01
540-01
☑ Auto-Focus

Endpoint 5501-01 | TE RID: 10.255.255.1

Color 1000

Summary

Admin State Up
Oper State Up
Binding SID 24016
Policy Type Circuit-Style
Profile ID -
Description -
Traffic Rate 0 Mbps
Unused True

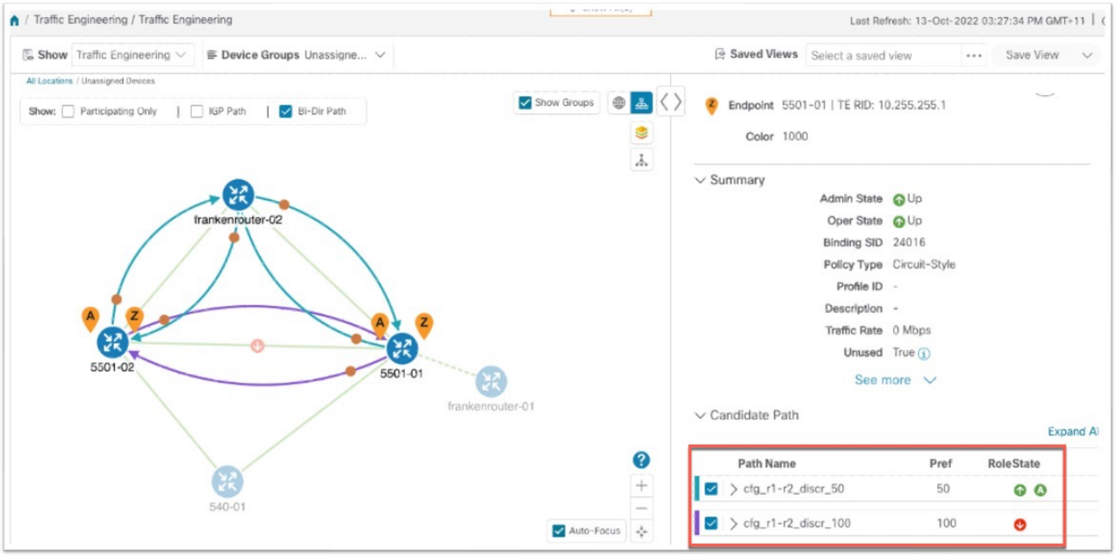
See more

Candidate Path

Expand Al

	Path Name	Pref	RoleState
☑	cfg_r1-r2_discr_100	100	⬆ Ⓐ
☑	cfg_r1-r2_discr_50	50	⬆

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


Traffic Engineering / Traffic Engineering
Show Traffic Engineering
Device Groups Unassigne...
Saved Views
Select a saved view
Save View
All Locations / Unassigned Devices
Show: ☐ Participating Only | ☐ IGP Path | ☑ Bi-Dir Path
☑ Show Groups
frankenrouter-02
A
Z
5501-02
A
Z
5501-01
frankenrouter-01
540-01
☑ Auto-Focus

Last Refresh: 13-Oct-2022 03:27:34 PM GMT+11

Endpoint 5501-01 | TE RID: 10.255.255.1

Color 1000

Summary

Admin State Up
Oper State Up
Binding SID 24016
Policy Type Circuit-Style
Profile ID -
Description -
Traffic Rate 0 Mbps
Unused True

See more

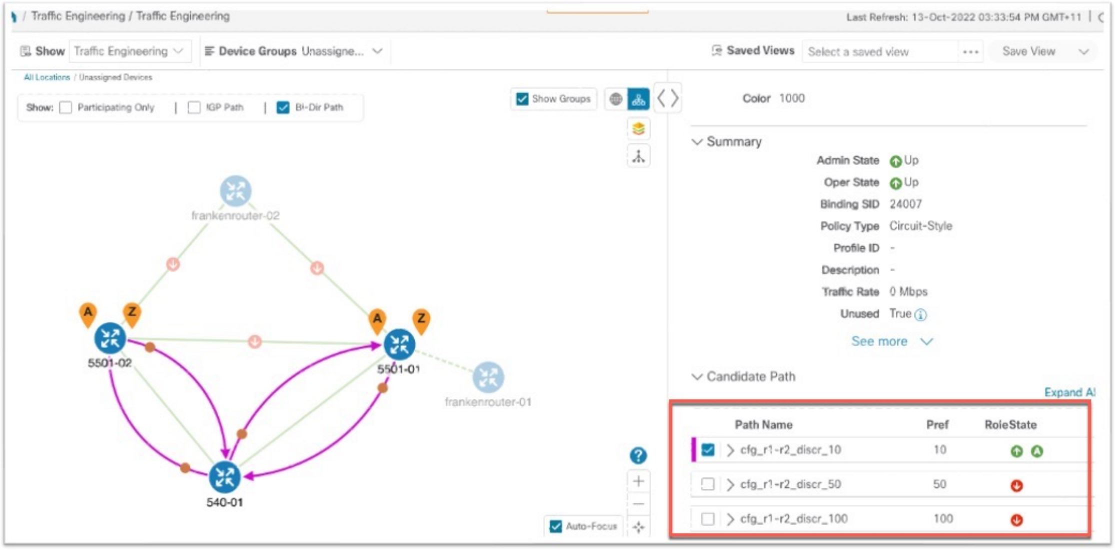
Candidate Path

Expand Al

	Path Name	Pref	RoleState
☑	cfg_r1-r2_discr_50	50	⬆ Ⓐ
☑	cfg_r1-r2_discr_100	100	⬇

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.


/ Traffic Engineering / Traffic Engineering
Last Refresh: 13-Oct-2022 03:33:54 PM GMT+11
Show Traffic Engineering
Device Groups Unassigne...
Saved Views
Select a saved view
Save View
All Locations / Unassigned Devices
Show: □ Participating Only | □ IGP Path | ☑ Bi-Dir Path
☑ Show Groups
frankenrouter-02
A
Z
5501-02
5501-01
frankenrouter-01
540-01
☑ Auto-Focus
Summary
See more
Candidate Path
Expand Al

Color 1000

Admin State Up
Oper State Up
Binding SID 24007
Policy Type Circuit-Style
Profile ID -
Description -
Traffic Rate 0 Mbps
Unused True

	Path Name	Pref	RoleState
☑	cfg_r1-r2_discr_10	10	↑ A
□	cfg_r1-r2_discr_50	50	↓
□	cfg_r1-r2_discr_100	100	↓

Workflow

Workflow steps	Detailed procedure links
1. Enable the SR Circuit Style Manager (CSM) feature pack.	Step 1: Enable SR Circuit Style Manager, on page 21.
2-4. Configure Circuit Style SR-TE policies on the devices. **Note** 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-TEpolicies using any of the following methods: • On the device, using the CLI. See Step 2: Configure Circuit Style SR-TE Policies Using Device CLI, on page 25 • Using the user interface. See Step 3: Configure Circuit Style SR-TE Policies Using Add, on page 28 • Import a JSON or XML file. See Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 30
5. Verify that the Circuit Style SR-TE policy appears in the SR Policy table and on the topology map.	See Step 5: View Circuit Style SR-TE Policies on the Topology Map, on page 33
6. Verify that the reserved bandwidth pool settings you defined in Step 1 are configured properly.	See Step 6: Verify Circuit Style SR-TE Policy Bandwidth Utilization , on page 40.
7. Trigger path re-computation after path failures.	See Step 7: Trigger Circuit Style SR-TE Path Recomputation, on page 41.

Step 1: Enable SR 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.

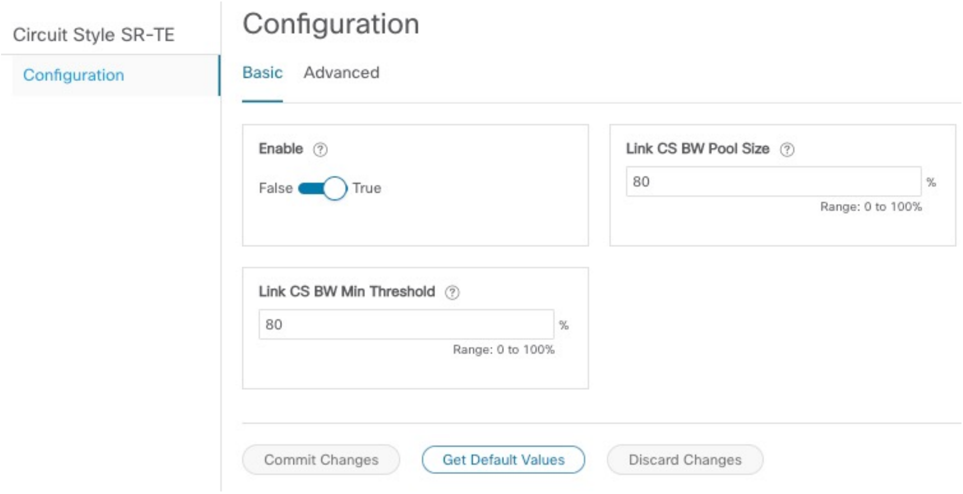
To help you estimate Circuit Style SR-TE bandwidth pool and threshold settings that are reasonable for your organization's implementation, this topic provides two examples showing how CSM handles policies that exceed either the bandwidth pool size or both the pool size and alarm threshold. For the purposes 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 25
- Step 3: Configure Circuit Style SR-TE Policies Using Add, on page 28
- Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 30

Step 1 From the main menu, choose **Services & Traffic Engineering** > **Circuit Style SR-TE** > **Configuration** > **Basic**.

Step 2 Toggle the **Enable** switch to **True**.



Enable: False / True (True)

Link CS BW Pool Size: 80 %
Range: 0 to 100%

Link CS BW Min Threshold: 80 %
Range: 0 to 100%

Step 3 Enter the required bandwidth pool size and threshold information. The following list describes additional field information. See also the examples below, and choose one of them to enter.

Field	Description
Basic	
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.
Advanced	
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.

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

Example

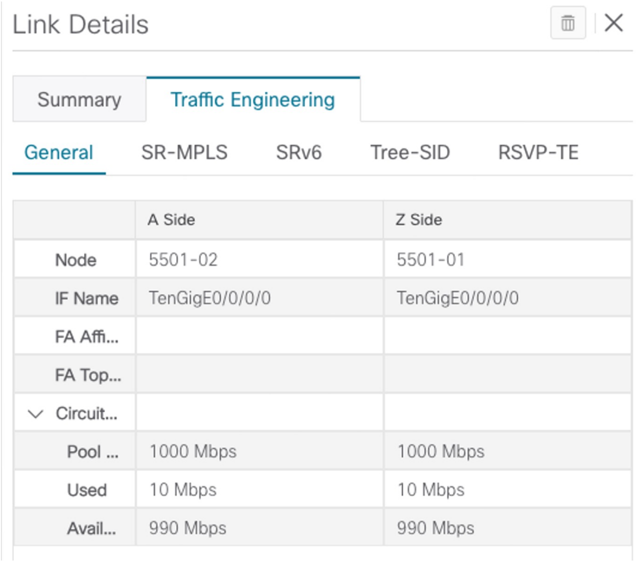
Example: Bandwidth Utilization Surpasses Defined Threshold

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

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

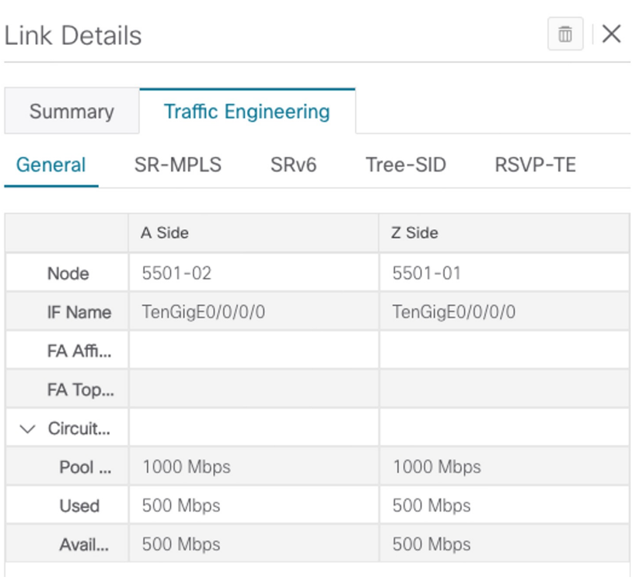
Our two nodes have 10 Gbps Ethernet interfaces, so the bandwidth pool size with these settings is 1Gbs and the alarm threshold is 100 Mbps.

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



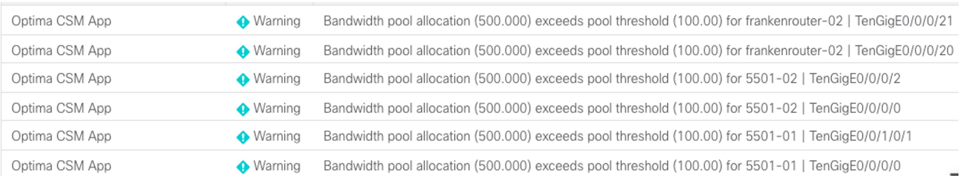
	A Side	Z Side
Node	5501-02	5501-01
IF Name	TenGigE0/0/0/0	TenGigE0/0/0/0
FA Affi...		
FA Top...		
Circuit...		
Pool ...	1000 Mbps	1000 Mbps
Used	10 Mbps	10 Mbps
Avail...	990 Mbps	990 Mbps

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



	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

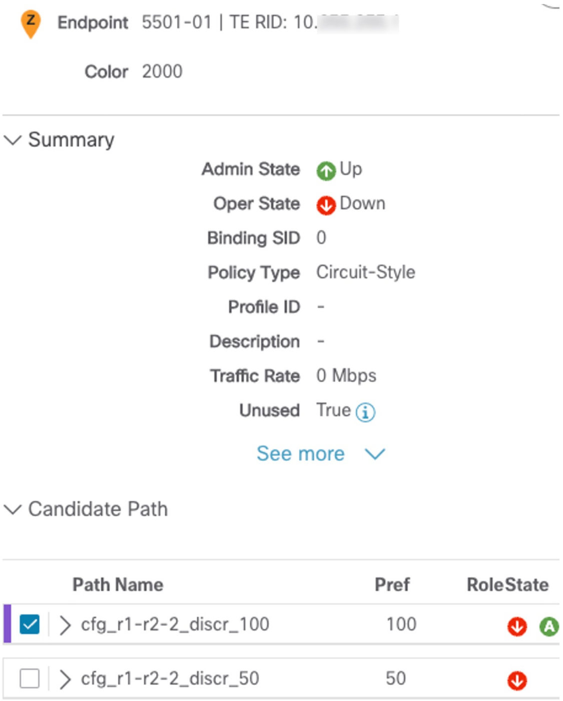
Example: Bandwidth Pool Size and Usage Exceeded

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 1Gbs 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.[redacted]

Color 2000

Summary

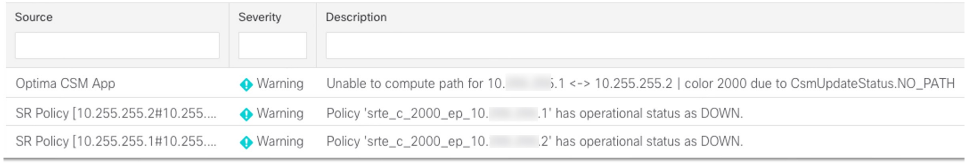
Admin State: Up
Oper State: Down
Binding SID: 0
Policy Type: Circuit-Style
Profile ID: -
Description: -
Traffic Rate: 0 Mbps
Unused: True

See more

Candidate Path

	Path Name	Pref	RoleState
☑	cfg_r1-r2-2_discr_100	100	A
□	cfg_r1-r2-2_discr_50	50	

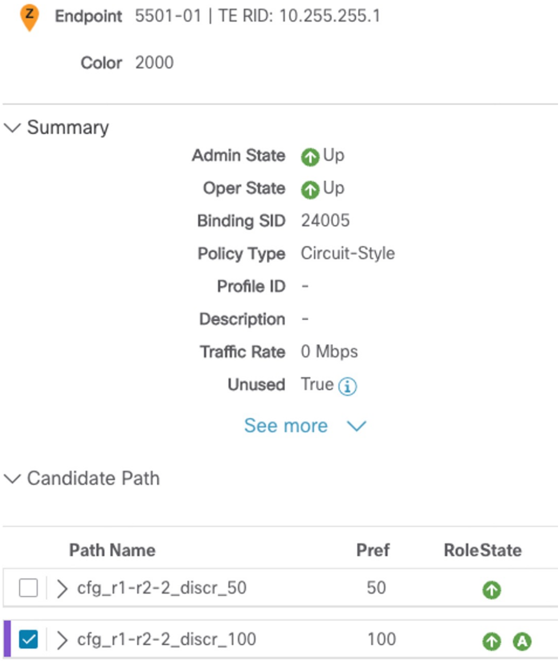
   - Alerts are triggered.



Source	Severity	Description
Optima CSM App	Warning	Unable to compute path for 10.[redacted].1 <-> 10.255.255.2 | color 2000 due to CsmUpdateStatus.NO_PATH
SR Policy [10.255.255.2#10.255....	Warning	Policy 'srte_c_2000_ep_10.[redacted].1' has operational status as DOWN.
SR Policy [10.255.255.1#10.255....	Warning	Policy 'srte_c_2000_ep_10.[redacted].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 polices (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).



Endpoint 5501-01 | TE RID: 10.255.255.1

Color 2000

Summary

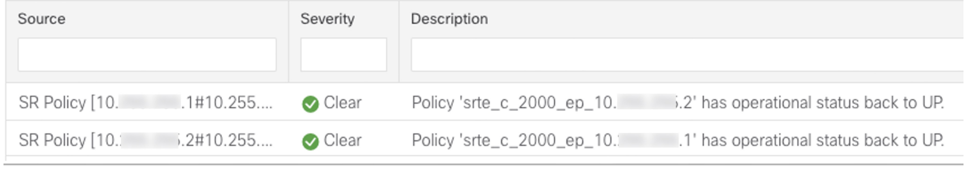
Admin State ↑ Up
Oper State ↑ Up
Binding SID 24005
Policy Type Circuit-Style
Profile ID -
Description -
Traffic Rate 0 Mbps
Unused True ⓘ

See more

Candidate Path

	Path Name	Pref	RoleState
□	cfg_r1-r2-2_discr_50	50	↑
☑	cfg_r1-r2-2_discr_100	100	↑ Ⓐ

- 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.[redacted].1#10.255....	✓ Clear	Policy 'srte_c_2000_ep_10.[redacted].2' has operational status back to UP.
SR Policy [10.[redacted].2#10.255....	✓ Clear	Policy 'srte_c_2000_ep_10.[redacted].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 28 or to Step 4: Configure Circuit Style SR-TE Policies Using Import, on page 30.

A Circuit Style SR-TE policy configuration must include the destination endpoint, the amount of requested bandwidth, and the bidirectional attribute. See Assumptions and Prerequisites, on page 12 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 Assumptions and Prerequisites, on page 12 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 30.

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

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 the > icon 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	• **Device**: Enter `NCS1`. • **Ip-address**: Enter `192.168.20.4`.
tail-end	• **Device**: Enter `NCS3`. • **Ip-address**: Enter `192.168.20.14`.
disjoint-path	Click **Enable disjoint-path**.
disjoint-path > forward-path	• **Type**: Select `Link`. • **group-id**: Enter `531`.
disjoint-path > reverse-path	• **Type**: Select `Link`. • **group-id**: Enter `5311`.
performance-measurement	Click **Enable performance-measurement**.
performance-measurement > Profile-type	Click **liveness**.
performance-measurement > Profile-type > liveness-detection	Click **Enable liveness-detection**. Then: • **Profile**: Enter `CS-active`. • **Backup**: Enter `CS-protected`.
working-path	Click **Enable working-path**. Then select **dynamic-path**.
working path > dynamic	Click **Enable dynamic-path**. Then: • **pce**: Check the checkbox. • **Metric-type**: Select `igp` • **Bidirectional-association-choice**: Select **bidirectional-association-id** and enter `230`in the field.
working path > dynamic > constraints > segments	Click **Enable segments**. Then in the **Protection** field, select `unprotected-only`.
protect-path	Click **Enable protect-path**. Then select **dynamic-path**.

Expand this:	**To specify this:**
protect-path > dynamic	Click **Enable dynamic**. Then: • **pce**: Check the checkbox. • **Metric-type**: Select `igp` • **Bidirectional-association-choice**: Select **bidirectional-association-id** and enter `231`in the field.
protect-path > dynamic > constraints > segments	Click **Enable segments**. Then in the **Protection**, field, select `unprotected-only`.
restore-path	Click **Enable restore-path**. Then select **dynamic-path**.
restore-path > dynamic	Click **Enable dynamic-path**. Then: • **pce**: Check the checkbox. • **Metric-type**: Select `igp` • **Bidirectional-association-choice**: Select **bidirectional-association-id** and enter `232`in the field.
restore-path > dynamic > constraints > segments	Click **Enable segments**. Then in the **Protection** field, select `unprotected-only`.

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**.

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** 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>
    <protect-path>
      <dynamic>
        <constraints>
          <segments>
            <protection>unprotected-only</protection>
          </segments>
        </constraints>
        <pce></pce>
        <metric-type>igp</metric-type>
        <bidirectional-association-id>231</bidirectional-association-id>
      </dynamic>
    </protect-path>
  <restore-path>
    <dynamic>
      <constraints>
        <segments>
          <protection>unprotected-only</protection>
          </segments>
        </constraints>
        <pce></pce>
        <metric-type>igp</metric-type>
        <bidirectional-association-id>232</bidirectional-association-id>
      </dynamic>
    </restore-path>
  </cs-sr-te-policy>
</config>
```

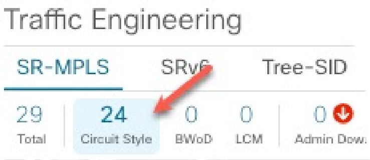
Step 8 When you have finished editing the file and saved your changes, navigate to **Services & Traffic Engineering** > **Provisioning** > **SR-TE** > **Circuit-Style Policy** again.

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.

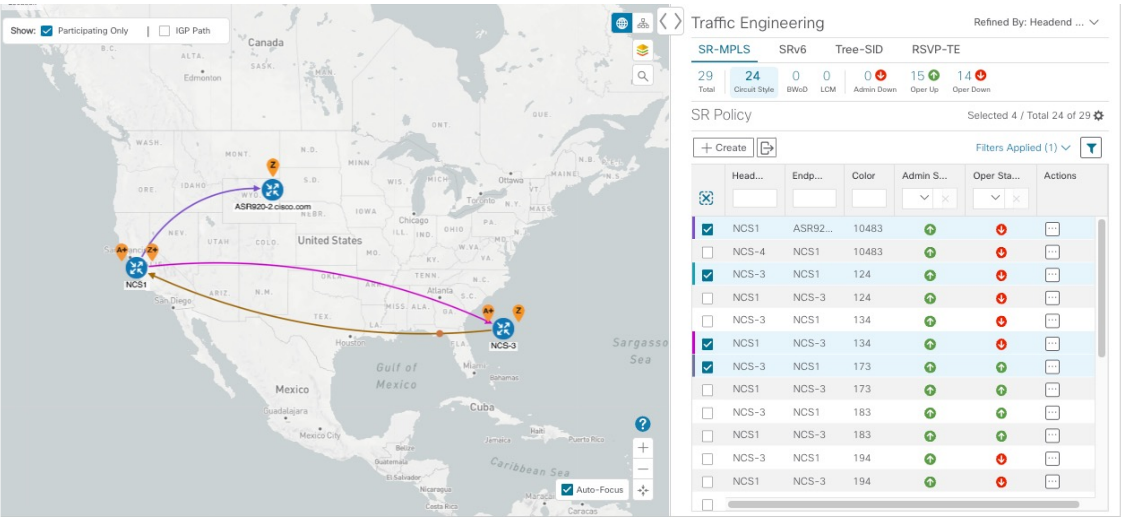
Step 1 From the main menu, choose **Services & Traffic Engineering** > **Traffic Engineering** > **SR-MPLS**. Then click **Circuit Style**.



The **SR Policy** table lists all policies.

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

Step 2 Check the check box next to **Show Participating Only** so that other links and devices that are not part of the selected Circuit Style SR-TE policies are hidden.



Traffic Engineering

Refined By: Headend ...

SR-MPLS SRv6 Tree-SID RSVP-TE

29 Total | 24 Circuit Style | 0 BWoD | 0 LCM | 0 Admin Down | 15 Oper Up | 14 Oper Down

SR Policy

Selected 4 / Total 24 of 29

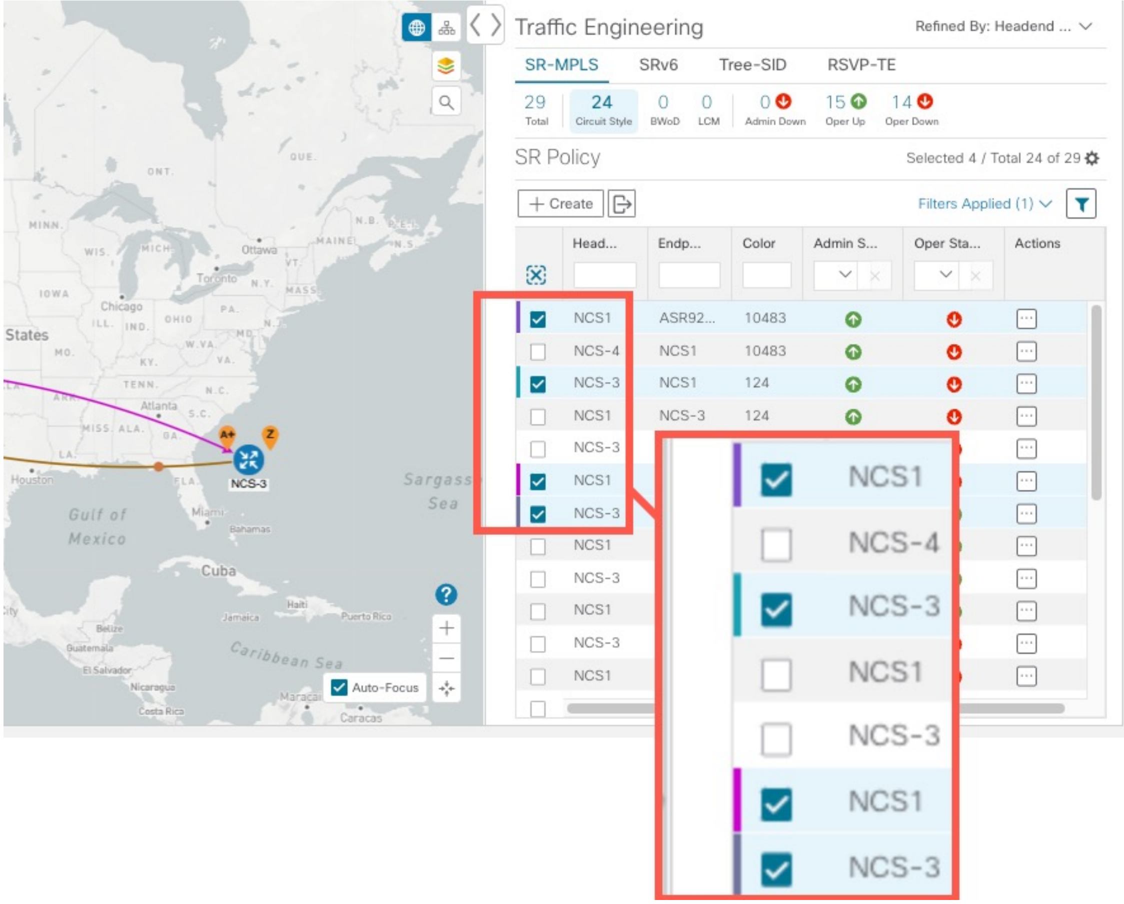
+ Create

Filters Applied (1)

	Head...	Endp...	Color	Admin S...	Oper Sta...	Actions
☑	NCS1	ASR92...	10483	⬆	⬇	···
□	NCS-4	NCS1	10483	⬆	⬇	···
☑	NCS-3	NCS1	124	⬆	⬇	···
□	NCS1	NCS-3	124	⬆	⬇	···
□	NCS-3	NCS1	134	⬆	⬇	···
☑	NCS1	NCS-3	134	⬆	⬇	···
☑	NCS-3	NCS1	173	⬆	⬆	···
□	NCS1	NCS-3	173	⬆	⬆	···
□	NCS-3	NCS1	183	⬆	⬆	···
□	NCS1	NCS-3	183	⬆	⬆	···
□	NCS-3	NCS1	194	⬆	⬇	···
□	NCS1	NCS-3	194	⬆	⬇	···

From the topology map above, note the following details:

- Four Circuit Style SR-TE policies are checked, but only three paths appear to be visible. The reason for this is that the last two Circuit Style SR-TE policies have the same endpoints (NCS1 and NCS-3) and share the same paths. The brown colored link indicates policies that use the same paths.
- The line representing each path defined in the policy appears on the topology map using a different line color. Vertical color bars next to each checked policy in the **SR Policy** table match the color used for the corresponding path line on the map. To see the color legend, explaining which colors are used and what each color shows, click the ⓘ.



Traffic Engineering   Refined By: Headend ...

SR-MPLS | SRv6 | Tree-SID | RSVP-TE

29 Total | 24 Circuit Style | 0 BWoD | 0 LCM | 0 Admin Down | 15 Oper Up | 14 Oper Down

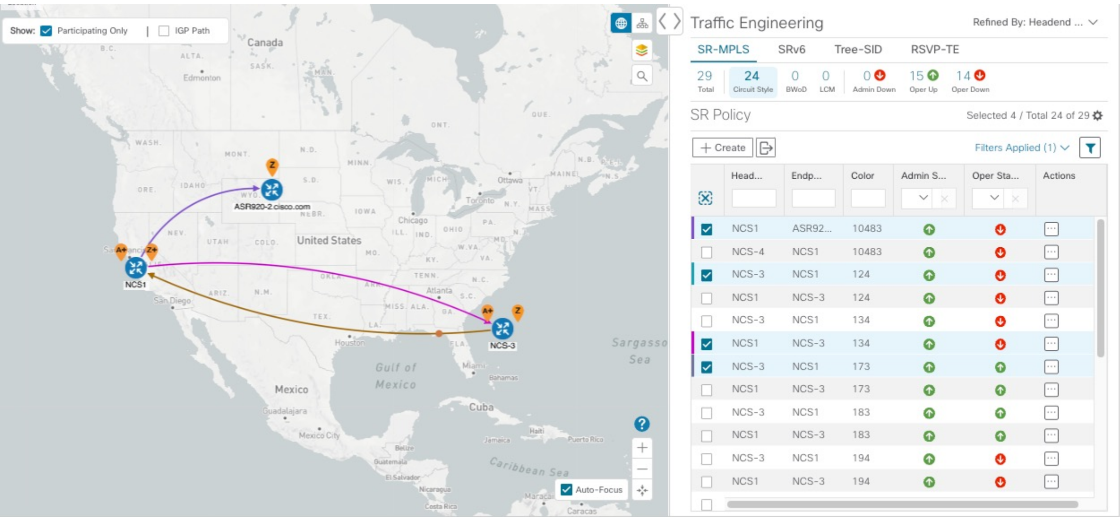
SR Policy   Selected 4 / Total 24 of 29

+ Create   Filters Applied (1)

	Head...	Endp...	Color	Admin S...	Oper Sta...	Actions
☑	NCS1	ASR92...	10483	↑	↓	⋯
□	NCS-4	NCS1	10483	↑	↓	⋯
☑	NCS-3	NCS1	124	↑	↓	⋯
□	NCS1	NCS-3	124	↑	↓	⋯
□	NCS-3					⋯
☑	NCS1					⋯
☑	NCS-3					⋯
□	NCS1					⋯
□	NCS-3					⋯
□	NCS1					⋯
□	NCS-3					⋯
□	NCS1					⋯

☑ NCS1
□ NCS-4
☑ NCS-3
□ NCS1
□ NCS-3
☑ NCS1
☑ NCS-3

- 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.



Traffic Engineering   Refined By: Headend ...

SR-MPLS | SRv6 | Tree-SID | RSVP-TE

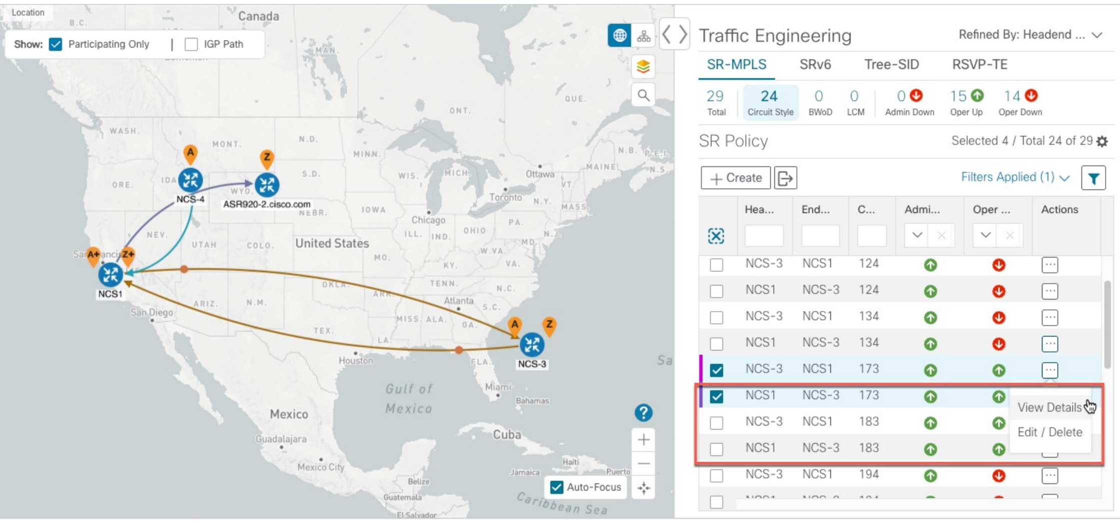
29 Total | 24 Circuit Style | 0 BWoD | 0 LCM | 0 Admin Down | 15 Oper Up | 14 Oper Down

SR Policy   Selected 4 / Total 24 of 29

+ Create   Filters Applied (1)

	Head...	Endp...	Color	Admin S...	Oper Sta...	Actions
☑	NCS1	ASR92...	10483	↑	↓	⋯
□	NCS-4	NCS1	10483	↑	↓	⋯
☑	NCS-3	NCS1	124	↑	↓	⋯
□	NCS1	NCS-3	124	↑	↓	⋯
□	NCS-3	NCS1	134	↑	↓	⋯
☑	NCS1	NCS-3	134	↑	↓	⋯
☑	NCS-3	NCS1	173	↑	↑	⋯
□	NCS1	NCS-3	173	↑	↑	⋯
□	NCS-3	NCS1	183	↑	↑	⋯
□	NCS1	NCS-3	183	↑	↑	⋯
□	NCS-3	NCS1	194	↑	↓	⋯
□	NCS1	NCS-3	194	↑	↓	⋯

Step 3 From the **Actions** column, click ⋯ > **View Details** for the NCS policies.



Traffic Engineering   Refined By: Headend ...

SR-MPLS | SRv6 | Tree-SID | RSVP-TE

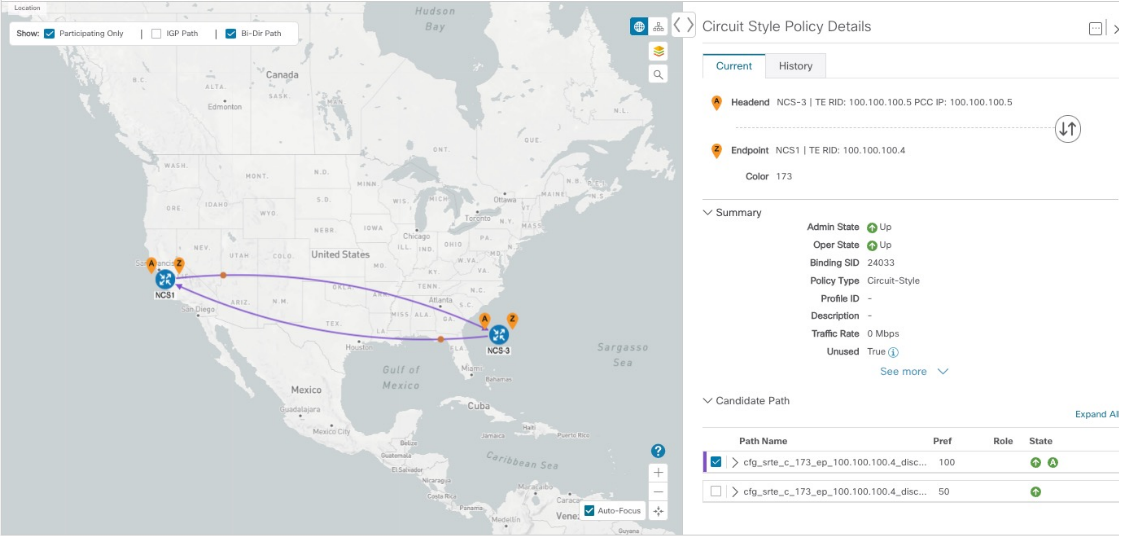
29 Total | 24 Circuit Style | 0 BWoD | 0 LCM | 0 Admin Down | 15 Oper Up | 14 Oper Down

SR Policy   Selected 4 / Total 24 of 29

+ Create   Filters Applied (1)

	Hea...	End...	C...	Admi...	Oper ...	Actions
□	NCS-3	NCS1	124	↑	↓	⋯
□	NCS1	NCS-3	124	↑	↓	⋯
□	NCS-3	NCS1	134	↑	↓	⋯
□	NCS1	NCS-3	134	↑	↓	⋯
☑	NCS-3	NCS1	173	↑	↑	⋯
☑	NCS1	NCS-3	173	↑	↑	View Details
□	NCS-3	NCS1	183	↑	↑	Edit / Delete
□	NCS1	NCS-3	183	↑	↑	
□	NCS-3	NCS1	194	↑	↓	⋯

Crosswork displays the **Circuit Style Policy Details** window in the side panel. By default, the Active path is displayed on the topology map. The display includes the bidirectional paths between NCS-1 and NCS-3 (i=f the **Bi-Dir Path** checkbox is checked).



Circuit Style Policy Details

Current | History

Headend NCS-3 | TE RID: 100.100.100.5 PCC IP: 100.100.100.5

Endpoint NCS1 | TE RID: 100.100.100.4

Color 173

Summary

Admin State Up
Oper State Up
Binding SID 24033
Policy Type Circuit-Style
Profile ID -
Description -
Traffic Rate 0 Mbps
Unused True

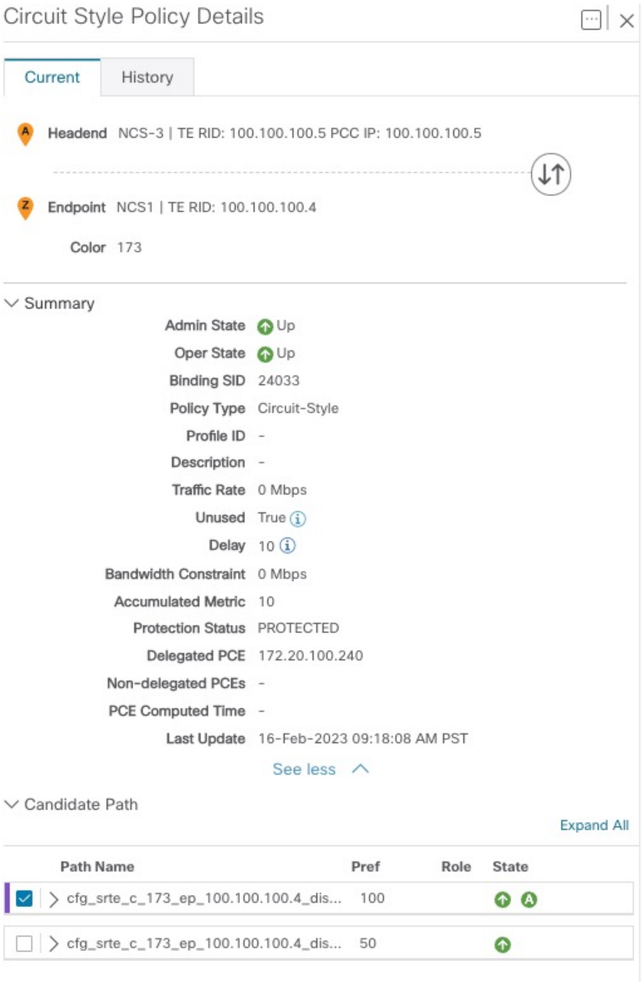
See more

Candidate Path

Expand All

	Path Name	Pref	Role	State
☑	cfg_srte_c_173_ep_100.100.100.4_disc...	100		↑ A
□	cfg_srte_c_173_ep_100.100.100.4_disc...	50		↑

Here is a closer look at the types of Summary details available to you. The **Candidate Path** list at the bottom of the window displays the Active and Protected paths. The Active path is the one that currently takes traffic.



Circuit Style Policy Details

Current | History

Headend NCS-3 | TE RID: 100.100.100.5 PCC IP: 100.100.100.5

Endpoint NCS1 | TE RID: 100.100.100.4

Color 173

Summary

Admin State	Up
Oper State	Up
Binding SID	24033
Policy Type	Circuit-Style
Profile ID	-
Description	-
Traffic Rate	0 Mbps
Unused	True
Delay	10
Bandwidth Constraint	0 Mbps
Accumulated Metric	10
Protection Status	PROTECTED
Delegated PCE	172.20.100.240
Non-delegated PCEs	-
PCE Computed Time	-
Last Update	16-Feb-2023 09:18:08 AM PST

See less

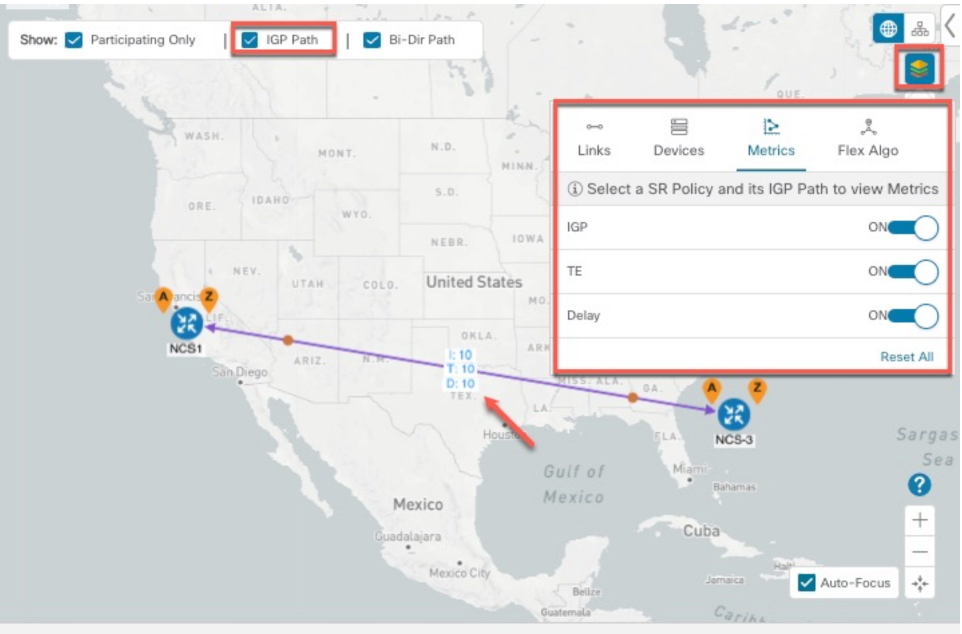
Candidate Path

Expand All

	Path Name	Pref	Role	State
☑	cfg_srte_c_173_ep_100.100.100.4_dis...	100		Up, A
□	cfg_srte_c_173_ep_100.100.100.4_dis...	50		Up

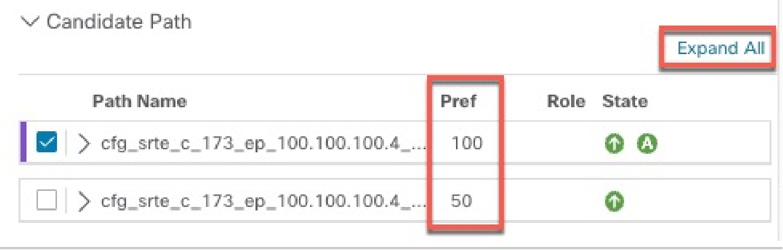
Note The Bandwidth Constraint value may differ from the bandwidth you requested if the value was increased and insufficient resources existed to satisfy demand on all Active and Protected candidate paths.

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



Step 5 View the Active and Protected path configuration details:

a) Within the **CS-SR Policy Details** window, you can drill down to view more information about the Active and Protected paths. In the following example, the Active path has a preference value of 100 and the Protected path has preference value of 50. The operational (Oper State Up) candidate path with the highest preference will always be the Active path (see What Happens When Path Failures Occur?, on page 18). Click **Expand All** to view more information about both the Active and Protected paths.


Candidate Path

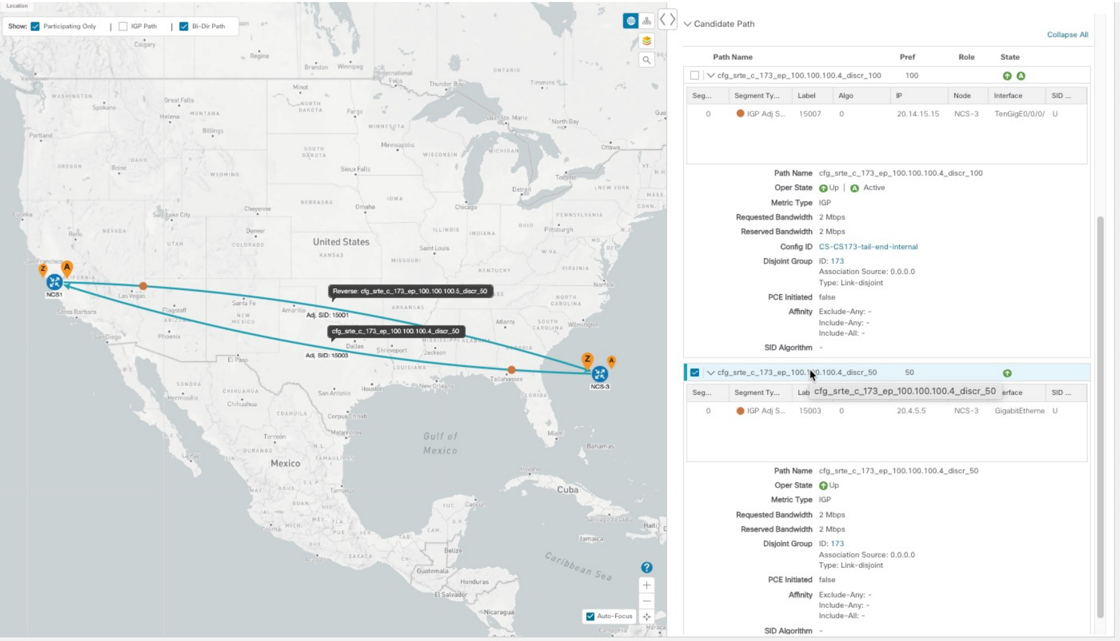
Expand All

	Path Name	Pref	Role	State
☑	cfg_srte_c_173_ep_100.100.100.4_...	100		↑ A
□	cfg_srte_c_173_ep_100.100.100.4_...	50		↑

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.

b) In the following example, the Protected path is checked and displayed on the topology map. If you hover your mouse over the path name, forward and reverse paths are displayed on the topology map.


Location
Show: ☑ Participating Only | □ IGP Path | ☑ Bi-Dir Path
Z
A
NCS1
Reverse: cfg_srte_c_173_ep_100.100.100.5_discr_50
Adj. SID: 15001
cfg_srte_c_173_ep_100.100.100.4_discr_50
Adj. SID: 15003
Z
A
NCS-3
United States
Mexico
Gulf of Mexico
Cuba
Auto-Focus

Candidate Path

Collapse All

	Path Name	Pref	Role	State
□	cfg_srte_c_173_ep_100.100.100.4_discr_100	100		● A

Seg...	Segment Ty...	Label	Algo	IP	Node	Interface	SID ...
0	● IGP Adj S...	15007	0	20.14.15.15	NCS-3	TenGigE0/0/0/	U

Path Name	cfg_srte_c_173_ep_100.100.100.4_discr_100
Oper State	Up | A Active
Metric Type	IGP
Requested Bandwidth	2 Mbps
Reserved Bandwidth	2 Mbps
Config ID	CS-CS173-tail-end-internal
Disjoint Group	ID: 173 Association Source: 0.0.0.0 Type: Link-disjoint
PCE Initiated	false
Affinity	Exclude-Any: - Include-Any: - Include-All: -
SID Algorithm	-

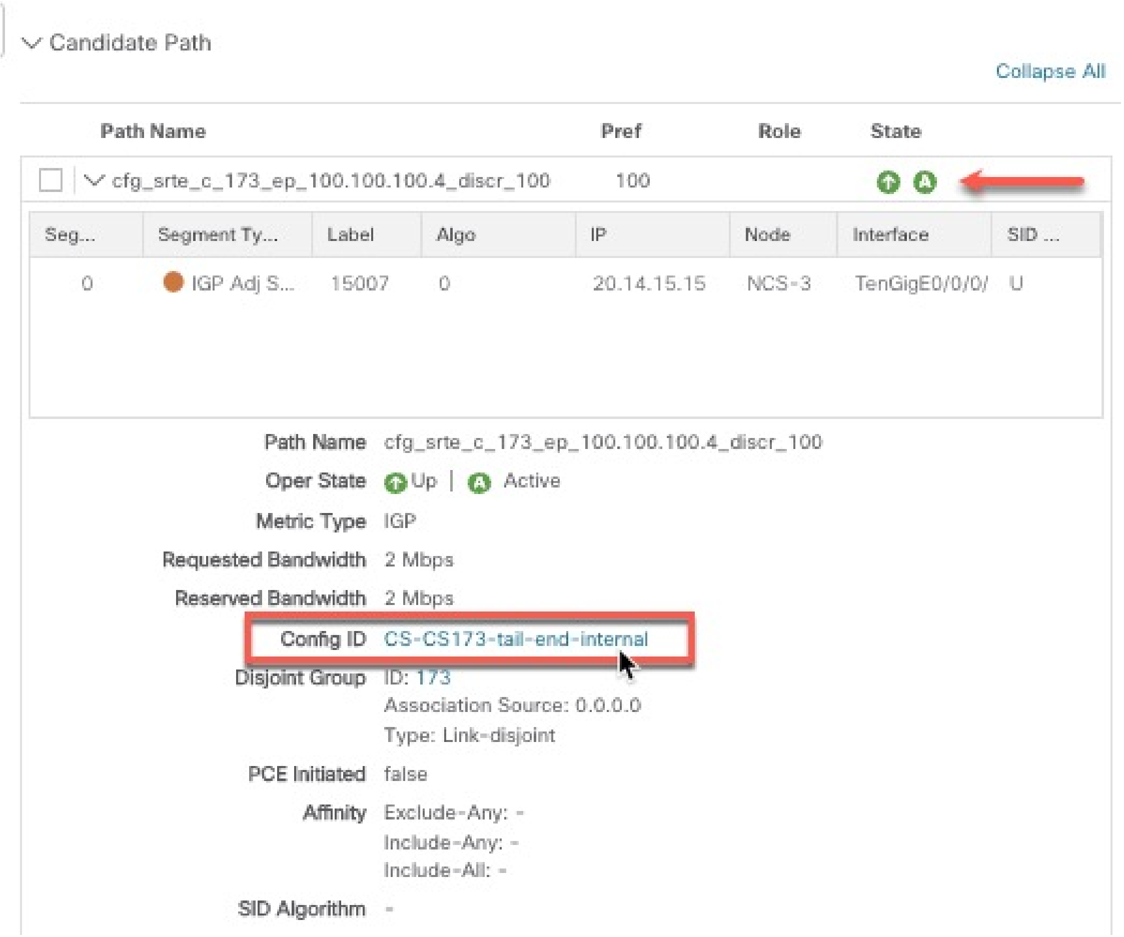
	Path Name	Pref	Role	State
☑	cfg_srte_c_173_ep_100.100.100.4_discr_50	50		●

cfg_srte_c_173_ep_100.100.100.4_discr_50

Seg...	Segment Ty...	Lab				erface	SID ...
0	● IGP Adj S...	15003	0	20.4.5.5	NCS-3	GigabitEtherne	U

Path Name	cfg_srte_c_173_ep_100.100.100.4_discr_50
Oper State	Up
Metric Type	IGP
Requested Bandwidth	2 Mbps
Reserved Bandwidth	2 Mbps
Disjoint Group	ID: 173 Association Source: 0.0.0.0 Type: Link-disjoint
PCE Initiated	false
Affinity	Exclude-Any: - Include-Any: - Include-All: -
SID Algorithm	-

c) Here is a closer view of an Active path's configuration details. Notice that it is designated with the "A" icon under **State** to indicate that it is currently the operational Active path. Also, if the policy configuration was done through Cisco Crosswork, you have the option to view the policy configuration. To see the configuration, click the link next to **Config ID**.



Candidate Path

	Path Name	Pref	Role	State
□	cfg_srte_c_173_ep_100.100.100.4_discr_100	100		↑ A

Seg...	Segment Ty...	Label	Algo	IP	Node	Interface	SID ...
0	● IGP Adj S...	15007	0	20.14.15.15	NCS-3	TenGigE0/0/0/	U

Path Name	cfg_srte_c_173_ep_100.100.100.4_discr_100
Oper State	↑ Up | A Active
Metric Type	IGP
Requested Bandwidth	2 Mbps
Reserved Bandwidth	2 Mbps
Config ID	CS-CS173-tail-end-internal
Disjoint Group	ID: 173 Association Source: 0.0.0.0 Type: Link-disjoint
PCE Initiated	false
Affinity	Exclude-Any: - Include-Any: - Include-All: -
SID Algorithm	-

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 SR Circuit Style Manager, on page 21) 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.

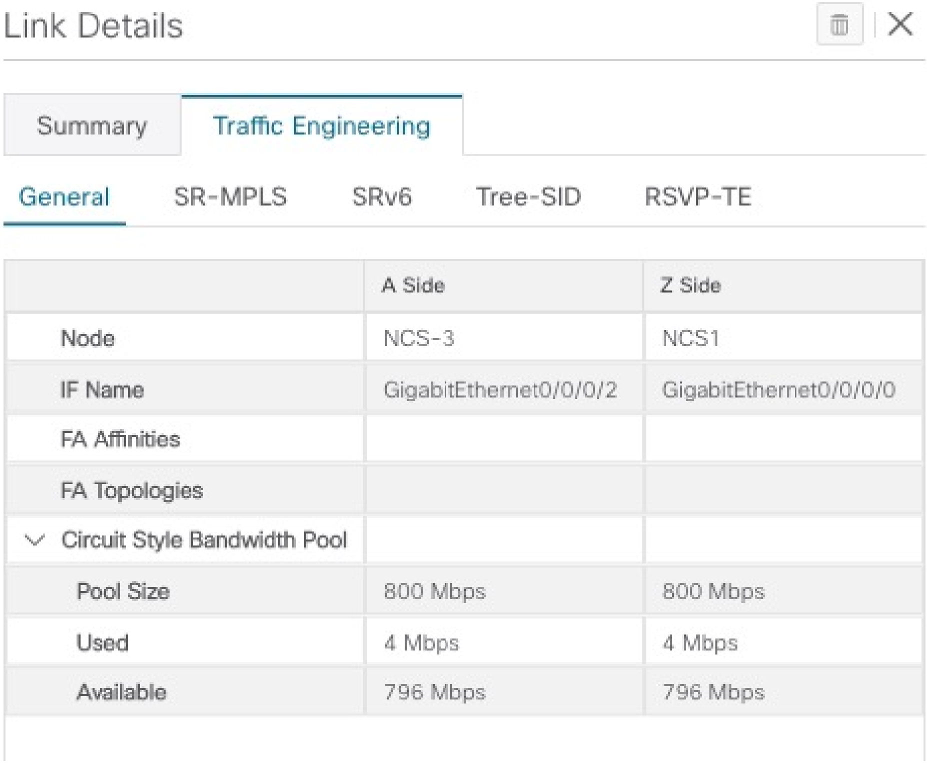
Step 3 On the topology map, click on a participating Circuit Style SR-TE policy node to display the **Device Details** for that node.

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 Click on the **Traffic Engineering** tab, then **General**. 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 what 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.



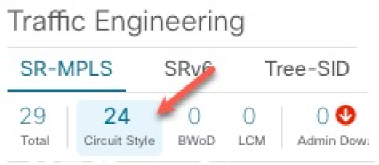
	A Side	Z Side
Node	NCS-3	NCS1
IF Name	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/0
FA Affinities		
FA Topologies		
Circuit Style Bandwidth Pool		
Pool Size	800 Mbps	800 Mbps
Used	4 Mbps	4 Mbps
Available	796 Mbps	796 Mbps

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 18.

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 Active path is displayed and shows 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.

Click the **Show 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**.

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.