



Cisco Crosswork Optimization Engine 3.0 User Guide

First Published: 2021-11-12

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1	Overview of Cisco Crosswork Optimization Engine	1
	Audience	1
	Overview of Cisco Crosswork Optimization Engine	1
	Crosswork Optimization Engine APIs	2
	Crosswork Optimization Engine and the Crosswork Network Controller Solution	3
	Segment Routing Path Computation Element (SR-PCE)	3
	About Segment Routing	3
	About Resource Reservation Protocol (RSVP)	6
CHAPTER 2	Set Up and Monitor Your Network View	9
	Get a Quick View in the Dashboard	9
	View Devices and Links on the Topology Map	10
	View Device and Link Details	12
	Use Device Groups to Filter Your Topology View	17
	Create and Modify Device Groups	20
	Enable Dynamic Device Grouping	21
	Customize Map Display Settings	22
	Customize the Display of Links and Devices	22
	Set Display Behavior of Device Groups for TE Tunnels	22
	Customize the Display of Traffic Engineering	23
	Configure Timeout Settings	23
	Save Topology Views for Easy Access	23
CHAPTER 3	Visualize SR-MPLS and SRv6 Policies	25
	View SR-MPLS and SRv6 Policies on the Topology Map	25

	View SR-MPLS and SRv6 Policy Details	27
	View Traffic Engineering Device Details	29
	Visualize SR-MPLS or SRv6 Policies Example	30
	Find Multiple Candidate Paths (MCPs)	37
	Visualize Underlying Paths Associated with a Defined Binding-Segment ID (B-SID) Label	41
	Visualizing Native SR Paths	43
	Visualize Native Path Device Prerequisites	45
<hr/>		
CHAPTER 4	Visualize Flexible Algorithms	47
	Visualize Flexible Algorithm	47
	Configure Flexible Algorithm Affinities	49
	Find Flexible Algorithms for Links and Devices	50
<hr/>		
CHAPTER 5	Visualize RSVP-TE Tunnels	53
	View RSVP-TE Tunnels on the Topology Map	53
	View RSVP-TE Tunnel Details	55
	View Traffic Engineering Device Details	57
<hr/>		
CHAPTER 6	Provision SR-MPLS Policies	59
	SR-MPLS Policy Support	59
	SR-TE Policy Configuration Sources	61
	PCC-Initiated SR-TE Policy Example	61
	Create Explicit SR-MPLS Policies	62
	Configure Link Affinities	63
	Create Dynamic SR-MPLS Policies Based on Optimization Intent	63
	Modify SR-MPLS Policies	64
<hr/>		
CHAPTER 7	Provision RSVP-TE Tunnels	67
	RSVP-TE Tunnel Support	67
	RSVP-TE Tunnel Configuration Sources	68
	PCC-Initiated RSVP-TE Tunnel Example	69
	Create Explicit RSVP-TE Tunnels	69
	Configure Link Affinities	70
	Create Dynamic RSVP-TE Tunnels Based on Optimization Intent	70

Modify RSVP-TE Tunnels 71

CHAPTER 8**Use Local Congestion Mitigation (LCM) to Mitigate Network Congestion Locally 73**

Local Congestion Mitigation Overview 73

LCM Important Notes 74

LCM Platform Requirements 74

BGP-LS Speaker Placement for Multiple AS Networks with a Dedicated IGP Instance Between ASBRs 75

Previously Monitored Interfaces Missing After Upgrade 76

LCM Calculation Workflow 76

Mitigate Congestion on Local Interfaces Example 78

Configure LCM 85

Add Individual Interface Thresholds 87

Monitor LCM Operations 87

CHAPTER 9**Use Bandwidth Optimization (BWOpt) to Optimize the Network 89**

Bandwidth Optimization Overview 89

BWOpt Important Notes 89

Automated Network Congestion Mitigation Example 91

Configure Bandwidth Optimization 94

Add Individual Interface Thresholds 95

Troubleshoot Bandwidth Optimization 95

CHAPTER 10**Define and Maintain Intent-Based Bandwidth Requirements 97**

BWoD Important Notes 97

Provision an SR-TE Policy to Maintain Intent-Based Bandwidth Requirements Example 98

PCC-Initiated BWoD SR-TE Policies 100

Configure Bandwidth on Demand 101

Troubleshoot BWoD 101



CHAPTER 1

Overview of Cisco Crosswork Optimization Engine

This is a post-installation document intended to cover the steps required to get up and running with Cisco Crosswork Optimization Engine and start using the user interface (UI). For administrative tasks including device and user management, see the *Cisco Crosswork Infrastructure and Applications Administration Guide*.

- [Audience, on page 1](#)
- [Overview of Cisco Crosswork Optimization Engine, on page 1](#)
- [Crosswork Optimization Engine APIs, on page 2](#)
- [Crosswork Optimization Engine and the Crosswork Network Controller Solution, on page 3](#)
- [Segment Routing Path Computation Element \(SR-PCE\), on page 3](#)
- [About Segment Routing, on page 3](#)
- [About Resource Reservation Protocol \(RSVP\), on page 6](#)

Audience

This guide is for experienced network administrators who want to use Cisco Crosswork Optimization Engine in their network. This guide assumes that you are experienced and familiar with using the following technologies:

- Networking technologies and protocols (BGP-LS, IGP (OSPF and IS-IS), PCEP, model-driven telemetry, and so on)
- Traffic Engineering (TE) Tunnels:
 - RSVP-TE tunnel provisioning
 - Segment Routing Traffic Engineering (SR-TE) policy provisioning
- Cisco Segment Routing Path Computation Element (SR-PCE)

Overview of Cisco Crosswork Optimization Engine

Crosswork Optimization Engine is part of the Cisco Crosswork Network Automation suite of products and provides the ability to preserve network intent with proactive network monitoring, network visualization, and

closed loop automation. It also provides real-time network optimization allowing operators to effectively maximize network utilization and increase service velocity.

Crosswork Optimization Engine provides the following:

- A topology map that gives valuable real-time network visualization of the following:
 - devices
 - links and link utilization
 - provisioned SR-TE (SR-MPLS and SRv6) policies and RSVP-TE tunnels
- A UI that allows the network operator to perform the following tasks:
 - Provision SR-MPLS policies and RSVP-TE tunnels and modify or remove them using an intuitive workflow
 - Preview an SR-MPLS policy or RSVP-TE tunnel before deploying it to the network
 - Continuously track SR-MPLS policy dynamic path computations to maintain SLA objectives (with correct licensing)
 - Visualize SR-TE policies and RSVP-TE tunnels that are created directly on the network devices providing a comprehensive view of the active network configuration
 - Visualize Flexible Algorithms in the network.
- APIs that extend Crosswork Optimization Engine functions to other Crosswork applications and third party applications.
- Crosswork Optimization Engine feature packs (available with correct licensing) provide congestion mitigation and closed loop bandwidth optimization. A user defines the optimization intent and the tools implement the intent, and continuously monitor, track, and react to maintain the original intent.

This guide covers the capabilities that are allowed by the Crosswork Optimization Engine. However, either due to licensing or the configuration of the role that is associated with your user account, you may not be able to access the features and functions.

For licensing and ordering information, work with your Cisco Partner or Cisco Sales representative to review an option described in the "Cisco Crosswork Optimization Engine Ordering Guide".

Crosswork Optimization Engine APIs

Advanced users can integrate other Crosswork applications and third-party applications with Crosswork Optimization Engine functions by using application programming interfaces (APIs) delivering new capabilities into their network operations.

For more information, see the [Cisco Crosswork Network Automation API Documentation on Cisco DevNet](#).

Crosswork Optimization Engine and the Crosswork Network Controller Solution

Cisco Crosswork Network Controller is a turnkey network automation solution for deploying and operating IP transport networks that delivers increased service agility, cost efficiency, and optimization for faster time-to-customer value and lower operating cost. The solution combines intent-based network automation to deliver critical capabilities for service orchestration and fulfillment, network optimization, service path computation, device deployment and management, and anomaly detection and automatic remediation. For more information, see [Cisco Crosswork Network Controller](#).

Throughout this document, when using the Crosswork Optimization Engine as part of the Crosswork Network Controller solution, some options are not available or are slightly different. For example, to navigate to the Traffic Engineering UI, instead of **Traffic Engineering > Traffic Engineering**, the navigation within the Crosswork Network Controller solution is **Services & Traffic Engineering > Traffic Engineering**.

Segment Routing Path Computation Element (SR-PCE)

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

Cisco SR-PCE (formerly Cisco XR Traffic Controller (XTC)) runs on the Cisco IOS XR operating system. SR-PCE provides stateful PCE functionality that helps control and reroute TE tunnels to optimize the network. PCE describes a set of procedures by which a Path Computation Client (PCC) can report and delegate control of headend tunnels that are sourced from the PCC to a PCE peer. The PCC and PCE establish a Path Computation Element Communication Protocol (PCEP) connection that SR-PCE uses to push updates to the network.

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



Note For more information, see the [Crosswork Optimization Engine Release Notes](#) for SR-PCE version support and compatibility.

About Segment Routing

Segment routing is a method of forwarding packets on the network that are based on the source routing paradigm. The source selects a path and encodes it in the packet header as an ordered list of segments. Segments are an identifier for any type of instruction. For example, topology segments identify the next hop toward a destination. The segment ID (SID) consisting of an unsigned 32-bit integer identifies each segment.

With segment routing for traffic engineering (SR-TE), the network no longer must maintain a per-application and per-flow state. Instead, it simply obeys the forwarding instructions that are provided in the packet.

Segments

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

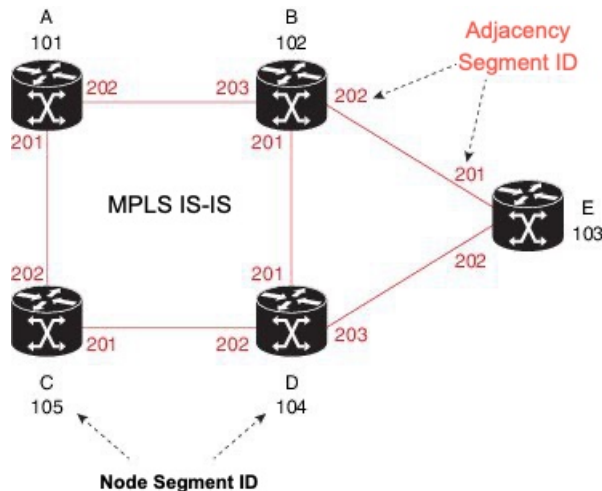
- A prefix SID is associated with an IP prefix. The prefix SID is manually configured from the segment routing global block (SRGB) range of labels, and is distributed by IS-IS or OSPF. The prefix segment steers the traffic along the shortest path to its destination. A node SID is a special type of prefix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

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

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

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

The following diagram shows a basic network with the Node SID and the Adjacency SID for each of the devices and connections between the devices noted.



Segment Routing Policies

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

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

Dynamic SR Policy

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

to a path computation engine (PCE). If a path isn't found, then the policy becomes operationally down (operation status down) and packets will not be routed based on the policy.

Explicit SR Policy

When you configure an explicit policy, you specify an explicit path which consists of a list of prefix or adjacency SIDs, each representing a node or link along on the path. Each segment is an end-to-end path from the source to the destination, and instructs the routers in the network to follow the specified path instead of the shortest path calculated by the IGP. If a packet is steered into an SR policy, the SID list is pushed on the packet by the headend. The rest of the network executes the instructions embedded in the SID list.



Note For PCC-initiated policies, if the explicit path is configured in the form of IP addresses, the policy goes operational status down if one of the hops goes down. If it is configured as a list of labels, then the policy goes operational status down only if it is the first hop that goes down. The remaining hops are not resolved by the PCC and so it will not take the policy operational status down if they fail.

Segment Routing over MPLS (SR-MPLS)

Segment Routing can be applied on an MPLS data plane. In an SR-MPLS enabled network, an MPLS label represents an instruction. The source nodes programs the path to a destination in the packet header as a stack of labels. For more information, see [IETF RFC 8660 Segment Routing with the MPLS Data Plane](#).

Segment Routing over IPv6 (SRv6)

Segment Routing over IPv6 (SRv6) extends Segment Routing support with an IPv6 data plane. SRv6 introduces the Network Programming framework that enables a network operator or an application to specify a packet processing program by encoding a sequence of instructions in the IPv6 packet header. Each instruction is implemented on one or several nodes in the network and identified by an SRv6 Segment Identifier (SID) in the packet. For more information, see [IETF RFC 8986 SRv6 Network Programming](#).

In SRv6, an IPv6 address represents an instruction. SRv6 uses a new type of IPv6 Routing Extension Header, called the Segment Routing Header (SRH), in order to encode an ordered list of instructions. The active segment is indicated by the destination address of the packet, and the next segment is indicated by a pointer in the SRH.

For more information, see <https://www.segment-routing.net/>.

SRv6 Limitations

- Cisco IOS XR 7.3.2 only supports SRv6 visualization with IS-IS IGP.
- Traffic collection on SRv6 policies is not currently supported.
- OSPFv3 IGP (PCE-initiated) SRv6 policies are not supported.
- SRv6 is not supported on Bandwidth Optimization, Bandwidth on Demand, or Local Congestion Mitigation feature packs.
- IPv4 and IPv6 topologies must be congruent. Different link metrics for IPv4 and IPv6 are not supported.
- Visualization of PCC-initiated dynamic path SRv6 policies only. PCE-initiated and explicit path are not supported.

Segment Routing for Traffic Engineering

SR-TE takes place through a policy between a source and destination pair. SR-TE uses the concept of source routing, where the source calculates the path and encodes it in the packet header as a segment.

SR-TE utilizes network bandwidth more effectively than traditional MPLS-TE networks by using ECMP at every segment level. It uses a single intelligent source and relieves remaining routers from the task of calculating the required path through the network.

Disjointness

Crosswork can use a disjoint policy to compute two unique paths that steer traffic from the same source and destination avoiding common specified resources (links or nodes). This results in no single point of failure in steering traffic through the network. The following disjoint path computations are supported:

- **Link** – Specifies that links are not shared on the computed paths.
- **Node** – Specifies that nodes are not shared on the computed paths.
- **SRLG** – Specifies that links with the same Share Risk Link Group (SRLG) value are not shared on the computed paths.
- **SRLG-node** – Specifies that SRLG and nodes are not shared on the computed paths.



Note

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

Related Links

[Provision SR-MPLS Policies](#), on page 59

[Configure Link Affinities](#), on page 63

About Resource Reservation Protocol (RSVP)

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

The RSVP-TE process contains the following functionalities:

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

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

RSVP-TE Explicit Routing (Strict, Loose)

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

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

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

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



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

RSVP FRR

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

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

The Record Route Object (RRO) reports in the RESV message the availability or use of local protection on an LSP, and whether bandwidth and node protection are available for that LSP.

The signaling of the FRR requirements is initiated at the TE tunnel headend. Points of Local Repair (PLR) along the path act on the FRR requirements based on the backup tunnel availability at the PLR, and signal the backup tunnel selection information to the headend. When an FRR event is triggered, the PLR sends PATH messages through the backup tunnel to the merge point (MP) where the backup tunnel rejoins the original LSP. The MP also sends RESV messages to the PLR using the RSVP-Hop object that is included by the PLR in its PATH message. This process prevents the original LSP from being torn down by the MP. Also, the PLR signals the tunnel headend with a PATH-ERROR message to indicate the failure along the LSP and that FRR is in active use for that LSP. This information is used by the headend to signal a new LSP for the TE tunnel, and to tear down the existing failed path after the new LSP is set up through make-before-break techniques.



CHAPTER 2

Set Up and Monitor Your Network View

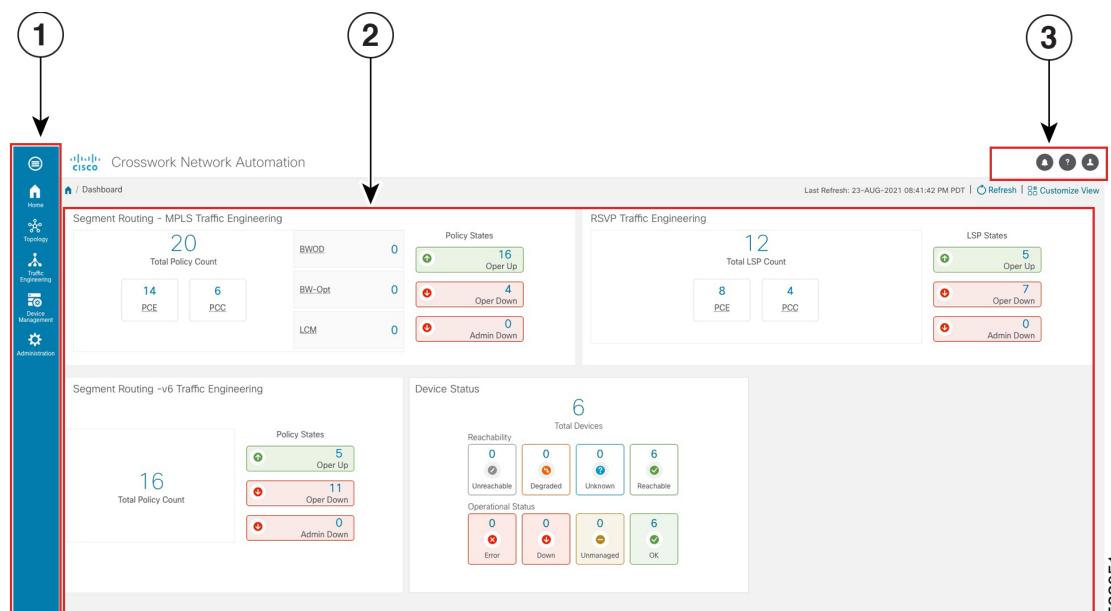
Familiarize yourself with the UI and set up your network view before managing SR policies and RSVP-TE tunnels. This section contains the following topics:

- [Get a Quick View in the Dashboard, on page 9](#)
- [View Devices and Links on the Topology Map, on page 10](#)
- [Use Device Groups to Filter Your Topology View, on page 17](#)
- [Customize Map Display Settings, on page 22](#)
- [Configure Timeout Settings, on page 23](#)
- [Save Topology Views for Easy Access, on page 23](#)





Get a Quick View in the Dashboard

The Home page displays a customizable collection of dashlets which provide an at-a-glance operational summary of the network being managed, including reachability and operational status of devices. Each dashlet represents different types of data belonging to the same category.

Figure 1: Crosswork Home page



522051

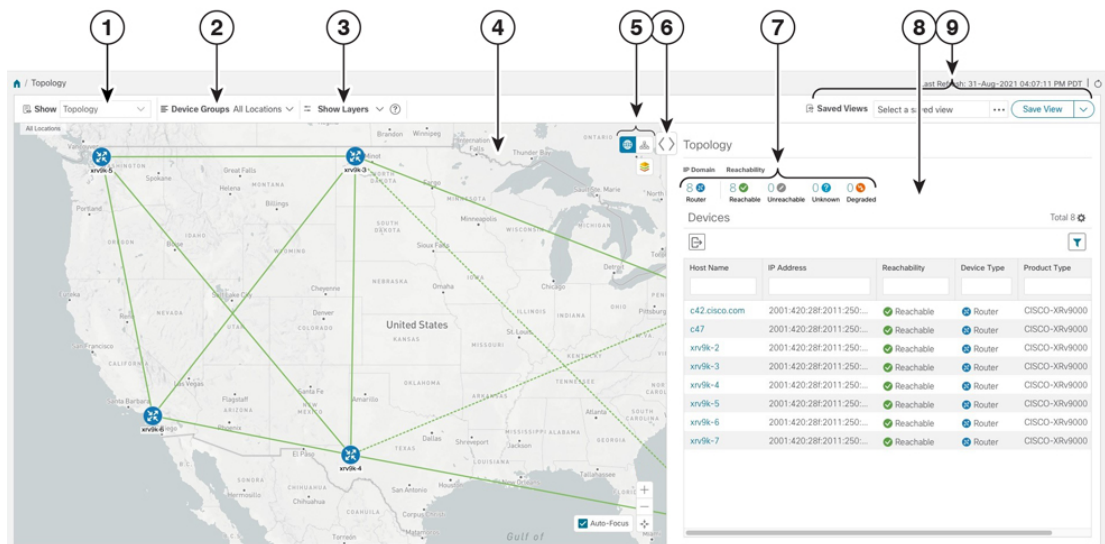
Callout No.	Description
1	Main Menu: The main menu allows you to navigate to installed Cisco Crosswork applications and device management and administrative tasks. Menu options may look slightly different depending on what Cisco Crosswork applications are installed.
2	Dashlets: Information varies depending on what Cisco Crosswork applications are installed. <ul style="list-style-type: none"> To drill down for more information within a dashlet, click on a value. A window appears displaying only the filtered data you clicked on. To add or change the layout of dashlets, click Customize View. Move the dashlets to your desired layout and click Save.
3	Settings icons: <ul style="list-style-type: none">  The Alerts icon notifies you of any current error conditions related to the system operations which require attention, and provides a link to detailed information about those conditions.  The Events icon notifies you of new events related to system operation, and also provides access to the history of all system events.  The About icon displays the current version of the Cisco Crosswork product.  The User Account icon lets you view your username, change your password, and log out.

View Devices and Links on the Topology Map


To view the network topology map, from the main menu choose **Topology**.




For more information, see [View Device and Link Details](#), on page 12.

Figure 2: Cisco Crosswork UI and Topology Map



522060

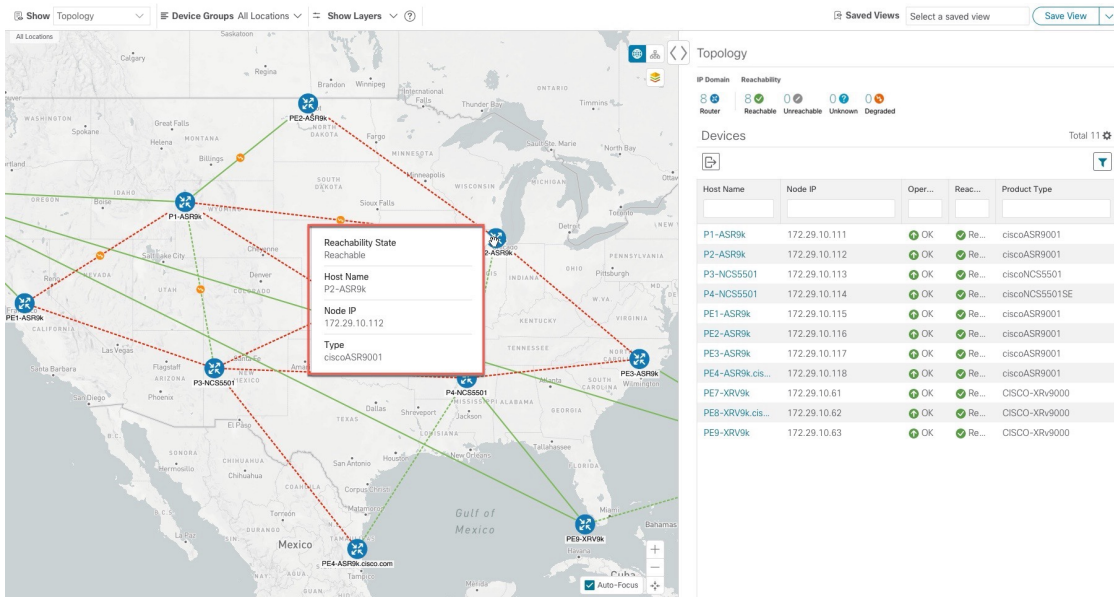
Callout No.	Description
1	<p>Topology Map View: From the Show drop-down list, click the option that displays the data that you would like to see on the map.</p> <p>If Topology is selected, devices and links in the network are displayed.</p> <p>If Traffic Engineering is selected, TE tunnel information is displayed. For more information on the Traffic Engineering topology map, see View SR-MPLS and SRv6 Policies on the Topology Map, on page 25 and View RSVP-TE Tunnels on the Topology Map, on page 53.</p>
2	<p>Device Groups: From the drop-down list, click the group of devices you want displayed on the map. All other device groups will be hidden.</p>
3	<p>Show Hide: From the drop-down list, click the network layers you want displayed on the map. All devices and links that belong to the selected layers are then displayed. By default, all layers are displayed.</p>
4	<p>Topology Map: The network topology can be displayed on a logical map or a geographical map, where the devices and links are shown in their geographic context. From the map, you can drill down to get detailed information about devices and links.</p> <p>Devices:</p> <ul style="list-style-type: none"> • To view a device configuration summary, hover the mouse cursor over the device icon. A pop up window displaying the host name, state, node ID, and device type appears. • To view device details, click on the device icon. • If devices are in close physical proximity, the geographical map shows them as a cluster. <p>The number in a blue circle () indicates the number of devices in the cluster. Displaying devices in this manner helps prevent overlap and clutter on the map.</p> <p>Links:</p> <ul style="list-style-type: none"> • A solid line indicates a <i>single link</i> between two devices. If there is more than one link between two devices, or between a device and a cluster of devices, the line is shown dashed instead. A dashed line indicates an <i>aggregated</i> link that represents more than one link, or the use of multiple protocols (for example, IPv4 and IPv6) on the same physical link. • A and Z indicates headend and endpoint, respectively. • To view link information details, click on the link. <p>Note Although aggregated, dual stack links show as one single line.</p>

Callout No.	Description
5	<p>: The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm.</p> <p>: The geographical map shows single devices, device clusters, links, and tunnels, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory.</p> <p>: The Display Preferences window allows you to change display settings for devices, links, utilization, Flexible Algorithms, and TE tunnel metrics.</p>
6	Expand/Collapse/Hide Side Panel: Expand or collapse the contents of the side panel. Close the side panel to get a larger view of the topology map.
7	The Mini Dashboard provides a summary of the IP Domain and device reachability status. If filters are applied, the Mini Dashboard is updated to reflect what is displayed in the Devices table.
8	The content of this window changes depending on what Show is set to for the Topology Map and if you have selected to view more information on a device, link, SR-MPLS policy, SRv6 policy, or RSVP-TE tunnel.
9	Saved Custom Map Views: Lets you create a named custom view using the settings and layout for your current map, settings of the tables saved in the saved views, or display a custom view you have created previously. It also saves any filters applied to the Devices and Traffic Engineering tables.

View Device and Link Details

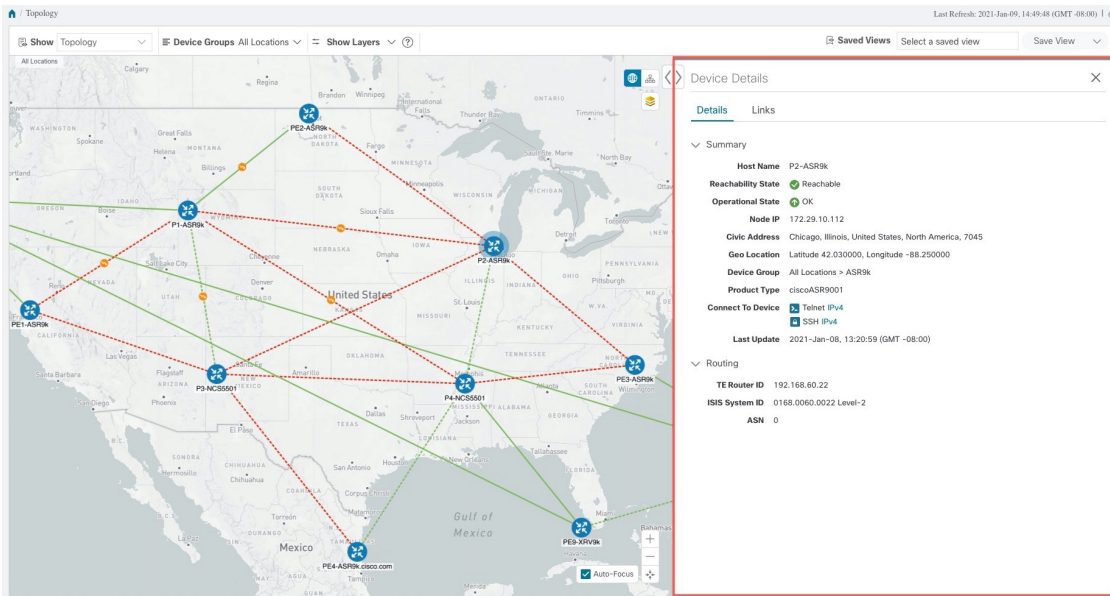
This example shows how you can view device and link details (including Link Aggregation Group (LAG) details, see Step 6) using the topology map.

-
- Step 1** From the main menu choose **Topology** or **Traffic Engineering > Traffic Engineering**.
- Step 2** To quickly view the host name, reachability state, IP address and type of device, hover the mouse over the device icon.



Step 3 To view more device details, click on the device icon.

a) The following examples show the Device details from the Topology map.



In a multiple IGP setup, you can also view all the IGP, IS-IS, and OSPF processes in the Routing details. See the following examples:

Figure 3: Multiple IGP: OSPF Processes

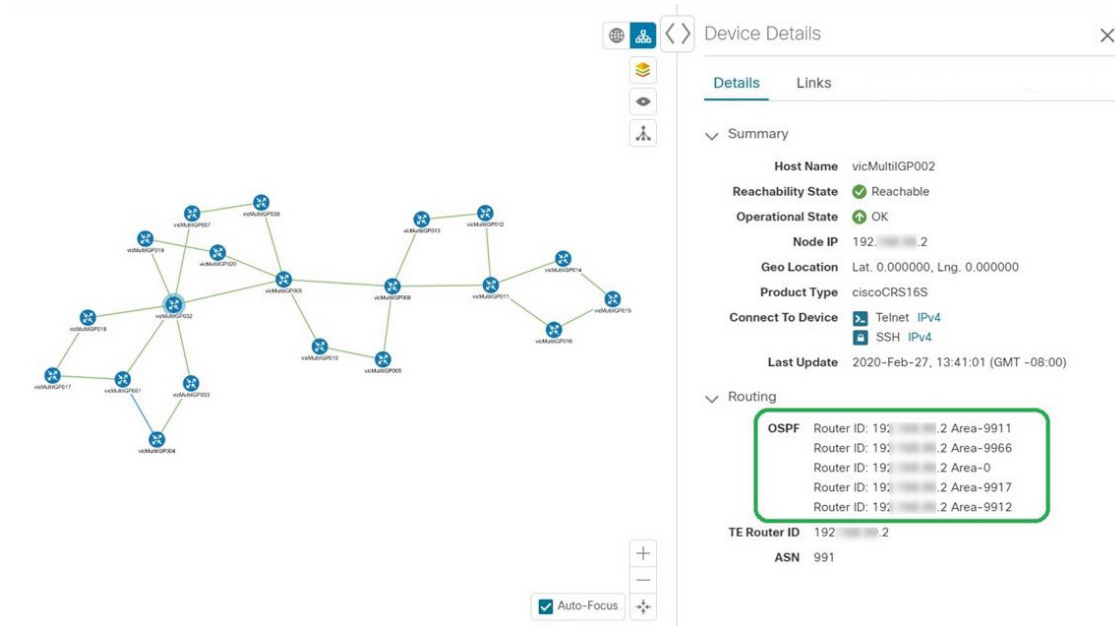


Figure 4: Multiple IGP: ISIS Processes

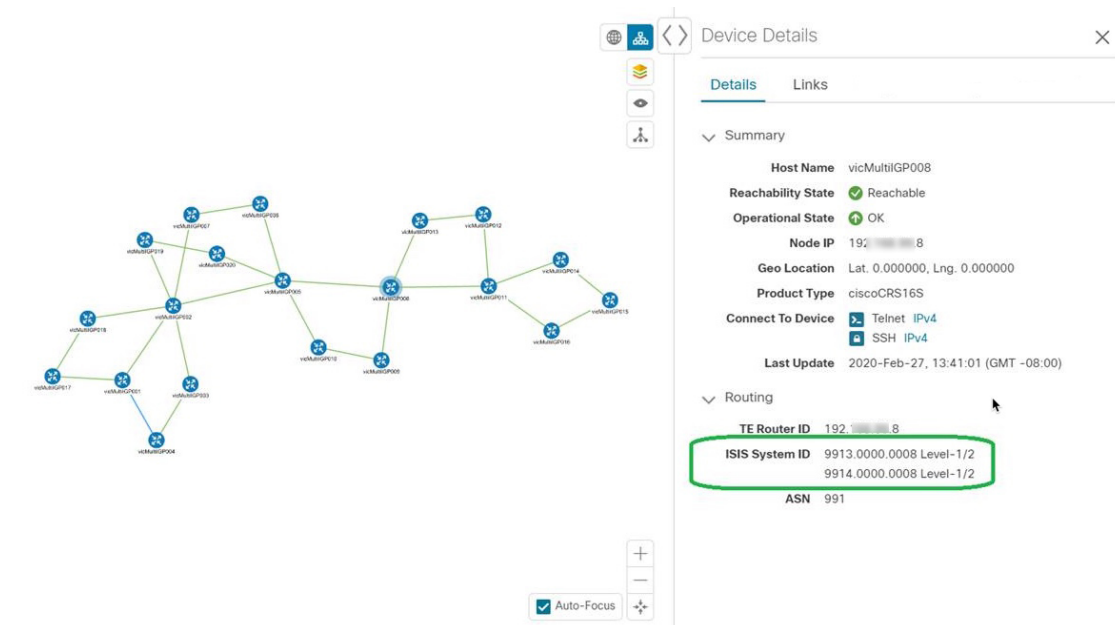
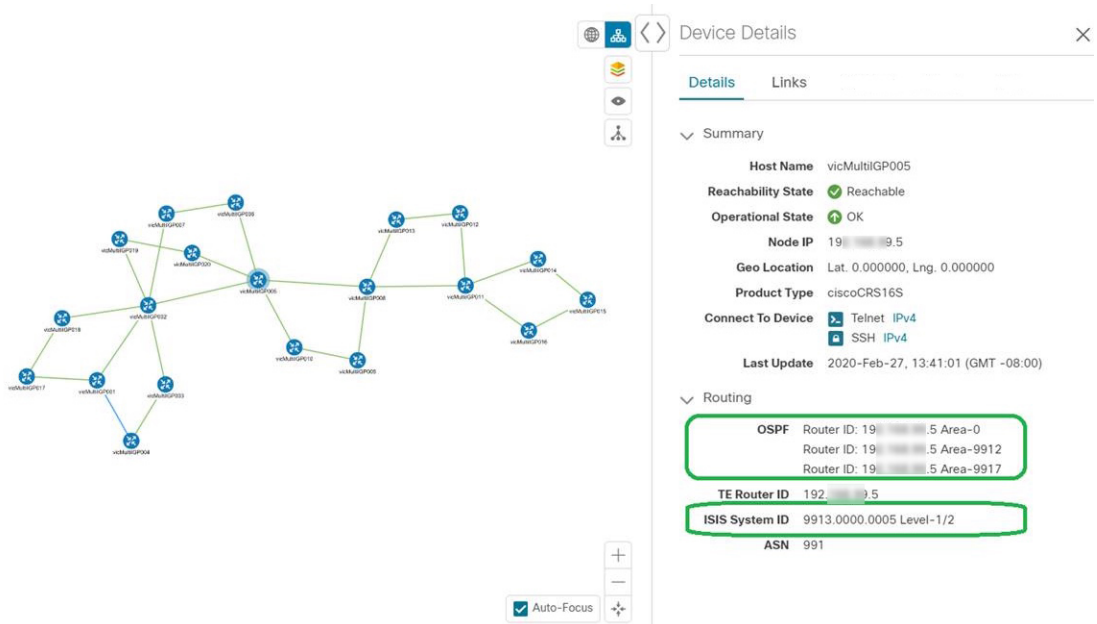
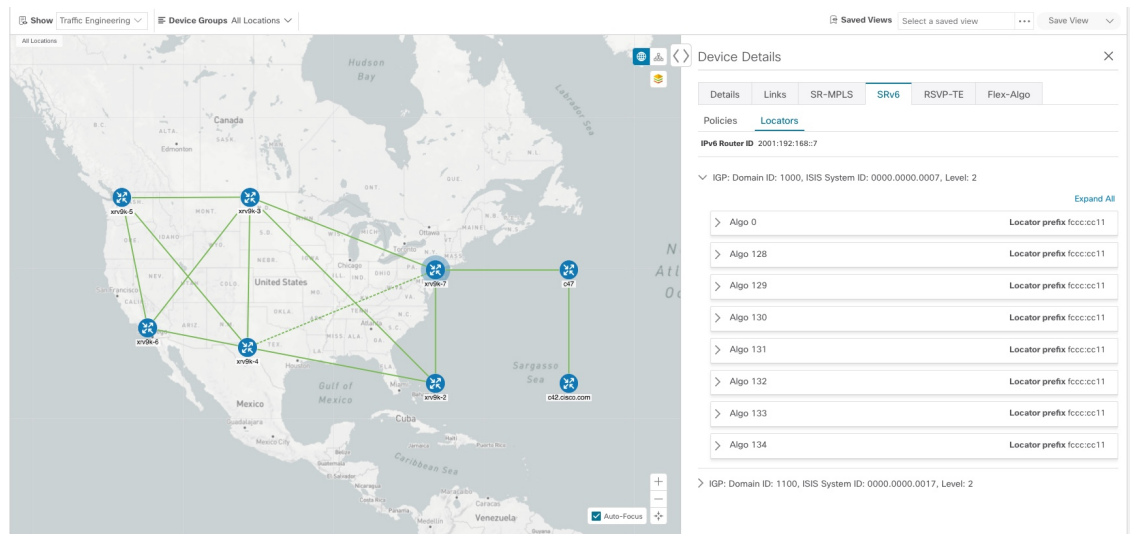


Figure 5: Multiple IGP: OSPF and ISIS Processes



- b) The following example shows additional Traffic Engineering Device details (SR-MPLS, SRv6, RSVP-TE, and Flexible Algorithm tabs) from the Traffic Engineering map. In this particular example, SRv6 Locators are listed for two domains.



Step 4 To view links on the device, click the **Links** tab and expand the right panel to see all the link details.

View Device and Link Details

Device Details

Links

Links on Device P2-ASR9k

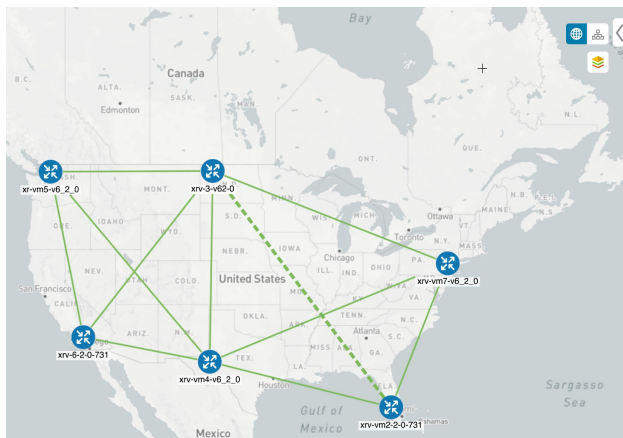
Total 14

State	Link Type	A Side Interface	Z Side Interface	A Side Utilization	Z Side Utilization
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	15.35% (153.5Mbps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	15.35% (153.5Mbps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/2	20.34% (203.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/4	GigabitEthernet0/0/0/2	20.34% (203.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 CDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/7	8.14% (81.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/7	8.14% (81.4Mbps/1Gbps)	0% (0Bps/1Gbps)
🟡	L2 LLDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/3	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
🟢	L2 CDP	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/4	0% (0Bps/1Gbps)	7.33% (73.3Mbps/1Gbps)
🟢	L2 LLDP	GigabitEthernet0/0/0/5	GigabitEthernet0/0/0/6	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
🟡	L2 LLDP	GigabitEthernet0/0/0/2	GigabitEthernet0/0/0/4	0% (0Bps/1Gbps)	7.33% (73.3Mbps/1Gbps)
🟢	L3 ISIS IPV4	Bundle-Ether9	Bundle-Ether9	0% (0Bps/1Gbps)	22.39% (223.9Mbps/1Gbps)

Step 5 Collapse the side panel and close the **Device Details** window.

Step 6 Click on a dashed line. A dashed line indicates an aggregated link that represents more than one link.

Note Dual stack links (although aggregate) are shown as one single line.



Links

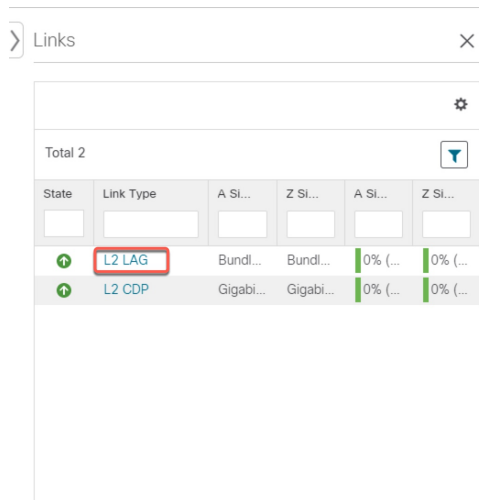
Total 5

State	Link Type	A Side Interface	Z Side Interface
🟢	L3 ISIS IPV6	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
🟢	L2 LLDP	GigabitEthernet0/0/0/6	GigabitEthernet0/0/0/6
🟢	L3 ISIS IPV4	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
🟢	L2 LLDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
🟢	L2 LAG	Bundle-Ether2	Bundle-Ether2

To view different bundle members and member details in a Link Aggregation Group (LAG), confirm that LAG discovery is enabled (**Administration > Settings > System Settings tab > Discovery > LAG** checkbox):

Note It takes a few minutes for LAG collection to complete after LAG discovery is enabled.

a) Click on a LAG link. For example:

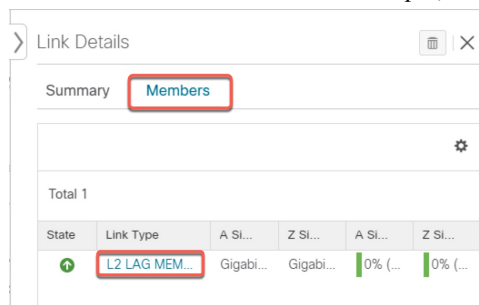


Links

Total 2

State	Link Type	A Si...	Z Si...	A Si...	Z Si...
Up	L2 LAG	Bundl...	Bundl...	0% (...)	0% (...)
Up	L2 CDP	Gigabi...	Gigabi...	0% (...)	0% (...)

b) Click the **Members** tab. In this example, only one link is displayed.



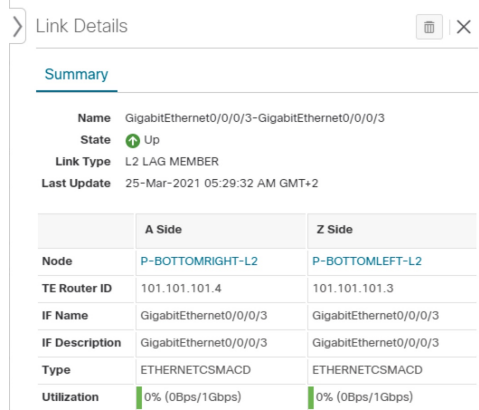
Link Details

Summary **Members**

Total 1

State	Link Type	A Si...	Z Si...	A Si...	Z Si...
Up	L2 LAG MEM...	Gigabi...	Gigabi...	0% (...)	0% (...)

c) Click the LAG member link.



Link Details

Summary

Name GigabitEthernet0/0/0/3-GigabitEthernet0/0/0/3
State Up
Link Type L2 LAG MEMBER
Last Update 25-Mar-2021 05:29:32 AM GMT+2

	A Side	Z Side
Node	P-BOTTOMRIGHT-L2	P-BOTTOMLEFT-L2
TE Router ID	101.101.101.4	101.101.101.3
IF Name	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/3
IF Description	GigabitEthernet0/0/0/3	GigabitEthernet0/0/0/3
Type	ETHERNETCSMACD	ETHERNETCSMACD
Utilization	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)

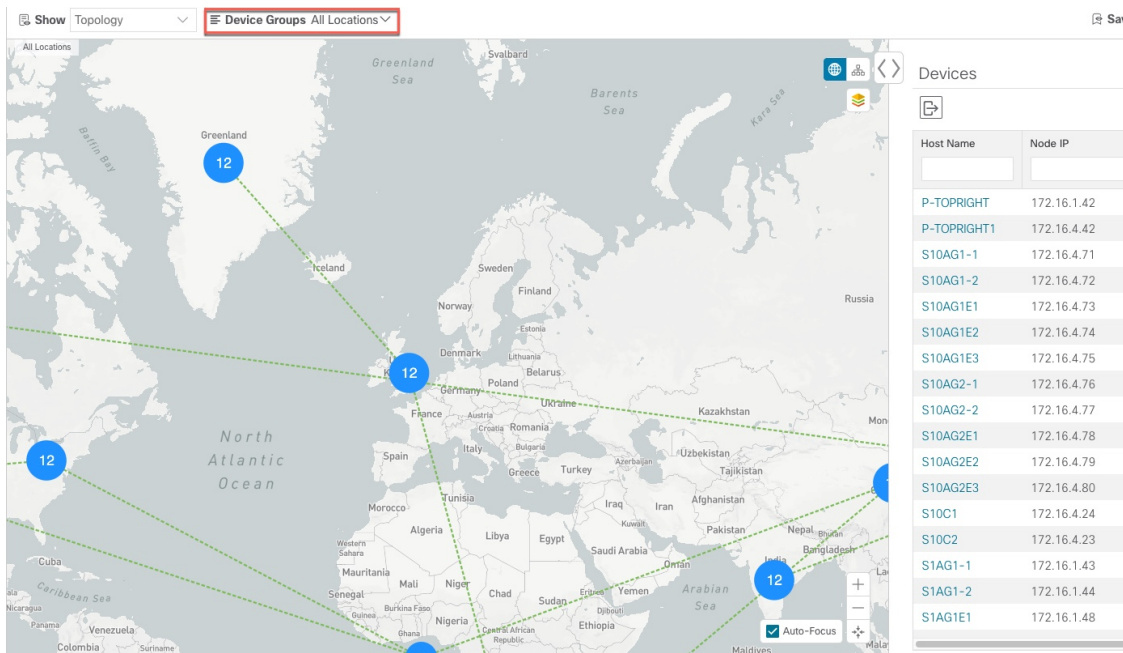
Use Device Groups to Filter Your Topology View

To help you identify, find, and group devices for a variety of purposes, you can create Device Groups. The Device Group window (**Device Management > Groups**) displays all devices and device groups they belong to. By default, all devices initially appear in the **Unassigned Devices** group.

Use Device Groups to Filter Your Topology View

This example walks you through how Device Grouping works in the geographical and logical maps.

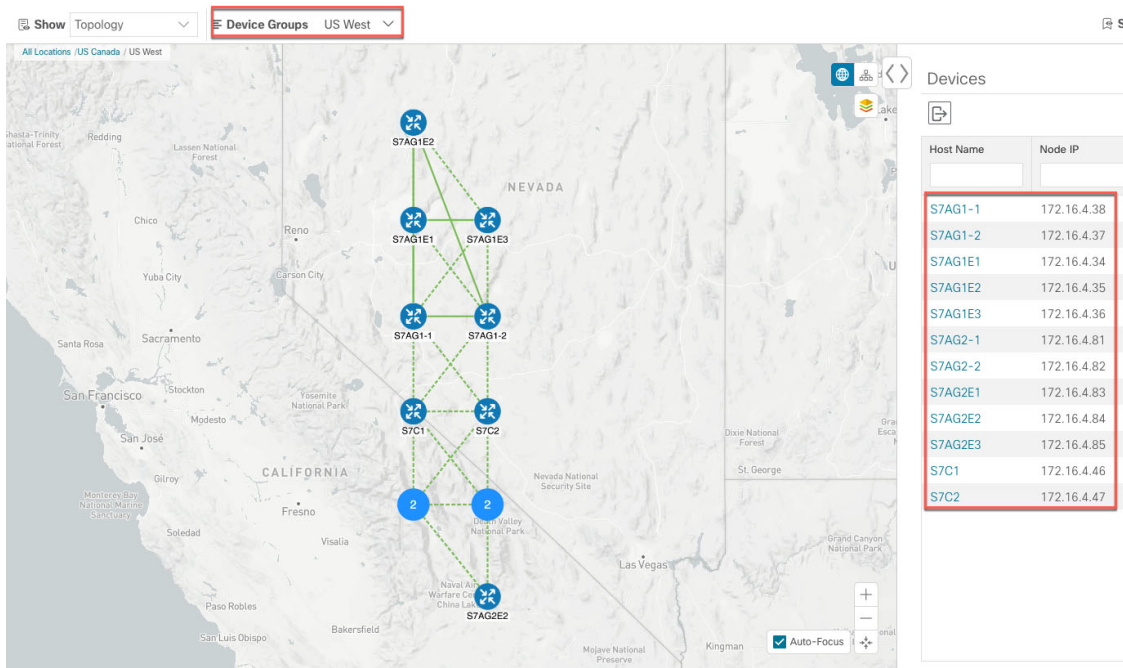
Step 1 From the main menu, choose **Topology**. By default, only devices that have Geo Location set will appear on the geographical map.



Devices


Host Name	Node IP
P-TOPRIGHT	172.16.1.42
P-TOPRIGHT1	172.16.4.42
S10AG1-1	172.16.4.71
S10AG1-2	172.16.4.72
S10AG1E1	172.16.4.73
S10AG1E2	172.16.4.74
S10AG1E3	172.16.4.75
S10AG2-1	172.16.4.76
S10AG2-2	172.16.4.77
S10AG2E1	172.16.4.78
S10AG2E2	172.16.4.79
S10AG2E3	172.16.4.80
S10C1	172.16.4.24
S10C2	172.16.4.23
S1AG1-1	172.16.1.43
S1AG1-2	172.16.1.44
S1AG1E1	172.16.1.48

Step 2 From the **Device Group** drop-down list select a group (US West). Only the devices in that group and related links are displayed on the geographical map. Note that the Devices table has also been filtered to list only those devices in the group.



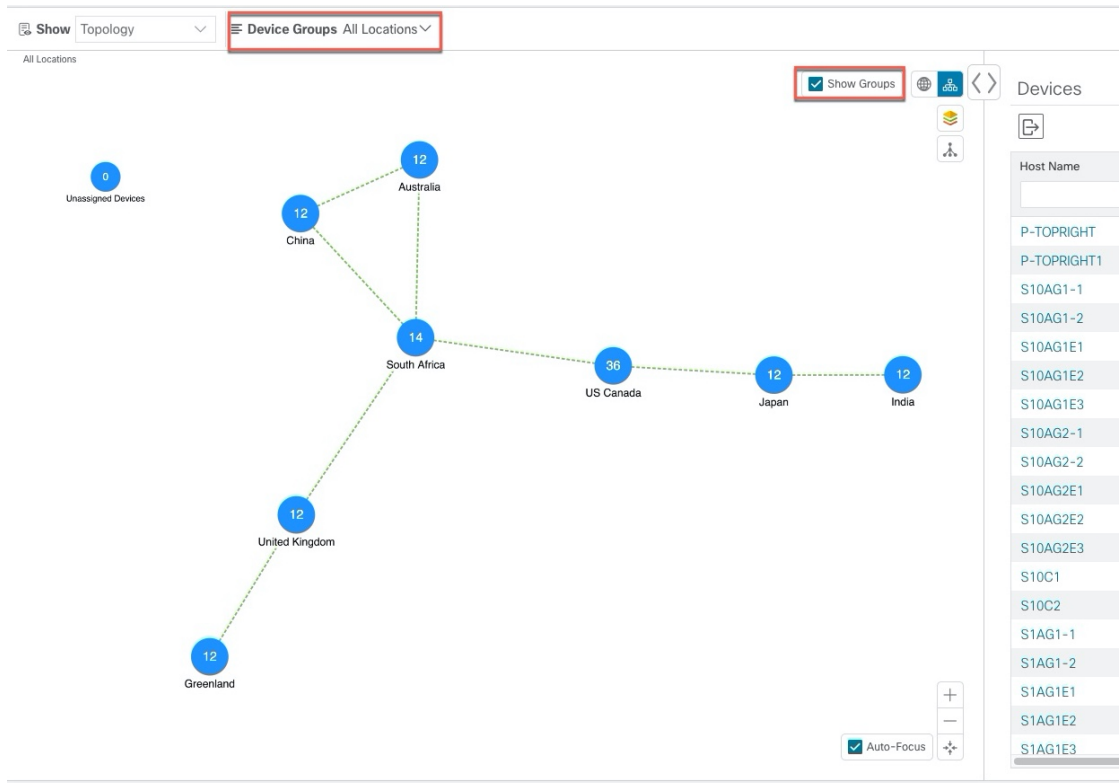
Devices

Host Name	Node IP
S7AG1-1	172.16.4.38
S7AG1-2	172.16.4.37
S7AG1E1	172.16.4.34
S7AG1E2	172.16.4.35
S7AG1E3	172.16.4.36
S7AG2-1	172.16.4.81
S7AG2-2	172.16.4.82
S7AG2E1	172.16.4.83
S7AG2E2	172.16.4.84
S7AG2E3	172.16.4.85
S7C1	172.16.4.46
S7C2	172.16.4.47

Step 3 Click .

Step 4 From the **Device Group** drop-down list, select **All Locations** and check **Show Groups** if it is not already checked. Note that you can see all device groups in this view. Device groups can be seen in this way only within the logical map.

Note If **Show Groups** checkbox is de-selected, all the device groups are expanded, and could lead to a cluttered map.



Step 5 Click the US West group. Again, only devices that belong to this group are shown in the topology map and the Devices table.

The screenshot shows a network topology map with various devices connected. On the right, there is a 'Devices' table listing the following information:

Host Name	Node IP
S7AG1-1	172.16.4.38
S7AG1-2	172.16.4.37
S7AG1E1	172.16.4.34
S7AG1E2	172.16.4.35
S7AG1E3	172.16.4.36
S7AG2-1	172.16.4.81
S7AG2-2	172.16.4.82
S7AG2E1	172.16.4.83
S7AG2E2	172.16.4.84
S7AG2E3	172.16.4.85
S7C1	172.16.4.46
S7C2	172.16.4.47

Step 6 Filter devices in the Device table by entering S7C in the hostname. The Device table displays only devices that match the filtering criteria. However, filtering the Device table does not filter the devices visually on the topology map. The only way to visually filter devices on the geographical or logical maps is to use device groups.

The screenshot shows the same network topology map as above. The 'Devices' table on the right is now filtered to show only two devices:



Host Name	Node IP	Oper...	Reac...	Product Type
S7C1	172.16.4.46	OK	Re...	ciscoCRS16S
S7C2	172.16.4.47	OK	Re...	ciscoCRS16S

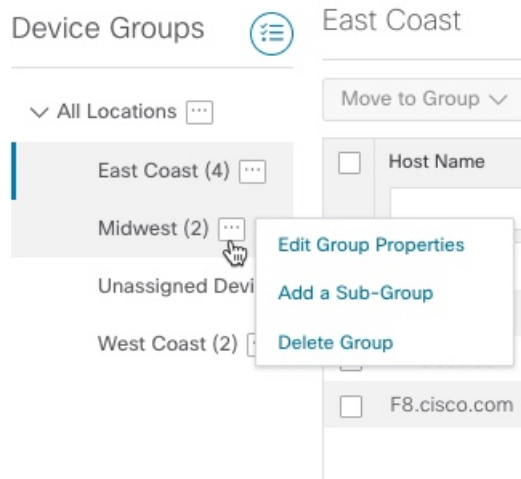
The 'Filters Applied (1)' dropdown is visible above the table, indicating the filter 'S7C' is active.

Create and Modify Device Groups

Device groups and assignment of devices to the groups can be done either manually (as described in this section) or automatically (as described in the next section).

Step 1 From the main menu choose **Device Management > Groups**.

- Step 2** To add a new sub-group, click  next to **All Locations**. A new sub-group gets added under **All Locations**.
- Step 3** To edit, delete, or add a sub-group under an existing group, from the Device Groups tree, click  next to a group.



- Step 4** Choose to add, delete, or edit (rename or move) a group. If you delete a group, all devices that belong to that group are moved to the Unassigned Devices group. Also, deleting a group deletes all the sub-groups under it.
- Note** Devices can belong to only one device group.
- Step 5** Click **Save**.

Enable Dynamic Device Grouping


You can create a rule to dynamically create device groups and automatically add unassigned devices to these groups using a Regular Expression (regex) on the device hostname. Any newly added or discovered devices that match the rule will be placed in the appropriate group.



Note Dynamic rules do not apply to devices that already belong to groups. You must move them to Unassigned Devices if you want them to be considered by the rule.

Before you begin

While you can follow examples given in the Dynamic Groups dialog, it is helpful to be familiar with Regular Expressions.

- Step 1** From the main menu choose **Device Management > Groups**.
- Step 2** Click  to open the **Manage Dynamic Grouping Rule** window.
- Step 3** Click **Show more details and examples** to help you fill out the required Host Name and Group Name fields.


- Step 4** If there are any existing devices in the Unassigned Devices group, click **Test Rule** to view a sampling of what type of group names will be created.
- Step 5** Check the **Enable Rule** checkbox. After the rule is enabled, the system checks for unassigned devices every minute and will assign them to the appropriate group based on the rule.
- Step 6** Click **Save**.
- Step 7** Groups that are created this way initially appear under Unassigned Groups (created when a rule is enabled for the first time). Move newly created groups to the desired group hierarchy.
- Step 8** To move newly created Unassigned groups to the correct group, do the following:
- Select ... next to All Locations and click **Add a Sub-Group**.
 - Enter the New Group details and click **Save**.
 - Select ... next to the unassigned created dynamic group and select **Edit Group Properties**.
 - Click **Change Parent Group** and select the appropriate group.

Customize Map Display Settings

You can configure visual settings on the topology map based on your needs and preferences. You can do the following:

- [Customize the Display of Links and Devices, on page 22](#)
- [Set Display Behavior of Device Groups for TE Tunnels , on page 22](#)

Customize the Display of Links and Devices

To set device and link map display preferences, choose **Topology** and click  on the topology map.

- Click **Links** to show aggregated links and how links should be colored so that you can easily see their state and utilization status. By default, aggregated links will be differentiated from single links on the map and links will be colored based on link utilization thresholds. Administrators can change the utilization thresholds and their corresponding colors.
- Click **Devices** to show the device state and how the devices should be labeled. By default, the device state is shown on the map and the host name is used to label devices.

Set Display Behavior of Device Groups for TE Tunnels

You can configure what is shown on the topology map when a device group is selected and a device in the selected TE tunnel does not belong in the group. To set the behavior, choose **Admin > Settings > User Settings** and select one of the behavior options.

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

Customize the Display of Traffic Engineering

To set Traffic Engineering display preferences, choose **Traffic Engineering** > **Traffic Engineering** and click  on the topology map

- Click **Links** to show aggregated links and how links should be colored so that you can easily see their state and utilization status. By default, aggregated links will be differentiated from single links on the map and links will be colored based on link utilization thresholds. Administrators can change the utilization thresholds and their corresponding colors.



Note Dual stack links (although aggregate) are shown as one single line.


- Click **Devices** to show the device state and how the devices should be labeled. By default, the device state is shown on the map and the host name is used to label devices.
- Click **Metrics** to show IGP, TE, and delay (latency) metrics when viewing IGP paths. By default, these metrics are not enabled.



Note Metrics cannot be shown when the IGP path goes over an aggregate link. If you try to view an IPv6 network that has both IPv4 and IPv6 links you need to check the **Show Participating Only** checkbox to see IPv6 metrics.

- Click **Flex Algo** to show the Flex Algorithm paths. For more information see [Visualize Flexible Algorithms](#), on page 47.

Configure Timeout Settings

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



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

Save Topology Views for Easy Access

When you rearrange the devices and links on a map, your changes are not normally saved. To easily access a useful map layout, you can save it as a named custom view and quickly retrieve it, without having to rearrange the map each time. This is especially useful when managing large networks with many devices.

When you save a custom view, the following settings will be saved:

- Whether it is a geographical or logical map.
- Device positions in the logical map layout.
- Device and link display settings
- Any filters used in the Device and Traffic Engineering tables



Note All custom views can be seen by all users. However, only users with the admin role or users that created the custom view can modify the view.

Step 1 Customize the current map view until it contains only the information you want and until the layout meets your needs.

Step 2 When you have the view the way you want it, click **Save View**.

The screenshot shows the Cisco Crosswork Optimization Engine interface. On the left, a geographical map of the United States displays a network topology with nodes labeled xrv9k-5, xrv9k-3, xrv9k-7, xrv9k-6, xrv9k-4, and srpce1. On the right, the 'Traffic Engineering' panel is visible, showing a table of SR Policies. The 'Save View' button in the top right corner is highlighted with a red box.

SR-MPLS	SRv6	RSVP-TE
15 PCE Init	15 PCC Init	0 Admin Down
		26 Oper Up
		4 Oper Down

SR POLICY					
Hea...	End...	C...	Ad...	Op...	Actions
<input type="checkbox"/>					
<input type="checkbox"/>	xrv9k-5	xrv9k-7	123...	↑	↑
<input type="checkbox"/>	xrv9k-5	xrv9k-7	222	↑	↑
<input type="checkbox"/>	xrv9k-5	xrv9k-7	333	↑	↑
<input type="checkbox"/>	xrv9k-6	xrv9k-7	607...	↑	↑
<input type="checkbox"/>	xrv9k-5	xrv9k-7	6521	↑	↑

Step 3 Enter a unique name for the new custom view and click **Save**. You can later modify the view (click **Select a saved view**) and choose to edit the topology, rename, or delete the view.




CHAPTER 3

Visualize SR-MPLS and SRv6 Policies

Crosswork Optimization Engine allows you to visualize SR-MPLS and SRv6 policies in your network. The SR-PCE discovers policies and displays them in the Traffic Engineering topology map.

SRv6 Notes and Limitations

- SRv6 visualization with IS-IS IGP is only supported with SR-PCE running Cisco IOS XR 7.3.2.
- Traffic collection on SRv6 policies is not currently supported.
- OSPFv3 IGP (PCE-initiated) SRv6 policies are not supported.
- When viewing metrics on an IPv6 network that has both IPv4 and IPv6 links, you need to check the **Show Participating Only** checkbox (**Traffic Engineering** > **Traffic Engineering** >  > **Metrics**).
- IPv4 and IPv6 topologies must be congruent. Different link metrics for IPv4 and IPv6 are not supported.
- SRv6 is not supported on Bandwidth Optimization, Bandwidth on Demand, or Local Congestion Mitigation feature packs.
- Visualization of PCC-initiated dynamic path SRv6 policies. PCE-initiated and explicit path visualization of SRv6 is not supported.

This section contains the following topics:

- [View SR-MPLS and SRv6 Policies on the Topology Map, on page 25](#)
- [View SR-MPLS and SRv6 Policy Details, on page 27](#)
- [View Traffic Engineering Device Details, on page 29](#)
- [Visualize SR-MPLS or SRv6 Policies Example, on page 30](#)
- [Find Multiple Candidate Paths \(MCPs\), on page 37](#)
- [Visualize Underlying Paths Associated with a Defined Binding-Segment ID \(B-SID\) Label, on page 41](#)
- [Visualizing Native SR Paths, on page 43](#)

View SR-MPLS and SRv6 Policies on the Topology Map

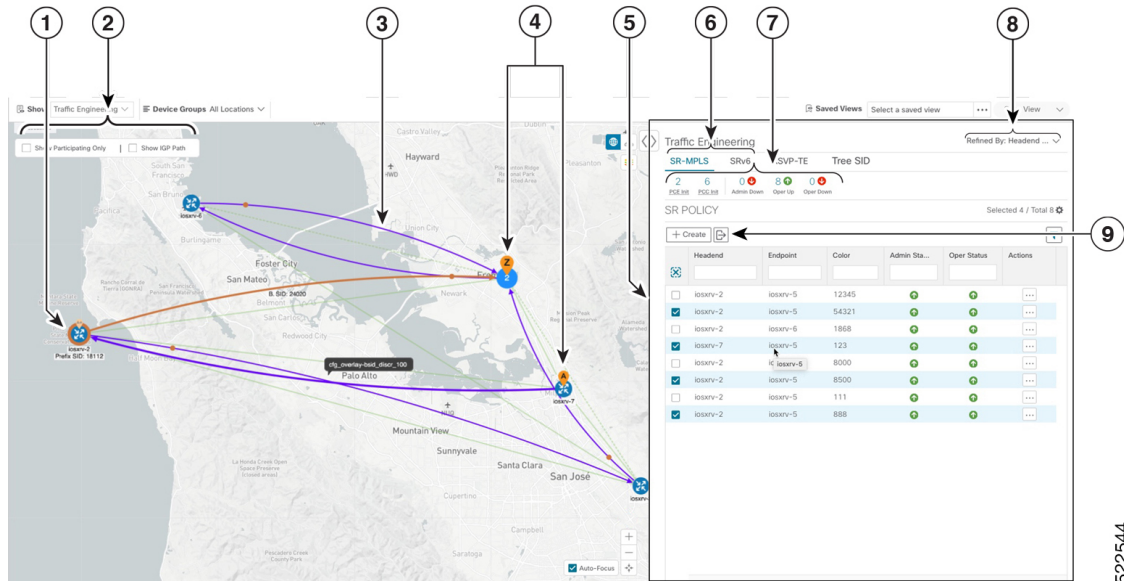
Crosswork Optimization Engine visualization provides the most value by giving you the ability to easily view and manage SR-MPLS and SRv6 policies. By visually examining your network, the complexity of provisioning and managing these SR-TE policies is significantly reduced.

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





Note Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using Crosswork Optimization Engine within the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering** and select either the **SR-MPLS** or **SRv6** tabs.

Figure 6: Traffic Engineering UI : SR-MPLS and SRv6 Policies



522544

Callout No.	Description
1	A device with an orange () outline indicates there is a node SID associated with that device or a device in the cluster.
2	Click the appropriate check box to enable the following options: <ul style="list-style-type: none"> • Show IGP Path—Displays the IGP path for the selected SR-TE policy. • Show Participating Only—Displays only links that belong to selected SR-TE policy. All other links and devices disappear.
3	When SR-TE policies are selected in the SR-MPLS or SRv6 tables, they show as purple directional lines on the map indicating source and destination. An adjacency segment ID (SID) is shown as an orange circle on a link along the path ().
4	SR-MPLS and SRv6 Policy Origin and Destination: If both A and Z are displayed in a device cluster, at least one node in the cluster is a source and another is a destination. The A+ denotes that there is more than one SR-TE policy that originates from a node. The Z+ denotes that the node is a destination for more than one SR policy.

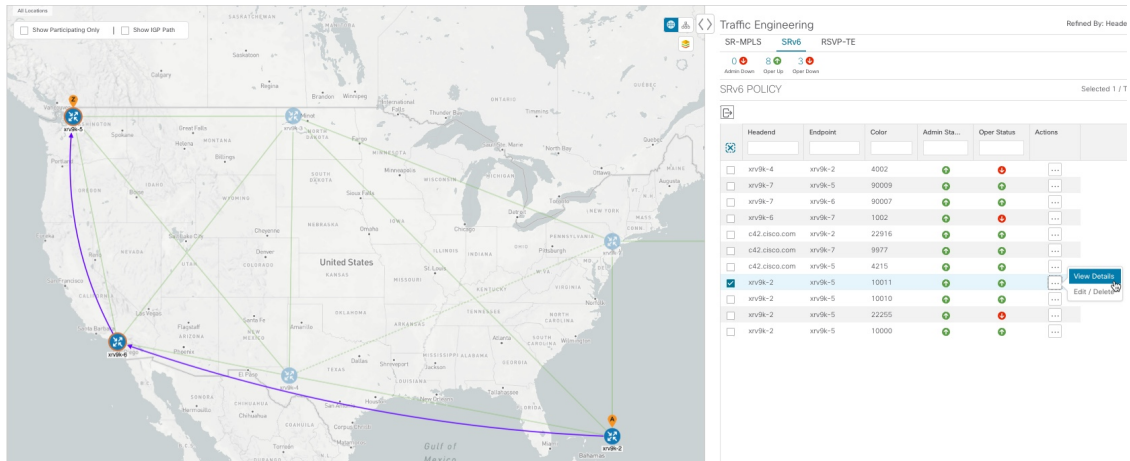
Callout No.	Description
5	<p>The content of this window depends on what has been selected or filtered. In this example, the SR-MPLS tab is selected and the SR Policy table is displayed. Depending on what is selected on the topology map, or whether you are in the process of viewing and managing SR-TE policies, you can do the following:</p> <ul style="list-style-type: none"> • Visualize SR-MPLS or SRv6 Policies Example, on page 30 • Provision SR-MPLS Policies, on page 59 • View Device and Link Details, on page 12
6	Click on either the SR-MPLS or SRv6 tabs to view the respective list of SR-TE policies.
7	The Mini Dashboard provides a summary of the operational SR-MPLS or SRv6 policy status. If filters are applied, the Mini Dashboard is updated to reflect what is displayed in the SR Policy and SRv6 Policy tables. In addition to the policy status, the SR-MPLS Mini Dashboard table displays the number of PCC and PCE initiated tunnels that are <i>currently</i> listed in the SR Policy table.
8	<p>This option allows you to choose how the group filter (when in use) should be applied on the table data. For example, if Headend only was selected, then it would only display policies where the headend device of the policy is in the selected group. This filter allows you to see specific configurations and is useful when you have a large network.</p> <p>Filter options:</p> <ul style="list-style-type: none"> • Headend or Endpoint—Show policies with either the headend or endpoint device in the selected group. • Headend and Endpoint—Show policies if both the headend and endpoint are in the group. • Headend only—Show policies if the headend device of the policy is in the selected group. • Endpoint only—Show policies if endpoint device of the policy is in the selected group.
9	Exports <i>all</i> data into a CSV file. You cannot export selected or filtered data.

View SR-MPLS and SRv6 Policy Details

View SR-MPLS or SRv6 policy details such as disjoint groups, metric type, candidate path, segment hop information, and so on.

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

View SR-MPLS and SRv6 Policy Details



Traffic Engineering

SR-MPLS SRv6 RSP-TE

Admin Down Open Up Open Down

SRv6 POLICY Selected: 1 / 7

Headend	Endpoint	Color	Admin Sta...	Oper Status	Actions
<input type="checkbox"/> sr9k-4	sr9k-2	4002	●	●	...
<input type="checkbox"/> sr9k-7	sr9k-5	90009	●	●	...
<input type="checkbox"/> sr9k-7	sr9k-6	90007	●	●	...
<input type="checkbox"/> sr9k-6	sr9k-7	1002	●	●	...
<input type="checkbox"/> c42.cisco.com	sr9k-2	22916	●	●	...
<input type="checkbox"/> c42.cisco.com	sr9k-7	9977	●	●	...
<input type="checkbox"/> c42.cisco.com	sr9k-5	4215	●	●	...
<input checked="" type="checkbox"/> sr9k-2	sr9k-5	10011	●	●	View Details Edit / Delete
<input type="checkbox"/> sr9k-2	sr9k-5	10010	●	●	...
<input type="checkbox"/> sr9k-2	sr9k-5	22255	●	●	...
<input type="checkbox"/> sr9k-2	sr9k-5	10000	●	●	...

Step 2 View SR-MPLS or SRv6 policy details.

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

SRv6 Policy Details ×

Headend A xrv9k-2 (TE RID: 192.168.0.2) PCC IP: 192.168.0.2
Source IP: 2001:192:168::2

Endpoint Z xrv9k-5 (TE RID: 192.168.0.5)
Dest IP: 2001:192:168::5

Color 10011

▼ **Summary**

- Admin State** ↑ Up
- Oper State** ↑ Up
- Binding SID** fccc:cc11:22:e01d::/64, Behavior - uB6 (Insert.Red)
- Segment Type** -
- Policy Type** Unknown
- Profile ID** -
- Utilization** 0 Mbps
- Delay** 124 ⓘ
- BWOD Policy Bandwidth** 0 Mbps
- Accumulated Metric** 124
- Delegated PCE** 2001:420:28f:2011:250:56ff:fe85:a025
- Non-delegated PCEs** -
- PCE Computed Time** 27-Oct-2021 12:33:03 PM PDT
- Last Update** 27-Oct-2021 12:39:55 PM PDT

Last Updated ×

27-Oct-2021 06:42:22 PM PDT

▼ **Candidate Path** Expand All

Path Name		Preference	Path Type
▼ cfg_srv6_test_disjoint2_discr_100		100	Unknown

Seg...	Seg...	SID	Behavior	Algo	Address	Node	Interface
0	uN	fccc:cc11:6...	uN (PSP/U...	0	2001:192:...	xrv9k...	
1	uN	fccc:cc11:5...	uN (PSP/U...	0	2001:192:...	xrv9k...	

Path Name cfg_srv6_test_disjoint2_discr_100

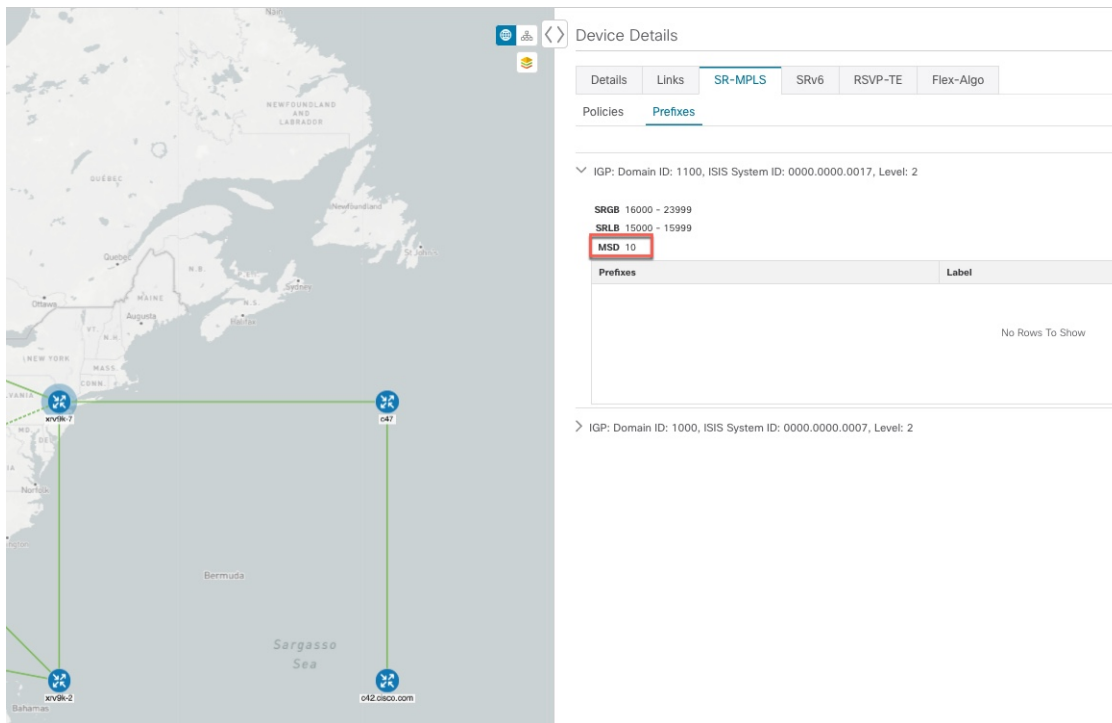
Metric Type TE

Disjoint Group ID: 18115
Association Source: 0.0.0.0
Type: Node-disjoint

View Traffic Engineering Device Details

To view Traffic Engineering Device details (SR-MPLS, SRv6, RSVP-TE, and Flexible Algorithm information), do the following:

- Step 1** From the main menu choose **Traffic Engineering > Traffic Engineering**.
- Step 2** From the Traffic Engineering map, click on a device.
- Step 3** From the **Device Details** page, click on the traffic engineering tab you are interested in. The tab displays associated data for that device. The following example shows SR-MPLS Prefix information which includes the MSD value for the device.



The screenshot displays a network topology map of North America with four nodes: xv9k-7 (New York), o47 (Boston), xv9k-2 (Bahamas), and o42.cisco.com (Miami). A 'Device Details' panel is open for the 'o47' node, showing the 'SR-MPLS' tab. The configuration includes IGP Domain ID: 1100, ISIS System ID: 0000.0000.0017, Level: 2. Policy ranges are listed as SRGB 16000 - 23999, SRLB 15000 - 15999, and MSD 10. A table for 'Prefixes' is shown with the text 'No Rows To Show'.

Visualize SR-MPLS or SRv6 Policies Example

This example walks you through several SR-TE (SR-MPLS and SRv6) policy visualization features that are available from the topology map. The topology map displays SR-TE policies that are provisioned using the UI along with policies that are discovered from the network by SR-PCE. Then you can drill down to details and visualization of participating SR-TE policies.

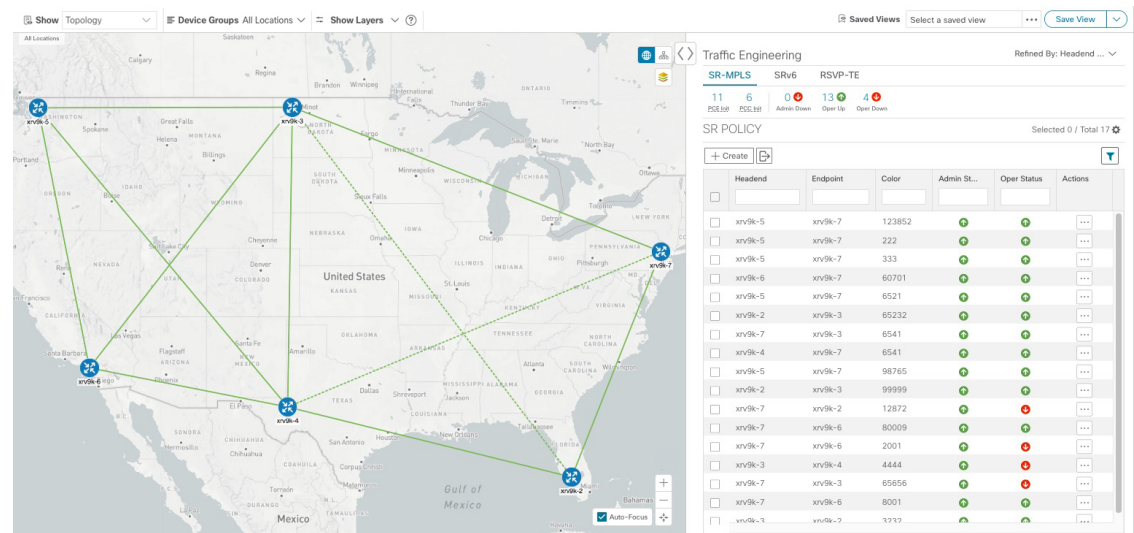
In this example, we assume that devices and SR-MPLS policies have been added and device groups have been created.



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

Click images to zoom in for a closer look.

Figure 7: Topology Map Example

**Step 1**

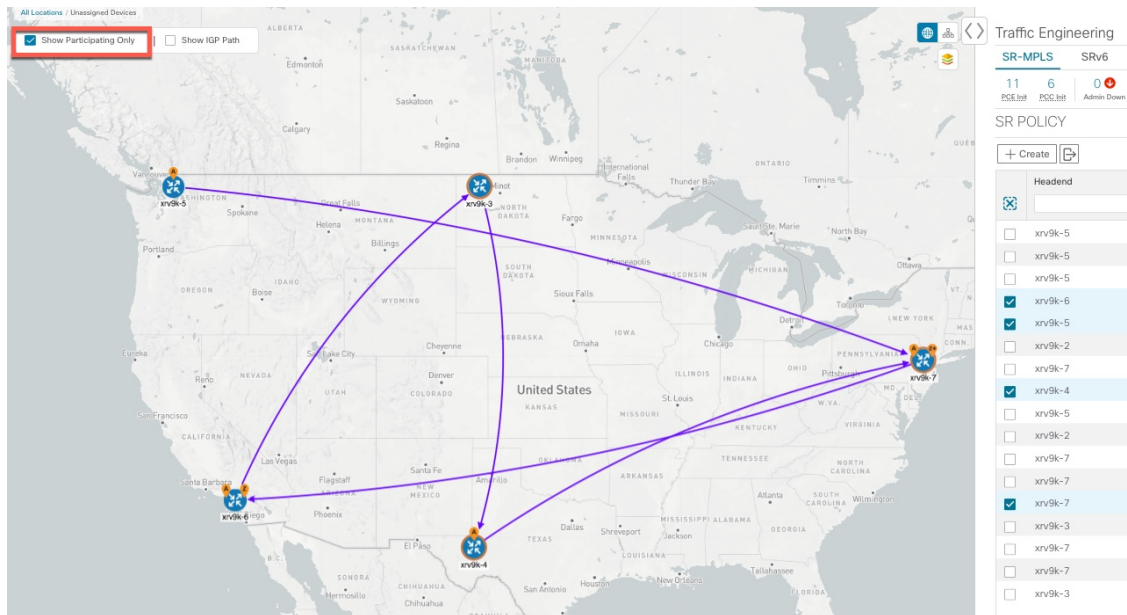
Select SR-MPLS policies for visualization and isolate them on the map.

- From the main menu, choose **Traffic Engineering > Traffic Engineering**.
- From the **SR Policy** table, check the check box next to the SR-MPLS policies you are interested in.
- Check the check box next to **Show Participating Only** so that other links and devices that are not part of the selected SR-TE policies are hidden.

In the following example, the topology map displays the following:

- Four SR-MPLS policies are selected.
- SR-MPLS policies appear as purple links with arrows that indicate the path direction.
- The **xrv9k-7** node is the destination for two of the selected policies. Both **xrv9k-3** and **xrv9k-2** are destinations for the selected policies. SR-MPLS policy origin and destination are marked with **A** and **Z**, respectively. The **A+** denotes that there is more than one policy that originates from a device. A **Z+** denotes that the device is a destination for more than one policy.
- The orange outline (🔴) indicates that **xrv9k-3**, **xrv9k-7**, and **xrv9k-4** have node SIDs.

Visualize SR-MPLS or SRv6 Policies Example

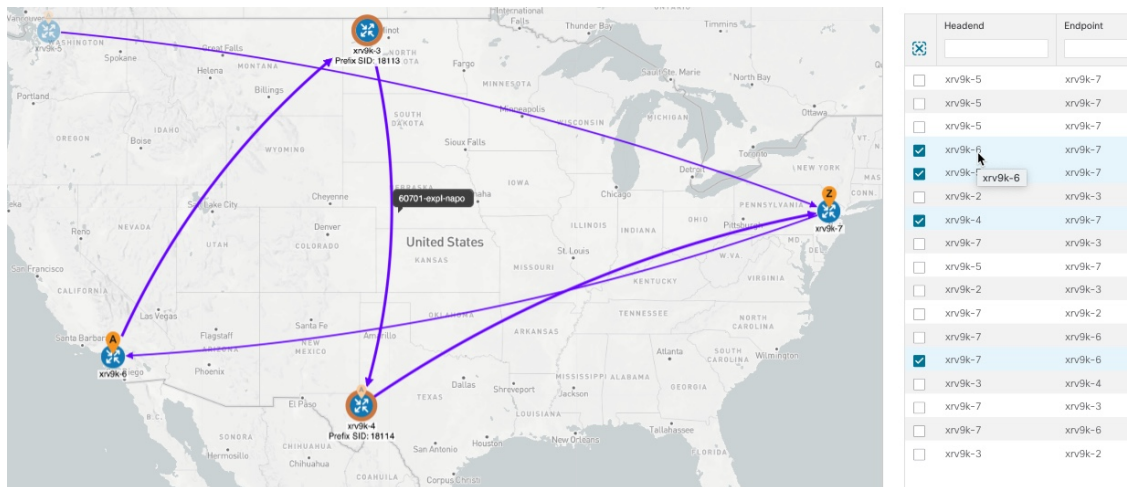


Step 2 Highlight and view more details for a particular SR-MPLS policy.

a) From the **SR Policy** table, *hover* over a selected policy.

The topology map displays the following details:

- The path is emphasized on the map. The path goes through **xrv9k-6 > xrv9k-3 > xrv9k-4 > xrv9k-7**.
- The prefix SID for xrv9k-3 and xrv9k-4 are displayed.
- The path name is displayed: **60701-expl-napo**



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

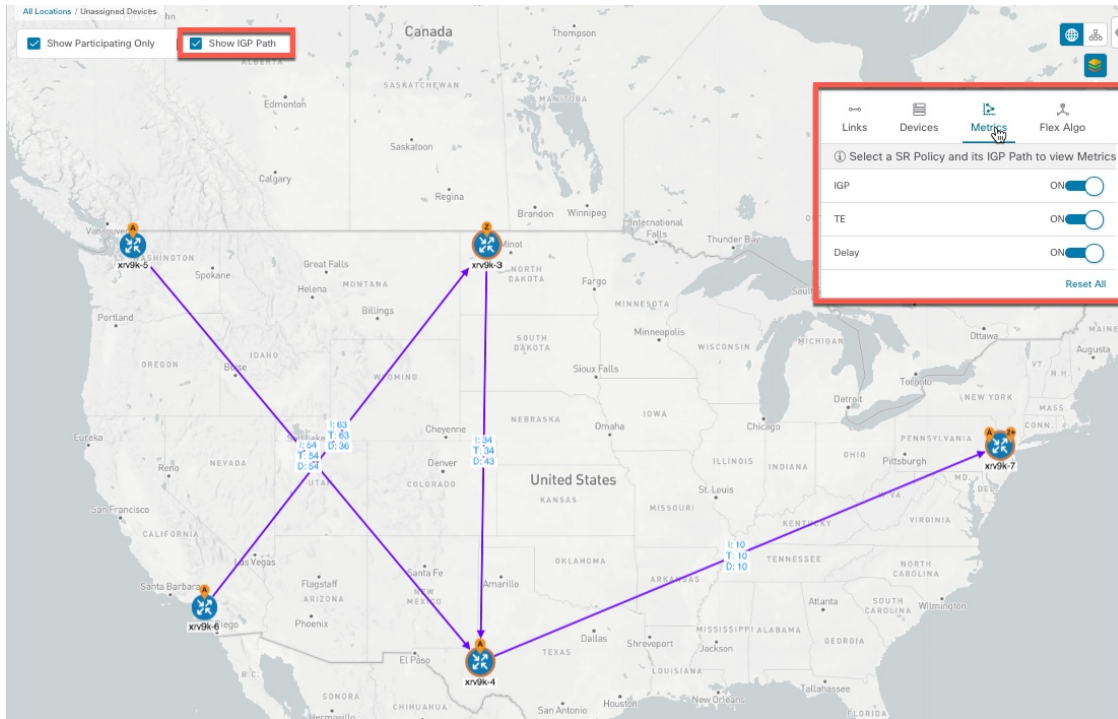
a) Check the **Show IGP Path** check box. The IGP paths for the selected SR-MPLS policies are displayed, with straight lines, instead of the segment hops.

b) Click .

c) Click the **Metrics** tab.

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

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

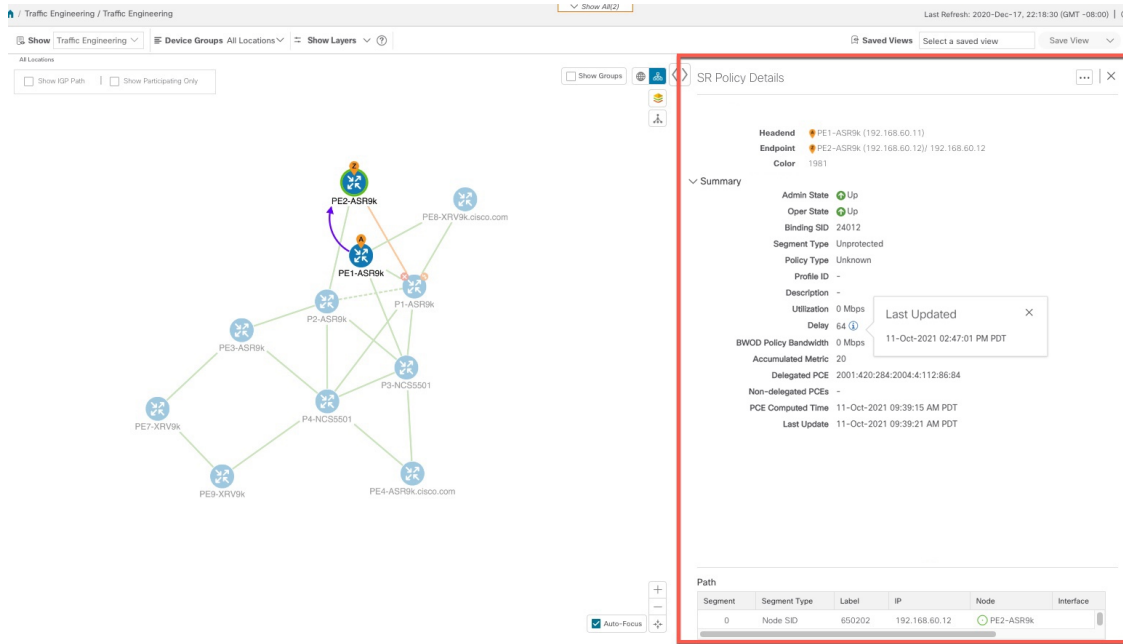


Step 4

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

a) From the **Actions** column, click  > **View Details** for one of the SR-MPLS policies.

The **SR Policy Details** window is displayed in the side panel. Note that only the selected policy is displayed on the topology map.



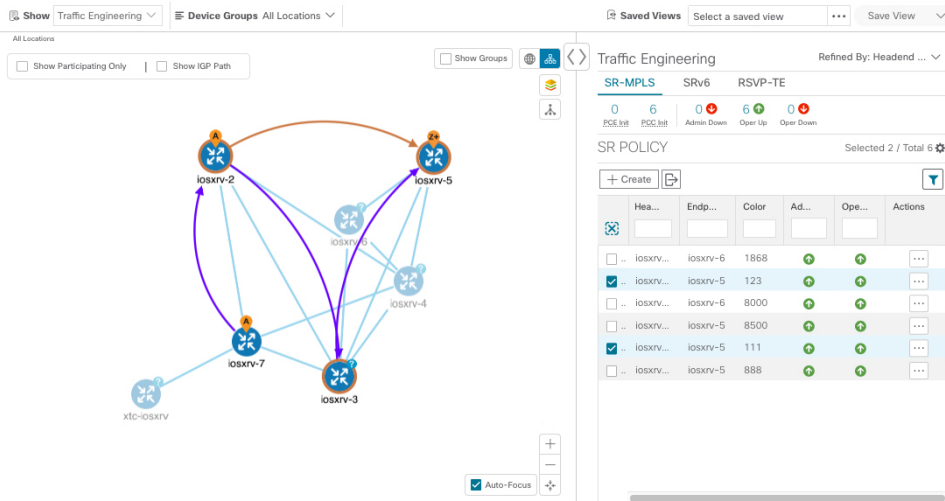
Step 5

Customize and save a logical view of the topology.

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

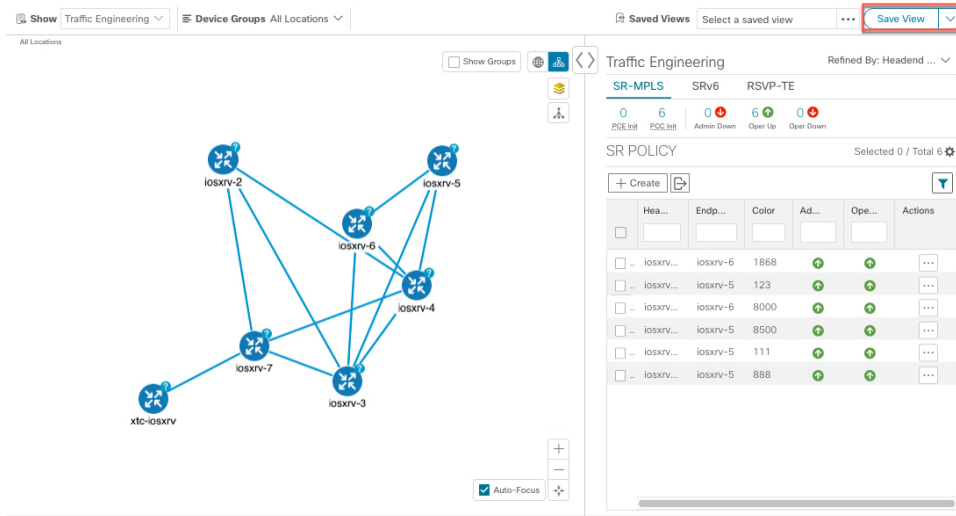
Example:

Figure 8: Logical Map (SR-MPLS Policies Selected)



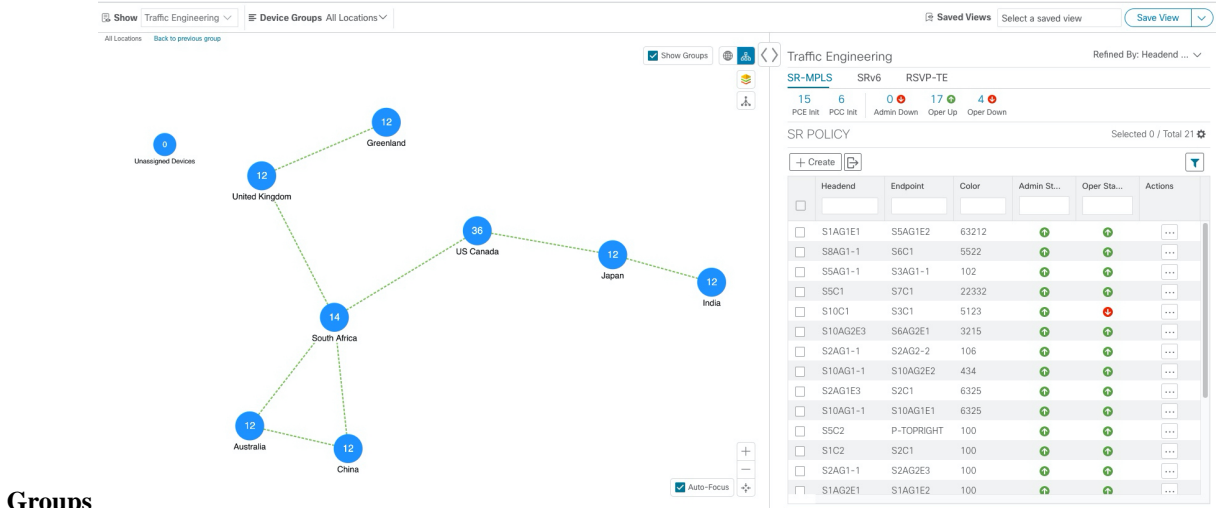
Example:

Figure 9: Logical Map (Save Without SR-MPLS Policies Selected)



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

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



Groups.

Step 8

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

Headend	Endpoint	Color	Admin St...	Oper Stat...	Actions
<input type="checkbox"/>	S1AG1E1	SSAG1E2	63212	●	●
<input type="checkbox"/>	S1C2	S2C1	100	●	●
<input checked="" type="checkbox"/>	S1AG2E1	S1AG1E2	100	●	●
<input type="checkbox"/>	SSC1	S1C2	111	●	●
<input type="checkbox"/>	S7C1	S1C2	202	●	●
<input checked="" type="checkbox"/>	S1AG1-2	S1C2	4521	●	●
<input type="checkbox"/>	S10AG1-1	S1AG1-1	3256	●	●

Step 9

If you select a policy where participating devices are not part of the selected group, then a dialog appears giving you an option to switch the group view. This is the default behavior. If this window does not appear, then the administrator has configured the display to automatically switch view or stay in the current view. For more information, see [Set Display Behavior of Device Groups for TE Tunnels](#), on page

Some of the participating devices are not in the current device group.
Click "Switch Device Group" to automatically switch to the device group that will show all participating devices.

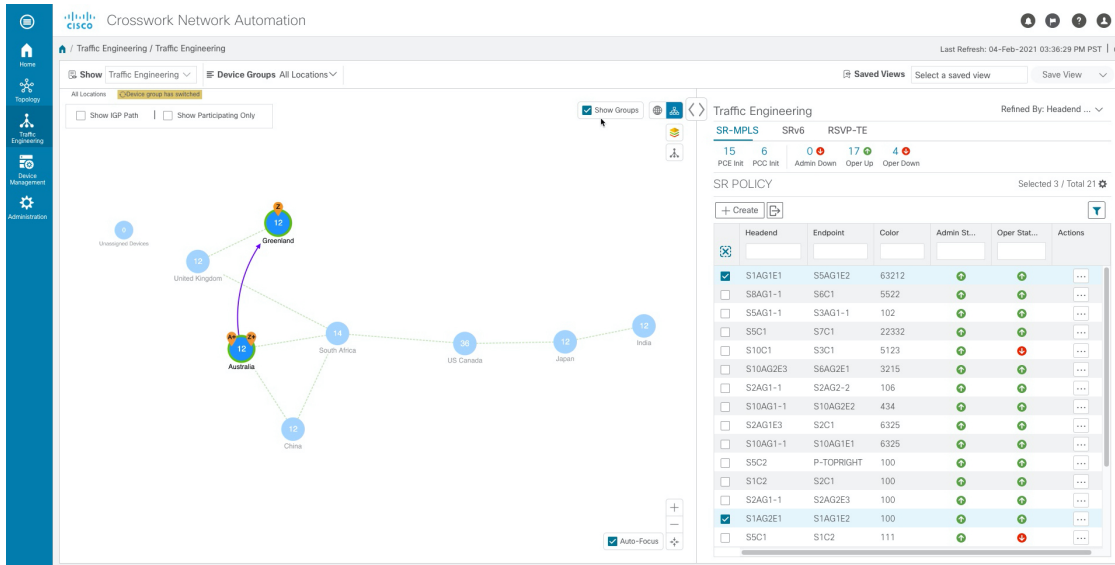
Don't show this message again

Headend	Endpoint	Color	Admin St...	Oper Stat...	Actions
<input checked="" type="checkbox"/>	S1AG1E1	SSAG1E2	63212	●	●
<input type="checkbox"/>	S1C2	S2C1	100	●	●
<input checked="" type="checkbox"/>	S1AG2E1	S1AG1E2	100	●	●
<input type="checkbox"/>	SSC1	S1C2	111	●	●
<input type="checkbox"/>	S7C1	S1C2	202	●	●
<input checked="" type="checkbox"/>	S1AG1-2	S1C2	4521	●	●
<input type="checkbox"/>	S10AG1-1	S1AG1-1	3256	●	●

Step 10

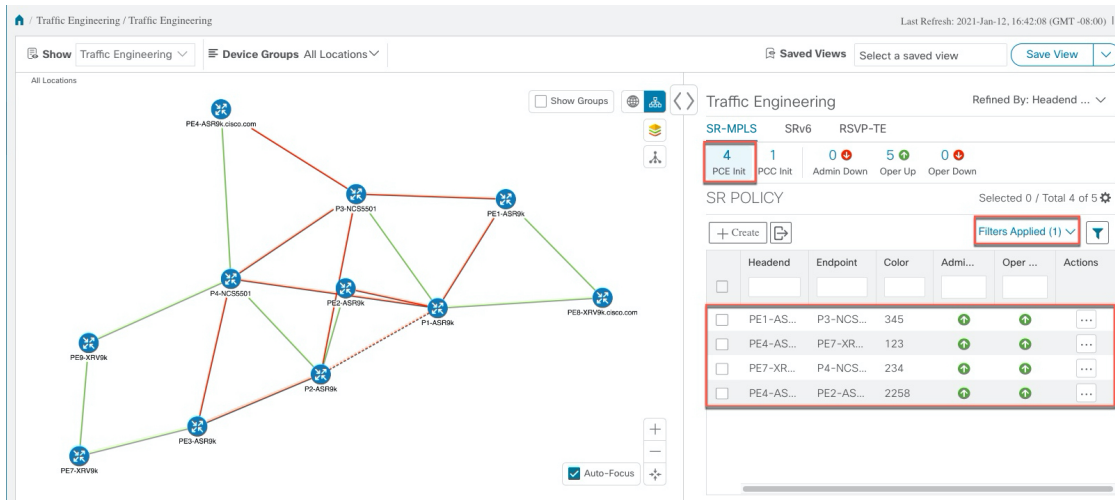
If you select **Switch Device Group**, then the group will change and you will see all participating devices for the SR-MPLS policies you have selected.

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



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

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



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

Find Multiple Candidate Paths (MCPs)

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

Important Notes

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

Before you begin

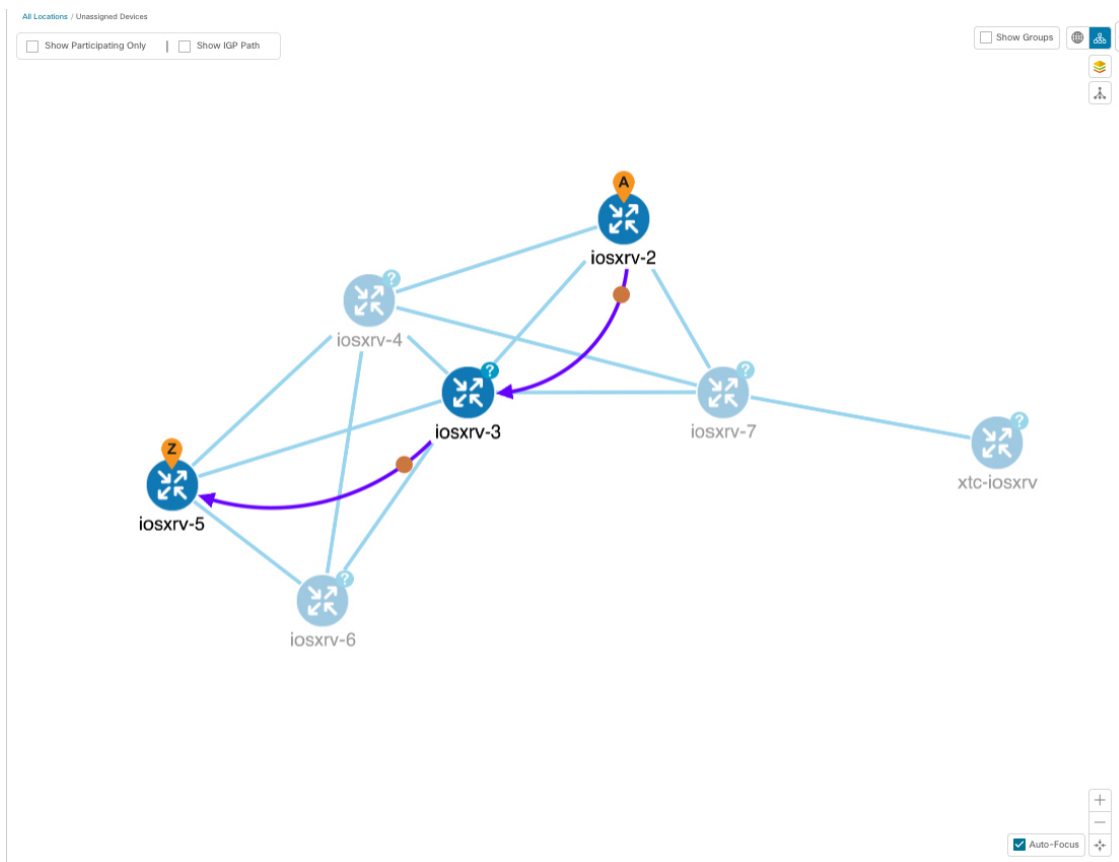
A policy must be configured with MCPs on devices before visualizing them on the Traffic Engineering topology map. This configuration can be done manually or within Crosswork Network Controller.

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


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

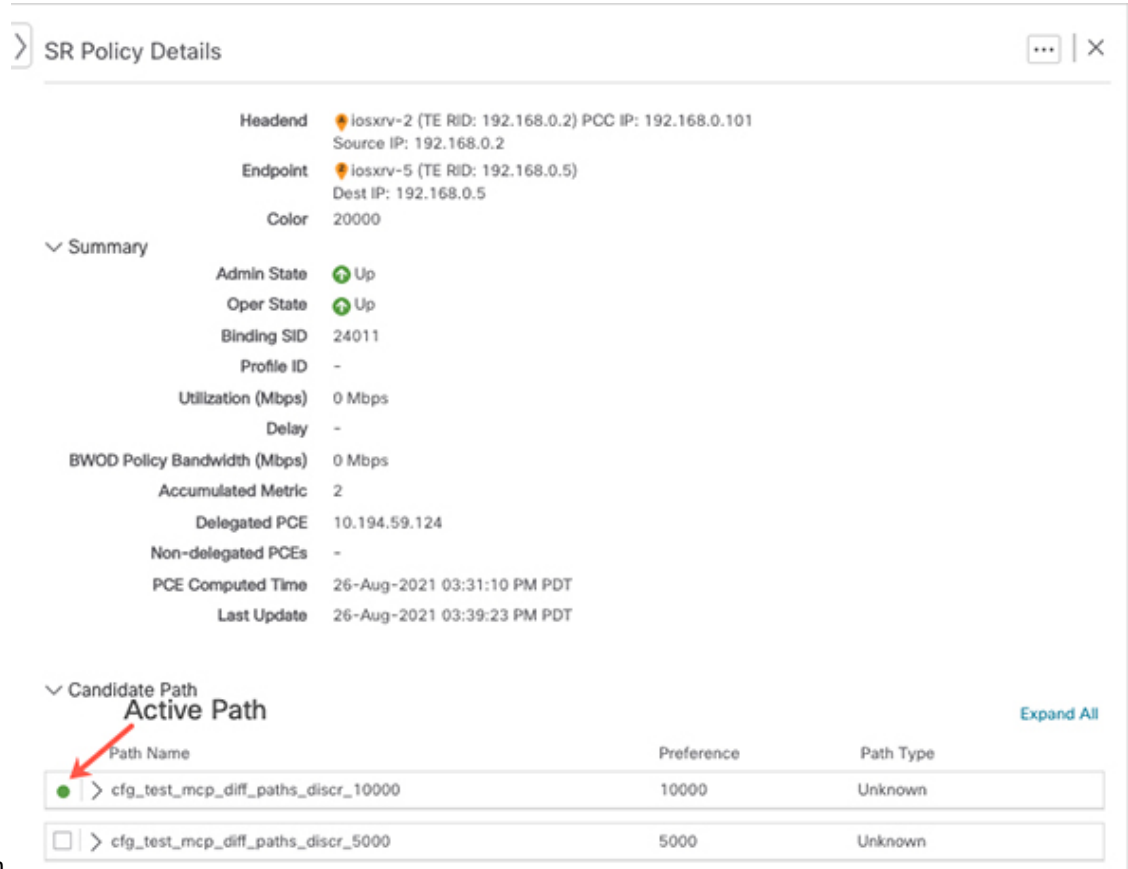
- Check the check box next to the SR-TE policy that has MCPs configured.
- View the SR-TE policy that is highlighted on the topology map.

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



Step 3 View the list of candidate paths.

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



The screenshot shows the 'SR Policy Details' window. It includes a 'Summary' section with the following information:

- Headend:** iosxrv-2 (TE RID: 192.168.0.2) PCC IP: 192.168.0.101, Source IP: 192.168.0.2
- Endpoint:** iosxrv-5 (TE RID: 192.168.0.5), Dest IP: 192.168.0.5
- Color:** 20000
- Admin State:** Up
- Oper State:** Up
- Binding SID:** 24011
- Profile ID:** -
- Utilization (Mbps):** 0 Mbps
- Delay:** -
- BWOD Policy Bandwidth (Mbps):** 0 Mbps
- Accumulated Metric:** 2
- Delegated PCE:** 10.194.59.124
- Non-delegated PCEs:** -
- PCE Computed Time:** 26-Aug-2021 03:31:10 PM PDT
- Last Update:** 26-Aug-2021 03:39:23 PM PDT

The 'Candidate Path' section is expanded to show an 'Active Path' table:

Path Name	Preference	Path Type
<input checked="" type="checkbox"/> > cfg_test_mcp_diff_paths_discr_10000	10000	Unknown
<input type="checkbox"/> > cfg_test_mcp_diff_paths_discr_5000	5000	Unknown

path.

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

Step 5 Visualize the candidate path on the topology map.

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

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

SR Policy Details ... ×

PCE Computed Time 26-Aug-2021 03:31:10 PM PDT
Last Update 26-Aug-2021 03:39:23 PM PDT

Candidate Path Collapse All

Path Name	Preference	Path Type																								
<input type="checkbox"/> ▼ cfg_test_mcp_diff_paths_discr_10000	10000	Unknown																								
<input type="checkbox"/> ▼ <table border="1"> <thead> <tr> <th>Segm...</th> <th>Segment Type</th> <th>Label</th> <th>Algo</th> <th>IP</th> <th>Node</th> <th>Interface</th> <th>Sid T...</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>IGP Adj SID</td> <td>24002</td> <td>0</td> <td>10.0.0.9</td> <td>iosxrv-2</td> <td></td> <td>P</td> </tr> <tr> <td>1</td> <td>IGP Adj SID</td> <td>24012</td> <td>0</td> <td>10.0.0.25</td> <td>iosxrv-3</td> <td></td> <td>P</td> </tr> </tbody> </table>	Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...	0	IGP Adj SID	24002	0	10.0.0.9	iosxrv-2		P	1	IGP Adj SID	24012	0	10.0.0.25	iosxrv-3		P		
Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...																			
0	IGP Adj SID	24002	0	10.0.0.9	iosxrv-2		P																			
1	IGP Adj SID	24012	0	10.0.0.25	iosxrv-3		P																			
<input checked="" type="checkbox"/> ▼ cfg_test_mcp_diff_paths_discr_5000	5000	Unknown																								
<input checked="" type="checkbox"/> ▼ <table border="1"> <thead> <tr> <th>Segm...</th> <th>Segment Type</th> <th>Label</th> <th>Algo</th> <th>IP</th> <th>Node</th> <th>Interface</th> <th>Sid T...</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Node SID</td> <td>18115</td> <td>0</td> <td>192.168.0.5</td> <td>iosxrv-5</td> <td></td> <td></td> </tr> </tbody> </table>	Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...	0	Node SID	18115	0	192.168.0.5	iosxrv-5												
Segm...	Segment Type	Label	Algo	IP	Node	Interface	Sid T...																			
0	Node SID	18115	0	192.168.0.5	iosxrv-5																					

Path Name cfg_test_mcp_diff_paths_discr_10000
Policy Type Unknown
Metric Type TE
Disjoint Group ID:
Association Source: -
Type: -
PCE Initiated false
Affinity Exclude-Any: -
Include-Any: -
Include-All: -

Path Name cfg_test_mcp_diff_paths_discr_5000
Policy Type Unknown
Metric Type IGP
Disjoint Group ID:
Association Source: -
Type: -
PCE Initiated false
Affinity Exclude-Any: -
Include-Any: -
Include-All: -

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

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

The screenshot displays the network topology and the SR Policy Details panel. The topology map shows a network of nodes (iosxrv-2, iosxrv-3, iosxrv-4, iosxrv-5, iosxrv-6, iosxrv-7, xtc-iosxrv) with a candidate path highlighted in orange. The SR Policy Details panel shows the following candidate paths:

Path Name	Preference	Path Type
✓ <input type="checkbox"/> cfg_test_mcp_diff_paths_discr_10000	10000	Unknown
<input checked="" type="checkbox"/> cfg_test_mcp_diff_paths_discr_5000	5000	Unknown

The selected path details are as follows:

Seg...	Segment ...	Label	Algo	IP	Node
0	IGP Adj ...	24002	0	10.0.0.9	iosxr...
1	IGP Adj ...	24012	0	10.0.0.25	iosxr...

The path name is `cfg_test_mcp_diff_paths_discr_5000`, the policy type is `Unknown`, the metric type is `TE`, and the disjoint group ID is `Association Source: -`. The path is associated with a B-SID label of `24020`.

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

Crosswork Optimization Engine allows you to visualize the underlying path of a B-SID hop that you have manually configured on a device or configured using Crosswork Network Controller. In this example, we have assigned **24020** as a B-SID label on an SR-MPLS policy hop.



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

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

- Step 1** From the main menu, choose **Traffic Engineering > Traffic Engineering > SR-MPLS** or **SRv6** tab.
- Step 2** Check the check box next to the SR-MPLS policy that contains a hop assigned with a B-SID label and hover your mouse over any part of the SR-MPLS row to see the B-SID name. The B-SID path is highlighted in orange on the topology map. In this example, you see that the path is going from **iosxrv-2** to a 2-device cluster.

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

The screenshot shows the Traffic Engineering interface. On the left, a map displays several SR-MPLS paths between nodes. One path is highlighted in purple, labeled 'cfg_overlay-bsid_discr_100', connecting 'iosrv-2' (Prefix SID: 18112) to 'iosrv-7'. On the right, the 'SR POLICY' table is visible, showing a list of policies with columns for Headend, Endpoint, Color, Admin State, Oper State, and Actions. The policy 'iosrv-7' to 'iosrv-5' with Color 123 is selected.

Headend	Endpoint	Color	Admin ...	Oper S...	Actions
<input type="checkbox"/>	iosrv-2	iosrv-5	12345	↑	↑
<input type="checkbox"/>	iosrv-2	iosrv-5	54321	↑	↑
<input type="checkbox"/>	iosrv-2	iosrv-6	1868	↑	↑
<input checked="" type="checkbox"/>	iosrv-7	iosrv-5	123	↑	↑
<input type="checkbox"/>	iosrv-2	iosrv-7	8000	↑	↑
<input type="checkbox"/>	iosrv-2	iosrv-5	8500	↑	↑
<input type="checkbox"/>	iosrv-2	iosrv-5	111	↑	↑
<input type="checkbox"/>	iosrv-2	iosrv-5	888	↑	↑

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

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

The screenshot shows the 'SR Policy Details' window. The 'Summary' section displays the following information:

- Headend: iosrv-7 (TE RID: 192.168.0.7) PCC IP: 192.168.0.7
- Endpoint: iosrv-5 (TE RID: 192.168.0.5) Dest IP: 192.168.0.5
- Color: 123
- Admin State: Up
- Oper State: Up
- Binding SID: 24015
- Profile ID: -
- Utilization (Mbps): 0 Mbps
- Delay: -
- BWOD Policy Bandwidth (Mbps): 0 Mbps
- Accumulated Metric: 0
- Delegated PCE: -
- Non-delegated PCEs: 10.194.59.124
- PCE Computed Time: -
- Last Update: 17-Aug-2021 09:30:42 AM PDT

The 'Candidate Path' section shows a table of paths:

Path Name	Preference	Path Type
<input checked="" type="checkbox"/> cfg_overlay-bsid_discr_100	100	Unknown

Expanding the active path shows the following segments:

Seg...	Segment ...	Label	Algo	IP	Node
0	Node SID	18112	130	192.168...	iosxr...
1	B-Sid	24020		192.168...	iosxr...

Step 5 In the **SR Policy Details** window for the underlying path, expand the active path name to view more details. In this example, you see the underlying path actually goes from **iosrv-2** > **iosrv-3** > **iosrv-5**.

SR Policy Details

Headend iosxr-2 (TE RID: 192.168.0.2) PCC IP: 192.168.0.2
Source IP: 192.168.0.2
Endpoint iosxr-5 (TE RID: 192.168.0.5)
Dest IP: 192.168.0.5
Color: 111

Summary

- Admin State: Up
- Oper State: Up
- Binding SID: 24020
- Profile ID: -
- Utilization (Mbps): 0 Mbps
- Delay: -
- BWOD Policy Bandwidth (Mbps): 0 Mbps
- Accumulated Metric: 0
- Delegated PCE: -
- Non-delegated PCEs: 10.194.59.124
- PCE Computed Time: -
- Last Update: 17-Aug-2021 01:29:02 AM PDT

Candidate Path

Path Name	Preference	Path Type
cfg_test_explicit_mcp_discr_600	600	Unknown

Seg...	Segment ...	Label	Algo	IP	Node
0	Node SID	18113	0	192.168.0.2	iosxr-2
1	Node SID	18115	0	192.168.0.5	iosxr-5

Path Name: cfg_test_explicit_mcp_discr_600
Policy Type: Unknown
Metric Type: TE
Disjoint Group: ID: -
 Association Source: -
 Type: -
PCE Initiated: false

Visualizing Native SR Paths

Crosswork Optimization Engine The topology of a L3VPN service will show only the logical path and not the actual physical path. Since the feature uses multipaths, all ECMP paths will be shown between the source and destination. Visualizing the native path will help you in OAM (Operations, Administration and Maintenance) activities to monitor label-switched paths (LSPs) and quickly isolate forwarding problems to assist with fault detection and troubleshooting in the network.



Note This is applicable only for SR-MPLS policies.

To create a path query, do the following:

Before you begin

Confirm that device requirements are met. See [Visualize Native Path Device Prerequisites](#), on page 45.

For more information, see the [Cisco Crosswork Infrastructure and Applications Administration Guide](#) and the [Cisco Crosswork Infrastructure and Applications Installation Guide](#).

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

Visualizing Native SR Paths

- Step 2** On the Query Path Dashboard, click **New Query**.
- Step 3** Under the New Path Query, select the required values and click **Get Paths**.
- Step 4** Click **View Result** to view the query result.
- Step 5** (Optional) On the result pop-up click, **View Past Result**. Check the query ID to view the available results.

Example:

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

Figure 10: Path Details

The screenshot displays the Path Details interface. On the left, a map of the United States shows a path highlighted in purple between two points labeled PE-A and PE-B. The right panel, titled 'Path Details', contains the following information:

Select from the fields below to find available Native SR IGP Paths * Required field

Select Service: Select Type | Select Instance

Headend: PE-A (100.100.100.5)

Endpoint: PE-B (100.100.100.6)

Get Paths

Available Paths

Path 0

Output: tunnel-tc220
 Nexthop: 20.20.10.2
 Source: 100.100.100.5
 Destination: 127.0.0.0

Hop Details

Hop Index:0 | Hop Origin IP:100.100.100.5 | Hop Destination IP:20.20.10.2 | MRU:1500 | Labels: [24007/implicit-null] | net code:0 | return char: | multipaths:0

Hop Index:1 | Hop Origin IP:20.20.10.2 | Hop Destination IP:20.20.10.14 | MRU:1500 | Labels: [24022/implicit-null] | net code:8 | return char:L | multipaths:1

Hop Index:2 | Hop Origin IP:20.20.10.14 | Hop Destination IP:20.20.10.26 | MRU:1500 | Labels: [implicit-null/implicit-null] | net code:8 | return char:L | multipaths:1

Hop Index:3 | Hop Origin IP:20.20.10.26 | MRU:0 | net code:3 | return char?: | multipaths:0

- Step 6** From the **Actions** column, click **View Details**.
- Step 7** From the available paths, click **Path 0** to expand and view the active path.
- Example:**

Figure 11: Path Details

Path Details

Select from the fields below to find available Native SR IGP Paths * Required field

Select Service

Headend *

Endpoint *

Available Paths

Path 0

Output tunnel-te220
 Nexthop 20.20.10.2
 Source 100.100.100.5
 Destination 127.0.0.0

Hop Details

Hop Index:0 | Hop Origin IP:100.100.100.5 | Hop Destination IP:20.20.10.2 | MRU:1500 | Labels: [24007/implicit-null] | ret code:0 | return char: | multipaths:0

Hop Index:1 | Hop Origin IP:20.20.10.2 | Hop Destination IP:20.20.10.14 | MRU:1500 | Labels: [24022/implicit-null] | ret code:8 | return char:L | multipaths:1

Hop Index:2 | Hop Origin IP:20.20.10.14 | Hop Destination IP:20.20.10.26 | MRU:1500 | Labels:[implicit-null/implicit-null] | ret code:8 | return char:L | multipaths:1

Hop Index:3 | Hop Origin IP:20.20.10.26 | MRU:0 | ret code:3 | return char:! | multipaths:0

Visualize Native Path Device Prerequisites

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

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


```
grpc
port 50000
no-tls
address-family dual
!
mpls oam
!
```







Note

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

3. Devices should have GNMI capability enabled and configured.

- a. From **Device Management**, click on a device and view device details ().
- b. Confirm that GNMI capability and connectivity details are configured.

∨ Connectivity Details

Protocol *	IP Address / Subnet Mask *	Port *	Timeout	Encoding Type	
TELNET	172.29.105.236 / 24	23	30		
SNMP	172.29.105.236 / 24	161	30		
SSH	172.29.105.236 / 24	22	30		
GNMI	172.29.105.236 / 24	57400	30	JSON	

[+ Add Another](#)

Capability*

YANG MDT
 TL1
 YANG CLI
 YANG EPNM
 SNMP
 GNMI

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

```
RP/0/RP0/CPU0:xrwr-7.2.1#config
```

```
RP/0/RP0/CPU0:xrwr-7.2.1(config)#router static
```

```
RP/0/RP0/CPU0:xrwr-7.2.1(config-static)#address-family ipv4 unicast <CDG Southbound interface IP: eg. 172.24.97.110> <Device Gateway eg: 172.29.105.1>
```

```
RP/0/RP0/CPU0:xrwr-7.2.1(config-static)#commit
```



CHAPTER 4

Visualize Flexible Algorithms

Flexible Algorithm allows operators to customize and compute the IGP shortest path according to their own needs and constraints (specific metrics and link properties). Many possible constraints can be used to compute a path over a network. For example, Flexible Algorithm can confine the path to a particular plane for networks with multiple logical planes. Since the meaning of the algorithm is not defined by any standard, but is defined by the user, it is called a Flexible Algorithm.

Crosswork enables you to filter the IGP topology based on Flexible Algorithm and visualize the subset of the network that is capable of providing a specific set of transport characteristics. The ability to visualize Flexible Algorithm topologies provides an important tool to help you deploy, maintain, and verify that the configured Flexible Algorithm intent is realized in your network. For example, to improve service availability, you may use Flexible Algorithm to define disjoint logical topologies to increase resiliency to network failures. Crosswork allows you to visualize both Flexible Algorithm topologies simultaneously and verify they have no common nodes or links. Or if they do, help you determine the common network elements so that you can update Flexible Algorithm configurations.

Important Notes

- Flexible Algorithm information is collected from the SR-PCE (running Cisco IOS XR 7.3.2).
- You cannot provision SR-MPLS policies or RSVP-TE tunnels with Flexible Algorithm constraints.
- You cannot filter Flexible Algorithms on multiple domains.



Note Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering**.

- [Visualize Flexible Algorithm, on page 47](#)
- [Configure Flexible Algorithm Affinities, on page 49](#)
- [Find Flexible Algorithms for Links and Devices, on page 50](#)

Visualize Flexible Algorithm


Crosswork allows you to visualize Flexible Algorithm nodes and links that have been configured manually in your network.

Before you begin

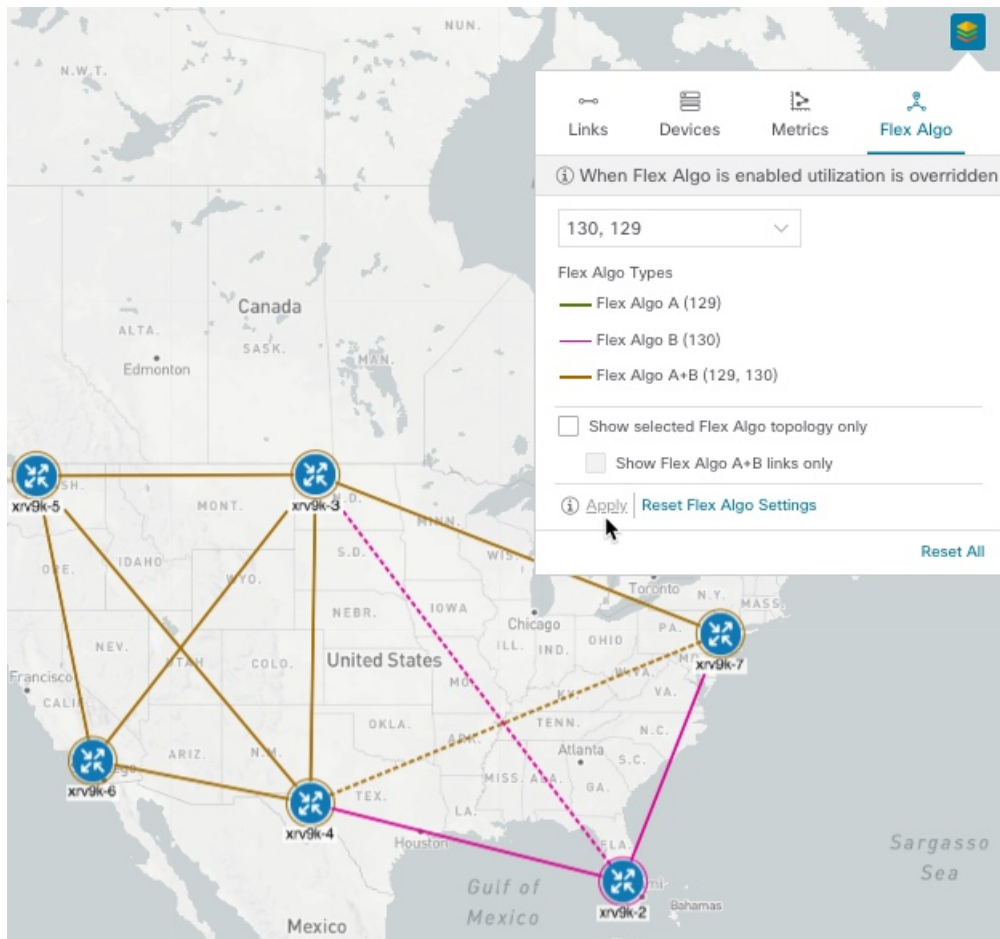
- You must configure Flexible Algorithms in your network. See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example: [Asr900 Flex Algorithm](#))
- You should know the Flexible Algorithm IDs that are used in your network. To view Flexible Algorithm membership, see [Find Flexible Algorithms for Links and Devices, on page 50](#).



Note You cannot visualize Flexible Algorithms if a Flexible Algorithm ID is the same across different domains.

-
- Step 1** From the main menu, select **Traffic Engineering > Traffic Engineering**.
- Step 2** From the topology map, click .
- Step 3** Click the **Flex Algo** tab.
- Step 4** From the drop-down list, select up to two Flexible Algorithm IDs.
- Step 5** View the Flexible Algorithm Types and confirm that the selection is correct. Also, note the color assignments for each Flexible Algorithm.
- Step 6** (Optional) Check the **Show selected Flex Algo topology only** check box to isolate the Flexible Algorithms on the topology map. When this option is enabled, SR policy selection is disabled.
- a) Check the **Show Flex Algo A+B links only** to show only those links and nodes that participate in both Flexible Algorithms.
- Step 7** Click **Apply**. You must click **Apply** for any additional changes to Flexible Algorithm selections to see the update on the topology map.

Example:



- Note**
- You cannot filter Flexible Algorithm IDs that are on multiple domains. Domain filtering is not supported based on Flexible Algorithms.
 - If a selected Flexible Algorithm is defined with criteria but there are no link and node combinations that match it (for example, a defined affinity to include all nodes or links with the color blue), then the topology map will be blank. If a selected Flexible Algorithm is not configured on a node or link, then the default blue link or node color appears.

Step 8 (Option) Click **Save View** to save the topology view and Flexible Algorithm selections.

Configure Flexible Algorithm Affinities

Flexible Algorithm affinities that are defined on devices are not collected by Crosswork Optimization Engine. The affinity mapping name is used for visualization. For this reason, you should manually collect Flexible Algorithm affinities on the device interface, then define an affinity mapping in the UI with the same name and bits that are used on the device interface.

The following ISIS and OSPF configuration sub-mode is used to configure Flexible Algorithm:

```
router isis instance flex-algo algo
router ospf process flex-algo algo
```

The following commands are used to configure Flexible Algorithm definition under the flex-algo sub-mode:

- IS-IS

```
metric-type delay
```



Note By default the regular IGP metric is used. If delay metric is enabled, the advertised delay on the link is used as a metric for Flexible Algorithm computation.

- OSPF

```
metric-type {delay | te-metric}
```



Note By default the regular IGP metric is used. If delay or TE metric is enabled, the advertised delay or TE metric on the link is used as a metric for Flexible Algorithm computation.

- *name*—name of the affinity map

```
affinity exclude-any name1, name2, ...
```

- *priority value*—priority

```
priority priority value
```

See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example: [Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#))



Note To edit or delete an affinity mapping, click the relevant menu options.

-
- Step 1** From the main menu, select **Traffic Engineering > Affinities > Flex-Algo Affinities**.
 - Step 2** To add a new Flexible Algorithm affinity mapping, click **+ Create**.
 - Step 3** Enter the name (color) and the bit it will be assigned.
 - Step 4** Click **Save** to save the mapping.
-

Find Flexible Algorithms for Links and Devices

If you want to know all Flexible Algorithms that a device or link is a member of, do the following:

Before you begin

You must configure Flexible Algorithm in your network.

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

Step 2 To view a device's Flexible Algorithm membership:

- a) From the topology map, click on a device that you know is a member of at least one Flexible Algorithm.
- b) In the **Device Details** window, click the **Flex-Algo** tab.

The screenshot shows the 'Device Details' window with the 'Flex-Algo' tab selected. It displays two Flexible Algorithms:

- Algo 128:**
 - Participating:** Yes
 - Elected Definition:** Metric Type: LATENCY
 - Exclude-Any Affinity: Yellow(253), Red(255)
 - Include-Any Affinity: Blue(3)
 - Include-All Affinity: Green(5)
 - Advertised:** Yes
 - Priority: 210
 - Definition Equal to Local: No
- Algo 130:**
 - Participating:** Yes
 - Elected Definition:** Metric Type: LATENCY
 - Exclude-Any Affinity:
 - Include-Any Affinity:
 - Include-All Affinity:
 - Advertised:** No
 - Priority: 200

Step 3 To view a link's Flexible Algorithm membership:

- a) From the topology map, click a link that you know is a member of at least one Flexible Algorithm.
- b) In the **Links** page, click one of the link types.
- c) By default, the **Summary** tab is displayed within the **Link Details** window. View **foreign agent Topologies** to see what Flexible Algorithm each source and destination device belong to.

Link Details



Summary

SR-MPLS

SRv6

RSVP-TE

Name GigabitEthernet0/0/0/1-GigabitEthernet0/0/0/0
State Up
Link Type L3 ISIS IPV4
ISIS Level 2
Last Update 24-Aug-2021 09:51:59 AM PDT

	A Side	Z Side
Node	xrv9k-7	xrv9k-3
TE Router ID	192.168.0.7	192.168.0.3
IF Name	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/0
IF Description	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/0
IF Alias	T-SDN Interface	
Type	ETHERNETCSMACD	ETHERNETCSMACD
IP Address	10.0.0.42	10.0.0.41
Utilization	0% (0Bps/1Gbps)	0% (0Bps/1Gbps)
IGP Metric	10	10
Delay Metric	10	10
TE Metric	10	10
FA Affinities		
Admin Groups	2,5	2,5
FA Topologies	128, 129, 130, 131, 132, 133, 134, 207	128, 129, 130, 131, 132, 133, 134



CHAPTER 5

Visualize RSVP-TE Tunnels



Note Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering**.

This section contains the following topics:

- [View RSVP-TE Tunnels on the Topology Map, on page 53](#)
- [View RSVP-TE Tunnel Details, on page 55](#)
- [View Traffic Engineering Device Details, on page 57](#)

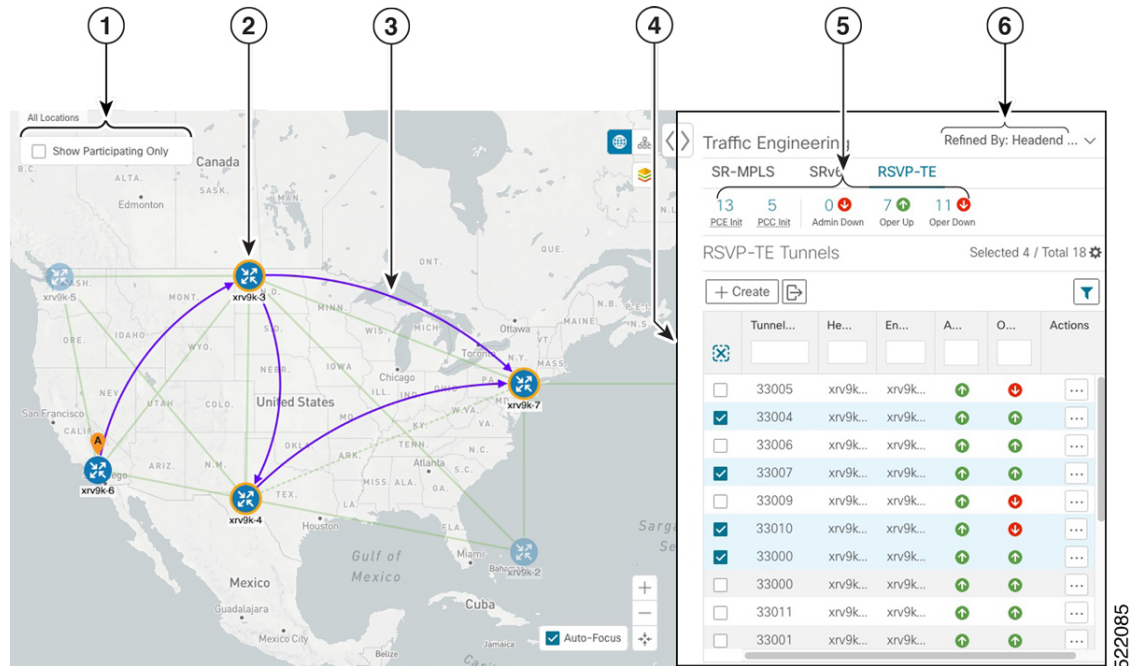
View RSVP-TE Tunnels on the Topology Map



To get to the Traffic Engineering topology map for RSVP-TE visualization, choose **Traffic Engineering > Traffic Engineering > RSVP-TE** tab.



Note Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering**.

Figure 12: Traffic Engineering UI - RSVP-TE Tunnels



Callout No.	Description
1	Click Show Participating Only to display links that only belong to the selected RSVP-TE tunnels. All other links and devices disappear.
2	A device with a solid orange outline () indicates that it is a strict hop. A dashed orange outline indicates that a loose hop was discovered. Note RSVP-TE tunnels cannot be configured with loose hops when provisioning in the UI.
3	When RSVP-TE tunnels are selected in the RSVP-TE Tunnel table, they show as purple directional lines on the map indicating source and destination. <ul style="list-style-type: none"> Record Route Object (RRO) paths are shown as straight lines. Explicit Route Object (ERO) paths are shown as curved lines. Note If both RRO and ERO paths are available, the RRO path is displayed by default. <ul style="list-style-type: none"> An adjacency segment ID (SID) is shown as a green dot on a link along the path (. <p>If both A and Z are displayed in a device cluster, at least one node in the cluster is a source and another is a destination. The A+ denotes that there is more than one RSVP-TE tunnel that originates from a node. The Z+ denotes that the node is a destination for more than one RSVP-TE tunnel.</p>

Callout No.	Description
4	<p>The content of this window depends on what has been selected or filtered. In this example, the RSVP-TE tab is selected and the RSVP-TE Tunnels table is displayed. Depending on what is selected on the topology map, or whether you are in the process of viewing and managing RSVP-TE tunnels, you can do the following:</p> <ul style="list-style-type: none"> • Create Dynamic RSVP-TE Tunnels Based on Optimization Intent, on page 70 • Create Explicit RSVP-TE Tunnels, on page 69 • Modify RSVP-TE Tunnels, on page 71 • View RSVP-TE Tunnel Details, on page 55 • View Device and Link Details, on page 12
5	Exports <i>all</i> data into a CSV file. You cannot export selected or filtered data.
6	The Mini Dashboard provides a summary of the operational RSVP-TE tunnel status and the number of PCC and PCE initiated tunnels that are <i>currently</i> listed in the RSVP-TE tables. If filters are applied, the Mini Dashboard is updated to reflect what is displayed in the RSVP-TE table.
7	<p>This option allows you to choose how the group filter (when in use) should be applied on the table data. For example, if Headend only was selected, then it would only display policies where the headend device of the policy is in the selected group. This filter allows you to see specific configurations and is useful when you have a large network.</p> <p>Filter options:</p> <ul style="list-style-type: none"> • Headend or Endpoint—Show policies with either the headend or endpoint device in the selected group. • Headend and Endpoint—Show policies if both the headend and endpoint are in the group. • Headend only—Show policies if the headend device of the policy is in the selected group. • Endpoint only—Show policies if endpoint device of the policy is in the selected group.

View RSVP-TE Tunnel Details

View RSVP-TE tunnel details such as binding label, delegated PCE, metric type, ERO/RRO, delay, and so on.

Step 1 From the **Actions** column, click  > **View Details** for one of the RSVP-TE tunnels.

View RSVP-TE Tunnel Details

The screenshot displays the Cisco Traffic Engineering interface. On the left, a map of North America shows several RSVP-TE tunnels (labeled xrv9k-3, xrv9k-4, xrv9k-6, xrv9k-7, xrv9k-2, xrv9k-5) connecting various nodes. A purple tunnel is highlighted. On the right, the 'Traffic Engineering' dashboard shows the 'RSVP-TE' tab selected. Below the dashboard, a table lists 15 RSVP-TE tunnels. The tunnel with ID 33000 is selected, and a 'View Details' button is visible over its row.

Tunnel ID	Headend	Endpoint	Admin St...	Oper Sta...	Actions
33005	xrv9k-3	xrv9k-7	+	+	...
33004	xrv9k-3	xrv9k-7	+	+	...
33006	xrv9k-3	xrv9k-7	+	+	...
33007	xrv9k-3	xrv9k-7	+	+	...
33009	xrv9k-3	xrv9k-7	+	+	...
33010	xrv9k-3	xrv9k-7	+	+	...
33000	xrv9k-6	xrv9k-7	+	+	View Details Edit / Delete
33000	xrv9k-7	xrv9k-5	+	+	...
33011	xrv9k-3	xrv9k-5	+	+	...
33001	xrv9k-7	xrv9k-5	+	+	...
32321	xrv9k-5	xrv9k-7	+	+	...
33013	xrv9k-3	xrv9k-7	+	+	...
33014	xrv9k-3	xrv9k-7	+	+	...
33015	xrv9k-3	xrv9k-7	+	+	...
1235	xrv9k-3	xrv9k-7	+	+	...

Step 2 View RSVP-TE tunnel details.**Note**

- For end-to-end delays on RSVP-TE tunnels, inter-domain RSVP-TE tunnels must all be explicit (every interface along that path is specified as an adjacency hop).
- The Delay value is calculated for all policies every 10 minutes. Hover your mouse over the "i" icon (next to the Delay value) to view the last time the value was updated.

RSVP-TE Tunnel Details
⋮ | ✕

Headend A xrv9k-6 (192.168.0.6)

Endpoint Z xrv9k-7 (192.168.0.7)

Tunnel ID 33000

▼ Summary

- Description** -
- Path Name** 60701-rsvp
- LSP ID** 6
- Path Type** Unknown
- Admin State** ↑ Up
- Oper State** ↑ Up
- Utilization** 0 Mbps
- Delay** 109 ⏱
- Signaled Bandwidth** 0 Mbps
- Setup / Hold Priority** 7 / 7
- Metric Type** IGP
- Fast Re-route (FRR)** Disable
- Binding Label** 24012
- Accumulated Metric** 20
- Disjoint Group** ID: -
Association Source: -
Type: -
- PCE Initiated** true
- Delegated PCE** 2001:420:28f:2011:250:56ff:fe85:a025
- Non-delegated PCEs** -
- Affinity** Exclude-Any: -
Include-Any: -
Include-All: -
- PCE Computed Time** 27-Oct-2021 12:33:03 PM PDT
- Last Update** 27-Oct-2021 12:39:58 PM PDT

Explicit Route Object (ERO)

Hop	Node	IP	Interface Name	Type
0	xrv9k-3	10.0.0.29	GigabitEthernet0/0/0/4	Strict
1	xrv9k-7	10.0.0.42	GigabitEthernet0/0/0/1	Strict

View Traffic Engineering Device Details

To view Traffic Engineering Device details (SR-MPLS, SRv6, RSVP-TE, and Flexible Algorithm information), do the following:

- Step 1** From the main menu choose **Traffic Engineering > Traffic Engineering**.
- Step 2** From the Traffic Engineering map, click on a device.
- Step 3** From the **Device Details** page, click on the traffic engineering tab you are interested in. The tab displays associated data for that device. The following example shows SR-MPLS Prefix information which includes the MSD value for the device.

View Traffic Engineering Device Details

Device Details

- Details
- Links
- SR-MPLS
- SRv6
- RSVP-TE
- Flex-Algo

Policies Prefixes

> IGP: Domain ID: 1100, ISIS System ID: 0000.0000.0017, Level: 2

SRGB 16000 - 23999
 SRLB 15000 - 15999
MSD 10

Prefixes	Label
No Rows To Show	

> IGP: Domain ID: 1000, ISIS System ID: 0000.0000.0007, Level: 2



CHAPTER 6

Provision SR-MPLS Policies



Note

- SRv6 policies cannot be provisioned using Crosswork Optimization Engine.
- Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using Crosswork Optimization Engine within the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering > Traffic Engineering**.

This section contains the following topics:

- [SR-MPLS Policy Support, on page 59](#)
- [SR-TE Policy Configuration Sources, on page 61](#)
- [Create Explicit SR-MPLS Policies, on page 62](#)
- [Configure Link Affinities, on page 63](#)
- [Create Dynamic SR-MPLS Policies Based on Optimization Intent, on page 63](#)
- [Modify SR-MPLS Policies, on page 64](#)

SR-MPLS Policy Support

Table 1: Supported Features

Capability	Notes
PCE-initiated policies (provisioned or discovered by Crosswork)	—
PCC-initiated policies (discovered by Crosswork)	—
SR-MPLS On-Demand Next Hop (ODN) policies discovered by Crosswork	—
Single consistent Segment Routing Global Block (SRGB) configured on routers throughout domain covered by Crosswork	If index SIDs are used and there are different SRGB bases along a path of a policy, the label can change along the path.
Prefix SID	—

Capability	Notes
Adjacency SID	—
EPE adjacency SID	—
Protected and Unprotected adjacency SIDs	—
Regular and Strict prefix SIDs	—
SR-MPLS policy optimization objective min-metric (IGP, TE, and Latency)	—
SR-MPLS policy path constraints (affinity and disjointness)	Only 2 SR-MPLS policies per disjoint group or sub-id are supported
Binding SID for explicit or dynamic policies	—
Profile ID	—

Table 2: Unsupported Features and Limitations

Description	Notes
Provisioning multiple candidate paths via Crosswork	These paths are not discovered if configured on PCC. Crosswork does not support configuration of these paths.
Weighted Equal-Cost Multipath (WECMP)	—
Multiple segment lists per candidate path	<ul style="list-style-type: none"> • This configuration is not supported • These segment lists will not be discovered if configured on a PCC.
Visualization of multiple candidate paths	Only the current active path can be seen in the UI.
Binding SIDs as Segment List Hops	—
SR IGP Flexible Algorithm (Flex Algo)	—
Anycast SIDs	—
Hop count metric type for policies	Cisco Crosswork does not support provisioning with this metric type and does not discover this metric type if configured on the PCC
Routers that are not SR-capable	The assumption is that all routers discovered by Cisco Crosswork are SR-capable

Description	Notes
SR-MPLS policies with Loopback IPs other than TE router ID for headend/endpoint and prefix SIDs in segment list	For more information, see the "Onboard and Manage Devices" chapter in the <i>Cisco Crosswork Infrastructure and Applications Administration Guide</i> .
SR-MPLS policy provisioned with IPv6 endpoints/hops	—
SRv6	Only 2 SR-TE policies per disjoint group/sub-id
SR-MPLS policy optimization objective min-metric with margin	Not supported for policies provisioned by Cisco Crosswork. Margin is not discovered for PCC-initiated policies.
SR-MPLS policy constraints (resource exclusion or metric bound)	Not supported for policies provisioned by Cisco Crosswork. Constraints are not discovered for PCC-initiated policies.

SR-TE Policy Configuration Sources

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

- PCC initiated—Policies configured on a PCC (see [PCC-Initiated SR-TE Policy Example, on page 61](#)). This policy type displays as **Unknown** in the UI.
- PCE initiated—Policies configured on a PCE or created dynamically by Crosswork Optimization Engine. SR-MPLS explicit or dynamic policies that are configured using the UI are the only types of SR-TE policies that you can modify or delete in Crosswork Optimization Engine. PCE Initiated policy types can be one of the following:
 - **Dynamic**
 - **Explicit**
 - **Bandwidth on Demand**
 - **Bandwidth Optimization**
 - **Local Congestion Mitigation**

PCC-Initiated SR-TE Policy Example

The following example shows a configuration of an SR-TE policy at the headend router. The policy has a dynamic path with affinity constraints computed by the headend router. See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example: [Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#)).

```
segment-routing
 traffic-eng
```


```


policy foo
  color 100 end-point ipv4 1.1.1.2
  candidate-paths
    preference 100
    dynamic
      metric
        type te
      !
    !
  constraints
    affinity
      exclude-any
        name RED
      !
    !
  !
!

```

Create Explicit SR-MPLS Policies

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

-
- Step 1** From the main menu, choose **Traffic Engineering > Traffic Engineering > SR-MPLS** tab.
- Step 2** From the **SR Policies** table, click **+ Create**.
- Step 3** Enter the required SR-MPLS policy values. Hover the mouse pointer over  to view a description of each field.
- Tip** If you have set up device groups, you can select the device group from the **Device Groups** drop-down menu. Then navigate and zoom in on the topology map to click the device for headend or endpoint selection.
- Step 4** Under Policy Path, click **Explicit Path** and enter a path name.
- Step 5** Add segments that will be part of the SR-MPLS policy path.
- Step 6** Click **Preview**.
- Step 7** If you want to commit the policy path, click **Provision**.
- Step 8** Validate the SR-MPLS policy creation:
- Confirm that the new SR-MPLS policy appears in the SR Policy table. You can also click the check box next to the policy to see it highlighted in the map.

Note The newly provisioned SR-TE policy may take some time, depending on the network size and performance, to appear in the **SR Policy** table. The **SR Policy** table is refreshed every 30 seconds.
 - View and confirm the new SR-MPLS policy details. From the **SR Policy** table, click  and select **View**.
- Note** On a scaled setup with high node, policy, or interface counts, a timeout may occur during policy deployment. To configure timeout options, see the [Cisco Crosswork Infrastructure and Applications Administration Guide](#).
-

Configure Link Affinities

Affinities defined on devices are not collected by Crosswork Optimization Engine. The affinity mapping name is only used for visualization in Crosswork Optimization Engine. For this reason, you should manually collect affinities on the device interface, then define affinity mapping in Crosswork Optimization Engine with the same name and bits that are used on the device interface. Crosswork Optimization Engine will only send bit information to SR-PCE during provisioning.

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

See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example: [Asr9000 Configuration](#))



Note To edit or delete an affinity mapping, click the relevant menu options.

- Step 1** From the main menu choose **Traffic Engineering > Affinities**. You can also define affinities while creating an SR-TE policy or RSVP-TE tunnel by clicking **Manage Mapping**.
- Step 2** To add a new affinity mapping, click **+ Create**.
- Step 3** Enter the name (color) and the bit it will be assigned.
- Step 4** Click **Save** to save the mapping.


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


Create Dynamic SR-MPLS Policies Based on Optimization Intent

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




Tip If you plan to use affinities, collect affinity information from your devices and then map them in Cisco Crosswork before creating a dynamic SR-MPLS policy. For more information, see [Configure Link Affinities, on page 63](#).

-
- Step 1** From the main menu, choose **Traffic Engineering > Traffic Engineering > SR-MPLS** tab.
- Step 2** From the **SR Policy** table, click + **Create**.
- Step 3** Under **Policy Details**, enter the required SR-MPLS policy values. Hover the mouse pointer over  to view a description of each field.
- Tip** If you have set up device groups, you can select the device group from the **Device Groups** drop-down menu. Then navigate and zoom in on the topology map to click the device for headend or endpoint selection.
- Step 4** Under **Policy Path**, click **Dynamic Path** and enter a path name.
- Step 5** Under **Optimization Objective**, select the metric you want to minimize.
- Step 6** Define any applicable constraints and disjointness.
- Note**
- Affinity constraints and disjointness cannot be configured on the same SR-MPLS policy. Also, there cannot be more than two SR-MPLS policies in the same disjoint group or subgroup. The configuration will not be allowed during Preview.
 - If there are existing SR-MPLS policies belonging to a disjoint group that you define here, all SR-MPLS policies that belong to that same disjoint group are shown during Preview.
- Step 7** Under **Segments**, select whether or not public segments should be used when available.
- Step 8** Click **Preview**. The path is highlighted on the map.
- Step 9** If you want to commit the policy path, click **Provision**.
- Step 10** Validate the SR-MPLS policy creation:
- a. Confirm that the new SR-MPLS policy appears in the SR Policy table. You can also click the check box next to the policy to see it highlighted in the map.

Note The newly provisioned SR-MPLS policy may take some time, depending on the network size and performance, to appear in the **SR Policy** table. The **SR Policy** table is refreshed every 30 seconds.
 - b. View and confirm the new SR-MPLS policy details. From the **SR Policy** table, click  and select **View**.
- Note** On a scaled setup with high node, policy, or interface counts, a timeout may occur during policy deployment. To configure timeout options, see the [Cisco Crosswork Infrastructure and Applications Administration Guide](#).
-

Modify SR-MPLS Policies

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

-
- Step 1** From the main menu, choose **Traffic Engineering > Traffic Engineering > SR-MPLS** tab.
- Step 2** From the SR Policy table, locate the SR-MPLS policy you are interested in and click .
- Step 3** Choose **View** or **Edit/Delete**.

Note

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



CHAPTER 7

Provision RSVP-TE Tunnels



Note Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering**.

This section contains the following topics:

- [RSVP-TE Tunnel Support, on page 67](#)
- [RSVP-TE Tunnel Configuration Sources, on page 68](#)
- [Create Explicit RSVP-TE Tunnels, on page 69](#)
- [Configure Link Affinities, on page 70](#)
- [Create Dynamic RSVP-TE Tunnels Based on Optimization Intent, on page 70](#)
- [Modify RSVP-TE Tunnels, on page 71](#)

RSVP-TE Tunnel Support

Table 3: Supported Features

Capability	Notes
PCE-initiated tunnels (provisioned or discovered by Crosswork Optimization Engine)	—
PCC-initiated tunnels (discovered by Crosswork Optimization Engine)	—
ERO strict hops	—
ERO loose hops (PCC-initiated only)	—
FRR protection on tunnels provisioned by Crosswork Optimization Engine	—
Path optimization objective min-metric (IGP, TE, or Latency)	—

Capability	Notes
Path constraints (affinity and disjointness)	Only 2 RSVP tunnels per disjoint group or sub-id is supported
Binding Label for explicit and dynamic tunnels	—
Signaled Bandwidth	—
Setup/Hold Priority	—

Table 4: Unsupported Features and Limitations

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

RSVP-TE Tunnel Configuration Sources

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

- PCC initiated—RSVP-TE tunnels configured on a PCC (see [PCC-Initiated RSVP-TE Tunnel Example, on page 69](#)).
- Dynamically created.

PCC-Initiated RSVP-TE Tunnel Example

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

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


Create Explicit RSVP-TE Tunnels

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

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

Step 2 From the right window, click **RSVP-TE**.

Step 3 Under **RSVP-TE Tunnels**, click **+ Create**.

Step 4 Enter the required RSVP-TE Tunnel values. Hover the mouse pointer over  to view a description of each field.

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

Step 5 Under Policy Path, click **Explicit Path** and enter a path name.

Step 6 Add segments that will be part of the RSVP-TE path.

Step 7 Click **Preview**. The path is highlighted on the map.

Step 8 If you want to commit the tunnel path, click **Provision**.

Step 9 Validate the RSVP-TE tunnel creation:

- a. Confirm that the new RSVP-TE tunnel appears in the RSVP-TE Tunnels table. You can also click the check box next to the policy to see it highlighted in the map.

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

- b. View and confirm the new RSVP-TE tunnel details. From the **RSVP-TE** table, click ******* (in the same row as the RSVP-TE tunnel), and select **View**.

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

Configure Link Affinities

Affinities defined on devices are not collected by Crosswork Optimization Engine. The affinity mapping name is only used for visualization in Crosswork Optimization Engine. For this reason, you should manually collect affinities on the device interface, then define affinity mapping in Crosswork Optimization Engine with the same name and bits that are used on the device interface. Crosswork Optimization Engine will only send bit information to SR-PCE during provisioning.

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

See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example: [Asr9000 Configuration](#))



Note To edit or delete an affinity mapping, click the relevant menu options.

- Step 1** From the main menu choose **Traffic Engineering > Affinities**. You can also define affinities while creating an SR-TE policy or RSVP-TE tunnel by clicking **Manage Mapping**.
- Step 2** To add a new affinity mapping, click **+ Create**.
- Step 3** Enter the name (color) and the bit it will be assigned.
- Step 4** Click **Save** to save the mapping.


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


Create Dynamic RSVP-TE Tunnels Based on Optimization Intent

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




Tip If you plan to use affinities, collect affinity information from your devices and then map them in Cisco Crosswork before creating a dynamic RSVP-TE tunnel. For more information, see [Configure Link Affinities, on page 63](#).

-
- Step 1** From the main menu, choose **Traffic Engineering > Traffic Engineering**.
- Step 2** From the right window, click **RSVP-TE**.
- Step 3** Under **RSVP-TE Tunnels**, click + **Create**.
- Step 4** Enter the required RSVP-TE Tunnel values. Hover the mouse pointer over  to view a description of each field.
- Tip** If you have set up device groups, you can select the device group from the **Device Groups** drop-down menu. Then navigate and zoom in on the topology map to click the device for headend or endpoint selection.
- Step 5** Under **Tunnel Path**, click **Dynamic Path** and enter the Path Name.
- Step 6** Under **Optimization Objective**, select the metric you want to minimize.
- Step 7** Define any applicable constraints and disjointness.
- Note** Affinity constraints and disjointness cannot be configured on the same RSVP-TE tunnel. Also, there cannot be more than two RSVP-TE tunnels in the same disjoint group or subgroup. If there are existing RSVP-TE tunnels belonging to a disjoint group that you define here, all RSVP-TE tunnels that belong to that same disjoint group are shown during Preview.
- Step 8** Click **Preview**. The path is highlighted on the map.
- Step 9** If you want to commit the tunnel path, click **Provision**.
- Step 10** Validate the RSVP-TE tunnel creation:
- a. Confirm that the new RSVP-TE tunnel appears in the RSVP-TE Tunnels table. You can also click the check box next to the policy to see it highlighted in the map.

Note The newly provisioned RSVP-TE tunnel may take some time, depending on the network size and performance, to appear in the **RSVP-TE Tunnels** table. The **RSVP-TE Tunnels** table is refreshed every 30 seconds.
 - b. View and confirm the new RSVP-TE tunnel details. From the **RSVP-TE** table, click  and select **View**.
- Note** On a scaled setup with high node, policy, or interface counts, a timeout may occur during policy deployment. Please contact a Cisco representative to fine tune the timers involved.
-

Modify RSVP-TE Tunnels

To view, modify, or delete an RSVP-TE tunnel, do the following:

-
- Step 1** From the main menu, choose **Traffic Engineering > Traffic Engineering**.
- Step 2** From the **Traffic Engineering** window select the **RSVP-TE** tab.
- Step 3** Locate the RSVP-TE tunnel you are interested in and click .
- Step 4** Choose **View** or **Edit/Delete**.

Note

- You can only modify or delete RSVP-TE tunnels that have been created with the UI.
 - After updating the RSVP-TE tunnel details, you can preview the changes on the map before saving it.
-



CHAPTER 8

Use Local Congestion Mitigation (LCM) to Mitigate Network Congestion Locally



Note

- Functionality described within this section is only available as part of the Advanced RTM license package.
- Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using Crosswork Optimization Engine within the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering**.

- [Local Congestion Mitigation Overview, on page 73](#)
- [LCM Important Notes, on page 74](#)
- [LCM Calculation Workflow, on page 76](#)
- [Mitigate Congestion on Local Interfaces Example, on page 78](#)
- [Configure LCM, on page 85](#)
- [Add Individual Interface Thresholds, on page 87](#)
- [Monitor LCM Operations, on page 87](#)

Local Congestion Mitigation Overview

Local Congestion Mitigation (LCM) searches for congestion on a configurable cadence (as opposed to a triggered event) and provides localized mitigation recommendations in surrounding interfaces (local interface-level optimization) within a domain. LCM computes the shortest paths for one or more tactical policies to divert the minimal amount of traffic on a congested interface to alternate paths with sufficient bandwidth. It attempts to keep as much of the traffic on the original IGP path. If the user approves, LCM performs the mitigation through the deployment of Tactical Traffic Engineering (TTE) SR policies. LCM will not modify paths of existing deployments of SR policies to mitigate congestion. With LCM, you are able to do the following:

- Visually preview LCM recommendations on your network before you decide whether to commit the Tactical Traffic Engineering (TTE) SR policy deployment.
- Enable LCM to deploy changes in the network automatically to address congestion and network failures based on LCM solution configurations. For more information, see the advanced configuration options (**Auto Repair Solution** and **Adjacency Hop Type**) in [Configure LCM, on page 85](#).

LCM allows for a wider applicability of the solution in various network topologies such as that involving multiple IGP areas due to its simpler path computation and limitation to specific network elements. Focusing on the problem locally within a domain eliminates the need for simulating edge-to-edge traffic flows in the network through a full traffic matrix and allows for better scaling of large networks. Also, LCM performs the collection of TTE SR policy and interface counters via SNMP and does not require the use of SR-TM.

TTE tunnel recommendations are listed in the **LCM Operational Dashboard**. From the dashboard, you can visually preview the TTE SR policy recommendations before deployment. TTE SR policy deployment to resolve congestion is not automated. You must approve and commit LCM recommended actions. LCM also recommends removal of previous TTE SR policies (instantiated by LCM) if they are no longer needed.

LCM Important Notes

Consider the following information when using LCM:

- You must have the Advanced RTM license package to use LCM.
- You cannot enable LCM if Bandwidth Optimization is enabled.
- LCM supports domains with up to 2000 devices. A *domain* is an identifier assigned to an IGP process. Domains are learned from the network. The domain ID is taken from router configuration (`link-state instance-id`) that you use to advertise IGP with BGP-LS.
- LCM recommended solutions use the resources within a single domain only.
- LCM evaluates network utilization on a regular, configurable cadence of 5 minutes or more. The cadence is typically set to be greater than or equal to the SNMP traffic polling interval. The default cadence is 10 minutes.
- LCM leverages ECMP across parallel TTE SR policies and assumes roughly equal splitting of traffic. The degree to which actual ECMP splitting adheres to this assumption depends on the presence of large elephant flows and the level traffic aggregation.
- Traffic that can be optimized must not be carried on existing SR-TE policies.
- When domain interfaces and links are removed (intentionally or unintentionally), the following occurs:
 - As links go down (LINK_DOWN state), LCM configuration and the Domain UI card (see [Configure LCM, on page 85](#)) will remain available until the links are aged out (after 4 hours). This behavior is intentional as it gives you time to recover domain interfaces and links if this was done by mistake.
 - If you want to force domain removal before links age out, then you can remove links manually from the UI. The domain will remain in a "ready for deletion" status until the last link is removed.

LCM Platform Requirements

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

- Strict SID labels should be configured for SR.

Congestion Mitigation:

- The headend device should support Equal Cost Multi-Path (ECMP) across multiple parallel SR-TE policies
- 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
```

See SR configuration documentation for your specific device to view descriptions and supported configuration commands (for example: [Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers](#))

Contact your Cisco sales representative for an exhaustive list of platform requirements.

BGP-LS Speaker Placement for Multiple AS Networks with a Dedicated IGP Instance Between ASBRs

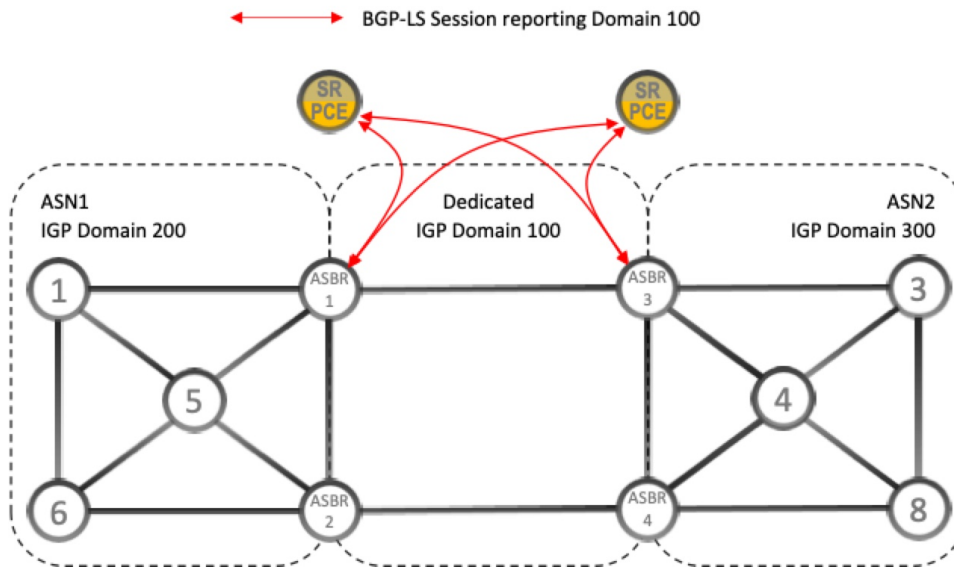
To support interdomain latency-optimized SR policy path computation by an SR-PCE (or other use cases where egress peer engineering (EPE) is not supported), a dedicated IGP instance may be configured between autonomous system border routers (ASBRs) in different ASNs. In these cases, it is important to identify which ASBRs report the topology via BGP-LS for proper topology discovery.

In the following example, at least one ASBR in each AS participating in the dedicated inter-AS IGP (Domain 100) must have BGP-LS enabled to report the IGP between each ASBR. Each ASBR must report the domain with the same BGP-LS identifier.



Note More than one ASBR per AS reporting the BGP-LS topology is also supported.

Figure 13: BGP-LS Session Reporting Domain 100



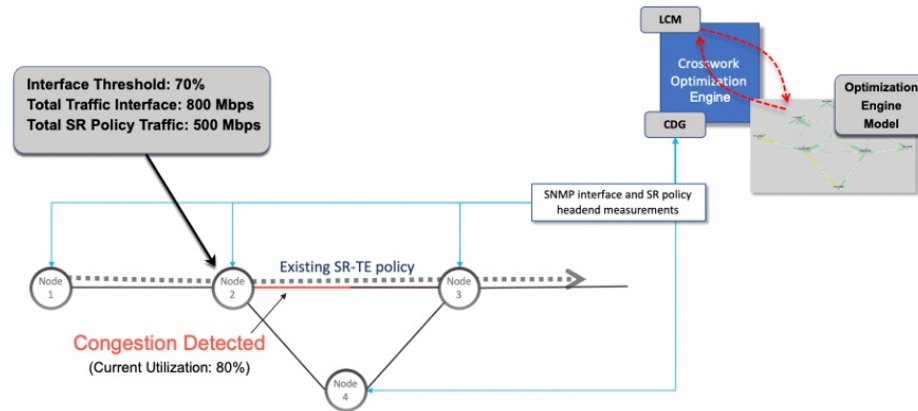
Previously Monitored Interfaces Missing After Upgrade

If a hostname change occurred in Crosswork Optimization Engine 2.0 and that system's backup is used to upgrade to the Crosswork Optimization Engine 3.0, any previously monitored LCM interface that belongs to the node with the updated hostname will not be migrated. Instead, these interfaces are dropped from the list of LCM monitored interfaces with a warning in the LCM logs. To workaround this, you can manually add the interfaces for LCM to monitor *after* the migration is complete and the system is stable.

LCM Calculation Workflow

This example walks you from congestion detection to the calculations LCM performs prior to recommending tactical tunnel deployment. With the release of Crosswork Optimization Engine 3.0, these calculations are done on a per domain basis which allows better scalability and faster calculation for larger networks.

Figure 14: LCM Configuration Workflow Example

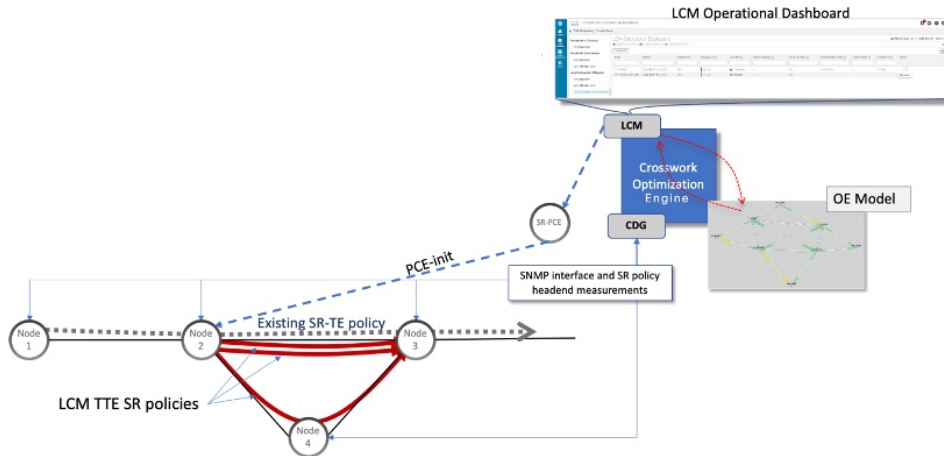


- Step 1** LCM first analyzes the Optimization Engine Model (a realtime topology and traffic representation of the physical network) on a regular cadence.
- Step 2** In this example, after a congestion check interval, LCM detects congestion when Node 2 utilization goes above the 70% utilization threshold.
- Step 3** LCM calculates how much traffic is eligible to divert.
- LCM only diverts traffic that is not already routed on an existing SR policy (for example: unlabeled, IGP routed, or carried via FlexAlgo-0 SIDs). The traffic within an SR-TE 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.
- $$\text{Total interface traffic} - \text{SR policy traffic} = \text{Eligible traffic that can be optimized}$$
- 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: $800 \text{ Mbps} - 500 \text{ Mbps} = 300 \text{ Mbps}$
- Step 4** LCM calculates the amount 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 100Mbps:
- $$800 \text{ Mbps} - 700 \text{ Mbps (70\% threshold)} = 100 \text{ Mbps}$$
- LCM must route 100 Mbps of 300 Mbps (eligible traffic) to another path. Note that if the Over-provisioning Factor (OPF) percentage is set to 10, then LCM must route 110 (100 Mbps x 1.10) of the eligible traffic. The OPF can be set in the Advanced tab within the LCM Configuration window. For more information, see [Configure LCM, on page 85](#).
- Step 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 detoured, 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 (100Mbps out of 300Mbps) 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 100Mbps) 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 hop via Node 4 (100 Mbps)

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



Step 6 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.

Mitigate Congestion on Local Interfaces Example

In this example, we will enable LCM and observe the congestion mitigation recommendations to deploy TTE SR policies when utilization on a device's interface surpasses a defined utilization threshold. We will preview the recommended TTE SR policies before committing them to mitigate the congestion. This example demonstrates the following workflow:

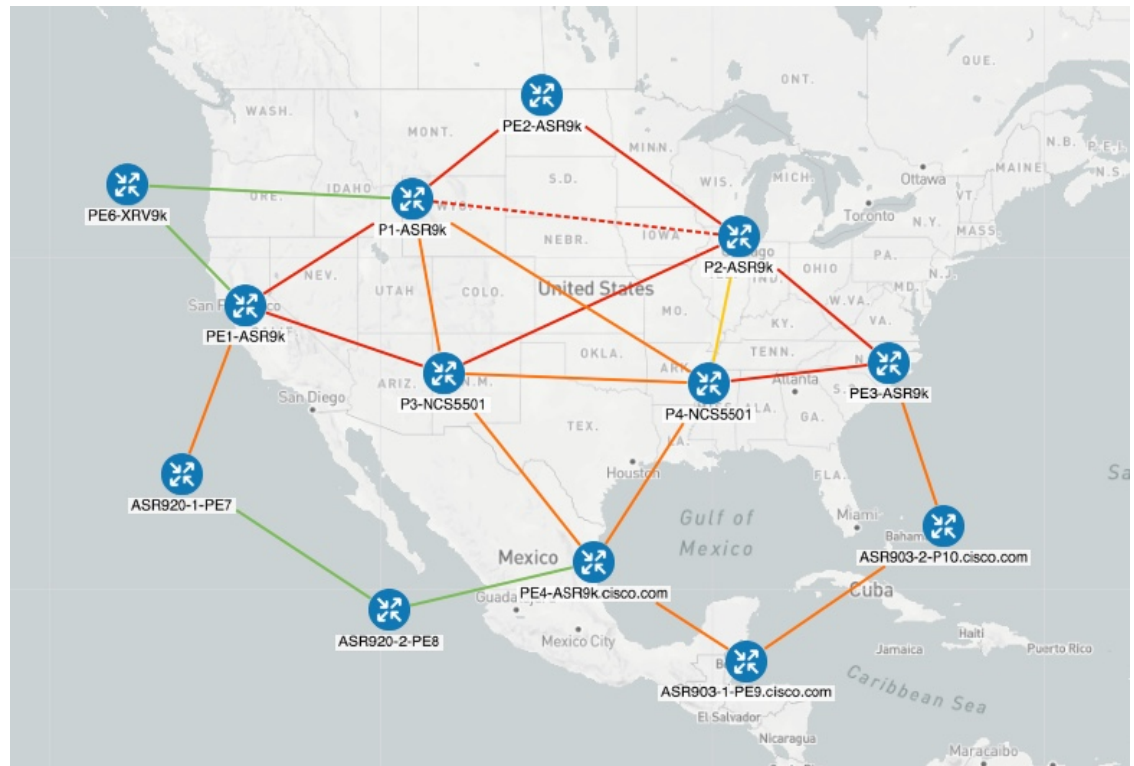
1. View uncongested topology.
2. Enable and configure LCM.
3. After LCM detects congestion, view LCM recommendations on the Operational Dashboard.
4. Preview the LCM TTE policies visually on the topology map.
5. Commit and deploy all LCM TTE policy recommendations to mitigate the congestion.
6. Verify that the LCM TTE policies have been deployed.



Note The utilization thresholds used in this example are extremely low (12%) and are best used for lab environments.

The following image shows the topology that will be used for this example.

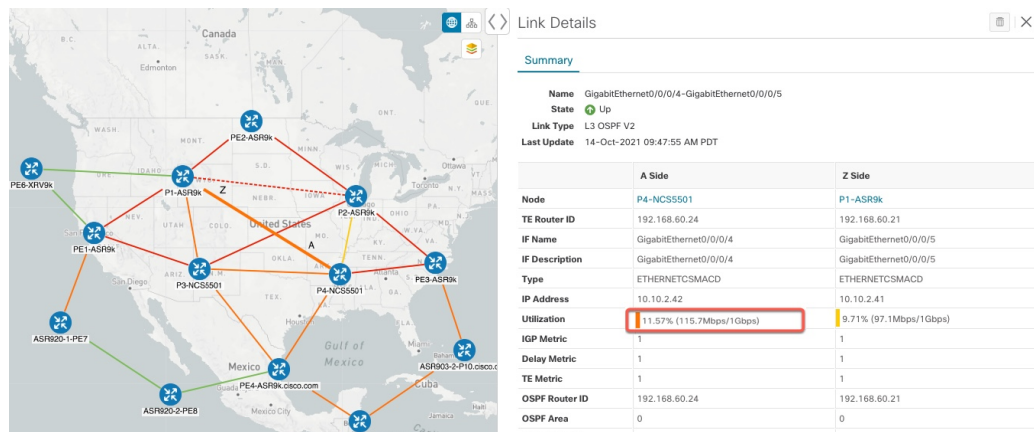
Figure 15: Initial Topology



Step 1 View initial topology and utilization prior to LCM configuration.

- Click on the link between P4-NCS5501 and P1-ASR9k to view link details. Note that utilization on P4-NCS5501 is 11.57% .

Figure 16: Initial Utilization



Step 2 Enable LCM and configure the global and custom interface utilization thresholds.

- a) From the main menu, choose **Traffic Engineering > Local Congestion Mitigation > Domain-ID > ... > Configuration**. In this example, the threshold is set at 12% and the **Interfaces to Monitor > Selected Interfaces** option is selected. For more information, see [Configure LCM, on page 85](#).

Figure 17: LCM Configuration Page

Configuration

Basic Advanced

Enable ⓘ False <input checked="" type="checkbox"/> True	Color ⓘ 2000 <small>Range: 1 to 4294967295</small>	Utilization Threshold ⓘ 12 <small>Range: 0 to 100</small>
Utilization Hold Margin ⓘ 5 <small>Range: 0 to Utilization Threshold</small>	Delete Tactical SR Policies when Disabled ⓘ False <input type="checkbox"/> True	Profile ID ⓘ 0 <small>Range: 0 to 65535</small>
Congestion Check Interval ⓘ 900 <small>Range: 600 to 86400 seconds</small>	Max LCM Policies per Set ⓘ 8 <small>Range: 1 to 8</small>	Interfaces to Monitor ⓘ <input checked="" type="radio"/> Selected Interfaces <input type="radio"/> All Interfaces
Description ⓘ LCM Startup Config		

- b) Click **Commit Changes** to save your configuration. 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.
- c) If you selected **Interfaces to Monitor > Selected Interfaces**, go to the **Link Management** page (**Traffic Engineering > Local Congestion Mitigation > Domain-ID > ... > Link Management**) and upload the list of interfaces with custom utilization thresholds. Only the interfaces listed on this page will be monitored for congestion. See the following example.

Note If **Interfaces to Monitor > All Interfaces** was selected then LCM would monitor all interfaces. This includes any individual thresholds that are imported to the **Link Management** page. The rest of the interfaces will be monitored using the global **Utilization Threshold** defined in the **Configuration** page.

Link Management

Total 4

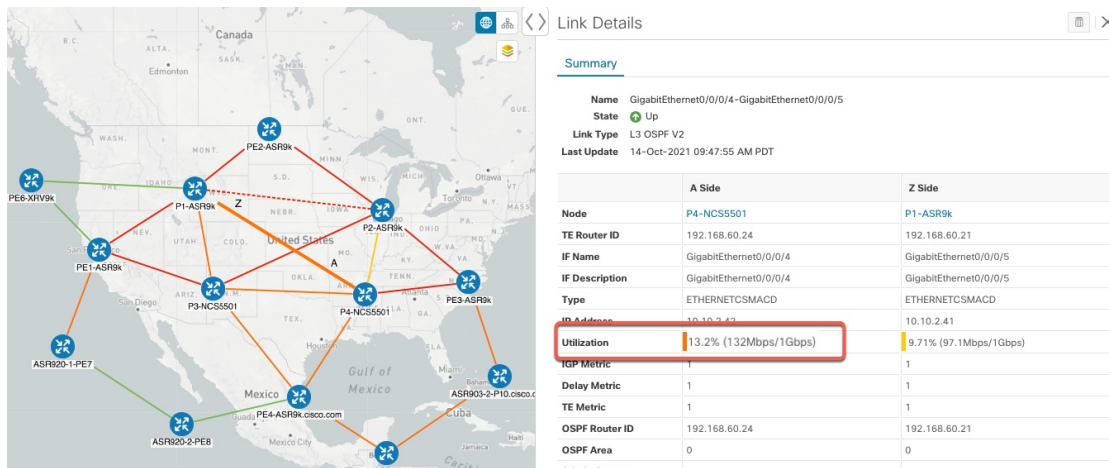
Interfaces with custom Thresholds should be uploaded to this page.

- If the **All Interfaces** option has been configured, interfaces and its Utilization Threshold defined and uploaded to this page will be monitored for congestion. All other interfaces will be monitored using the global Utilization Threshold defined in the Configuration page.
- If the **Selected Interfaces** option has been configured, only the interfaces and its Utilization Threshold defined and uploaded to this page will be monitored for congestion.

Node ↑	Interface	Threshold (%)
F3.cisco.com	GigabitEthernet0/0/0/1	30.0
F4.cisco.com	GigabitEthernet0/0/0/2	45.0
F5.cisco.com	GigabitEthernet0/0/0/0	20.0
F6.cisco.com	GigabitEthernet0/0/0/1	35.0

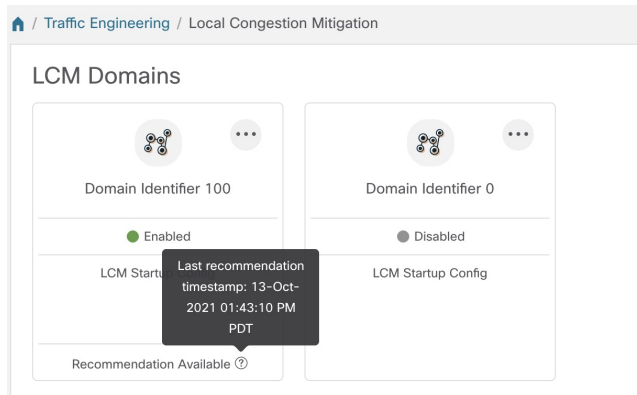
Step 3 After some time, congestion occurs surpassing the configured LCM threshold. In this example, utilization surpassed 12%.


Figure 18: Congestion



Step 4 View TTE SR policy recommendations in the LCM Operational Dashboard.

- Navigate to **Traffic Engineering > Local Congestion Mitigation**. When congestion is detected a domain will have a timestamp of recommended actions.



- b) (Optional) Click  > **Events** tab to view the new event. You can also monitor this window to view LCM events as they occur. You should see events for LCM recommendations, commit actions, and any exceptions. Below is an example of LCM events:

Alarms & Events

All System Network

Alarms **Events**

Selected / Total 929

Filters Applied (1)

Source	Severity	Description	Creation Time	Category	Correlated Alarm
LCM					
LCM for domain 100	Info	A new recommendation has been created: 2 creates, 0 updates, 0 delete...	30-AUG-2021 04:56:33 P...	System	NO
LCM for domain 100	Info	Recommendation committed.	30-AUG-2021 04:45:31 P...	System	NO
LCM for domain 100	Info	A new recommendation has been created: 0 creates, 0 updates, 6 delete...	30-AUG-2021 04:44:51 P...	System	NO
LCM for domain 100	Major	Mitigated interface F2.cisco.com GigabitEthernet0/0/0/5 is down.	30-AUG-2021 04:44:50 P...	System	NO
LCM for domain 100	Info	A new recommendation has been created: 0 creates, 2 updates, 4 delete...	30-AUG-2021 04:25:46 P...	System	NO
LCM for domain 100	Info	Recommendation committed.	30-AUG-2021 04:00:46 P...	System	NO
LCM for domain 100	Info	A new recommendation has been created: 1 creates, 5 updates, 0 delete...	30-AUG-2021 03:52:29 P...	System	NO
LCM for domain 100	Info	LCM is enabled	30-AUG-2021 03:52:11 P...	System	NO
LCM for domain 101	Info	LCM Worker with domain_id: '101' has started.	30-AUG-2021 03:52:04 P...	System	NO
LCM for domain 100	Info	LCM Worker with domain_id: '100' has started.	30-AUG-2021 03:52:04 P...	System	NO
LCM for domain 101	Info	LCM is disabled	30-AUG-2021 03:52:03 P...	System	NO

- c) Open the **Operational Dashboard (Traffic Engineering > Local Congestion Mitigation > Domain-ID > ... > Operational Dashboard)**.

The dashboard shows that the utilization has surpassed 12% and is at 13.01%. In the Recommended Action column, there is a recommendation to deploy TTE policy solution sets (Create Set) to address the congestion on the interface. The Expected Util column shows the expected utilization of each of the interface if the recommended action is committed. For more information, see [Monitor LCM Operations, on page 87](#).

Figure 19: LCM Operational Dashboard

Operational Dashboard

Last Refresh: 12-Oct-2021 09:14:03 AM PDT

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

Commit All Last Recommendation: 12-Oct-2021 09:02:23 AM PDT Urgency: MEDIUM

Node	Interface	Threshold Util	Evaluatio...	LCM State	Pol...	Pol...	Recomm...	Com...	Expected Util	Solution Up...	Actions
P4-NCS55	GigabitEthernet0/0/0/1	12%	13.01%	Congested	0	-	Create Set	None	11.97%	12-Oct-202...	...


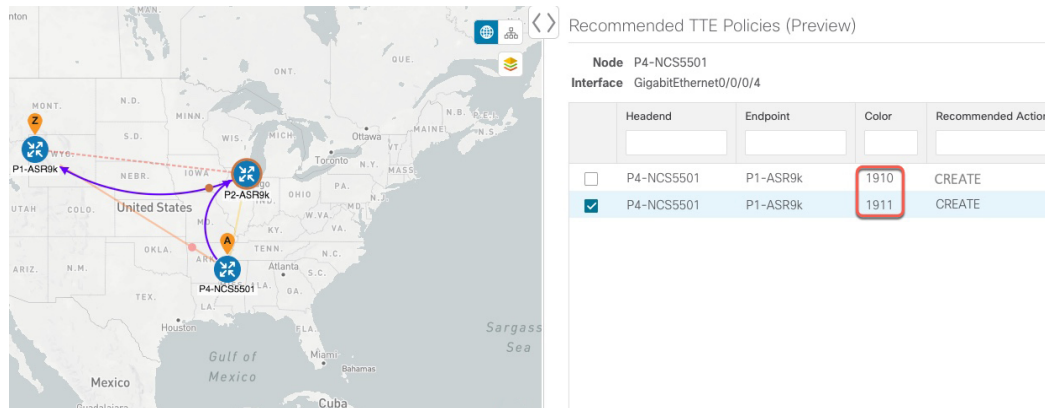
- d) Before committing TTE policies, you can preview the deployment of each TTE policy solution set. Click  in the Actions column and choose **Preview**. The window displays the node, interface, and the recommended action for each TTE policy. From the **Preview** window, you can select the individual TTE policies, and view different aspects and information as you would normally do in the topology map. The following figure shows the recommended TTE policies for the interface GigabitEthernet0/0/0/4. Note the Color IDs to later verify TTE policy deployment.

Figure 20: LCM TTE Deployment Preview



- e) After you are done viewing the recommended TTE policies on the map, navigate back to the **Operational Dashboard** and click **Commit All**. The LCM **Status** column changes to **Mitigating**.

Note 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 Last Refresh: 12-Oct-2021 09:14:03 AM PDT | ⌵

🔴 Congested Interfaces (0) | 🟡 Mitigating Interfaces (1) | 🟢 Mitigated Interfaces (0)

[Commit All](#) | Last Recommendation: 12-Oct-2021 09:02:23 AM PDT | Urgency: MEDIUM

Node	Interface	Threshold Util	Evaluation...	LCM State	Pol...	Pol...	Recomm...	Com...	Expected Util	Solution Up...	Actions
P4-NCS55	GigabitEthernet0/0/0/1	12%	13.01%	Mitigating	2	-	Create Set	None	11.97%	12-Oct-202...	⋮

Step 5 Validate TTE SR policy deployments.

- a) Click > **Events** tab. Note which LCM events are listed in the **Events** window.

Note 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. These alerts are reported in the UI and if desired can be forwarded to third party alerting/monitoring tools.

- b) Return to the **Operational Dashboard** to see that the LCM state changes to **Mitigated** for all TTE policy solution sets.

Note that the LCM state change will take up to 2 times longer than the SNMP cadence.

- c) Confirm the TTE policy deployment by viewing the topology map and the **SR Policy** table (**Traffic Engineering** > **Traffic Engineering** > **SR-MPLS** tab).

Mitigate Congestion on Local Interfaces Example

The screenshot shows the Traffic Engineering interface. On the left is a map of the United States with various network nodes and connections. On the right is the SR Policy configuration table. The table has columns for Headend, Endpoint, Color, Admin..., Oper..., and Actions. Two rows are selected and highlighted with a red box:

Headend	Endpoint	Color	Admin...	Oper ...	Actions	
<input type="checkbox"/>	PE2-AS...	ASR903...	2000	↑	↑	...
<input type="checkbox"/>	ASR920...	ASR903...	2001	↑	↑	...
<input type="checkbox"/>	ASR920...	PE2-AS...	3030	↑	↑	...
<input type="checkbox"/>	ASR903...	PE2-AS...	3040	↑	↓	...
<input type="checkbox"/>	ASR903...	PE4-AS...	5555	↑	↑	...
<input checked="" type="checkbox"/>	P4-NCS...	P1-ASR9k	1910	↑	↑	...
<input checked="" type="checkbox"/>	P4-NCS...	P1-ASR9k	1911	↑	↑	...
<input type="checkbox"/>	ASR903...	PE4-AS...	1910	↑	↑	...
<input type="checkbox"/>	ASR903...	PE4-AS...	1911	↑	↓	...
<input type="checkbox"/>	ASR903...	PE4-AS...	2000	↑	↑	...
<input type="checkbox"/>	ASR903...	PE4-AS...	2001	↑	↓	...
<input type="checkbox"/>	ASR903...	PE4-AS...	2201	↑	↓	...

d) Select one of the new SR-TE policies and view the SR policy details (click ... and choose **View Details**).

The screenshot shows the SR Policy Details view for the selected policy. The details are as follows:

- Headend:** P4-NCS5501 (TE RID: 192.168.60.24) PCC IP: 192.168.60.24
Source IP: 192.168.60.24
- Endpoint:** P1-ASR9k (TE RID: 192.168.60.21)
Dest IP: 192.168.60.21
- Color:** 1911
- Summary:**
 - Admin State: ↑ Up
 - Oper State: ↑ Up
 - Binding SID: 1004019
 - Segment Type: Unprotected
 - Policy Type: Local Congestion Mitigation** (highlighted with a red box)
 - Profile ID: 1981
 - Description: -
 - Utilization: 0 Mbps
 - Delay: 2 i
 - BWOD Policy Bandwidth: 0 Mbps
 - Accumulated Metric: 0
 - Delegated PCE: 172.29.10.121
 - Non-delegated PCEs: 172.29.10.122
 - PCE Computed Time: 14-Oct-2021 12:39:21 PM PDT
 - Last Update: 14-Oct-2021 12:39:21 PM PDT
- Candidate Path:**

Path Name	Preference	Path Type
● > lcm_to_P1-ASR9k_c_1911	100	Explicit

Step 6 Remove the TTE SR policies upon LCM recommendation.

- a) After some time, the deployed TTE SR policies might no longer be needed. This occurs if the utilization will continue to be under the threshold without the LCM-initiated TTE tunnels. In this case, LCM generates new recommended actions to delete the TTE SR policy sets. Click **Commit All** to remove the deployed TTE SR policies.
- b) Click **Commit All** to remove the SR policies.
- c) Confirm the removal by viewing the topology map and SR Policy table.

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-TE policies and decides whether or not they are still needed. If not, LCM recommends deleting them.

Related Topics

[Add Individual Interface Thresholds](#), on page 87

Configure LCM

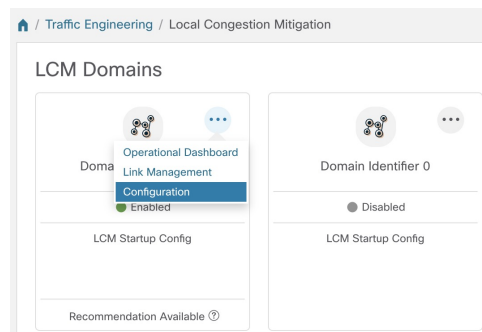
To enable and configure LCM:

Before you begin


Please review [LCM Important Notes](#), on page 74.

- Step 1** From the main menu, choose **Traffic Engineering > Local Congestion Mitigation > Domain-ID-card > ... > Configuration > Basic** tab.

Example:



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

- Step 3** Enter the required information. Hover the mouse pointer over  to view a description of each field.

The following list describes additional field information:

- **Utilization Threshold**—Set the utilization percent at which LCM will consider an interface to be congested. This value applies to all interfaces, unless you specify thresholds to individual interfaces in the **Link Management** page.

- **Profile ID**—This is a required configuration to enable traffic steering onto LCM policies. Autoroute (steers traffic into the tactical SR-TE policies LCM creates) is applied to SR-TE policies through the proper **Profile ID** option that is set here to align with the configuration on the PCC associating that Profile ID with autoroute feature.
- **Congestion Check Interval** (seconds)—This value determines the interval at which LCM will evaluate the network for congestion. Under a steady state, when there are no recommendation commits, it uses this interval to re-evaluate the network to determine if changes are required to recommendations. For example, if the interval is set to 600 seconds (10 minutes), LCM will evaluate the network every 10 minutes for new congestion and determine whether a new recommendation or modifications to existing recommendations are needed. Examples of modifications can include removal or updates to individual policies that were previously recommended. Since network changes may take time for the information to stabilize and propagate to LCM, set the interval to no less than twice the SNMP collection cadence.
- **Interfaces to Monitor**—By default, this is set to **Selected Interfaces** and you will need to add thresholds to individual interfaces by importing a CSV file in the **Link Management** page (**Traffic Engineering > Local Congestion Mitigation > Domain-ID > ... > Link Management**). Only interfaces defined in the **Link Management** page will be monitored. If set to **All Interfaces**, LCM will monitor the interfaces with custom thresholds that are uploaded in the **Link Management** page and the rest of the interfaces using the **Utilization Threshold** value configured on this page.
- **Advanced > Congestion Check Suspension Interval** (seconds)—This interval determines the time to wait (after a **Commit All** is performed) before resuming congestion detection and mitigation. Since this interval should allow time for network model convergence, set the interval to no less than twice the SNMP collection cadence.
- **Advanced > Auto Repair Solution**—If set to **True**, LCM will automatically delete any down, failed, or uncommitted LCM TTE policies. This option is mainly to address a failure in a policy.



If this option is disabled, and the **Urgency** status of the recommendation shown in the LCM Operational Dashboard is **High**, then the recommended solution is a candidate for the **Auto Repair Solution**. This means that a network failure will most likely occur if the solution is not deployed.
- **Advanced > Adjacency Hop Type**—If set to **Protected**, LCM will create SR policies using protected adjacency SIDs. This allows for Topology-Independent Loop-Free Alternate (TI-LFA) to compute a path for any adjacency failures.

Note This option should only be set to **Protected** if all nodes in the same IGP area as LCM is operating are strict SPF SID capable.
- **Advanced > Over-provisioning Factor** (OPF)—This option helps address unequal ECMP traffic distribution (elephant flows). This value determines the percentage of how much extra traffic should be accounted for when computing a path for a by-pass policy. If LCM needs to divert x amount of traffic due to congestion, then it will search for a path that can support $x * (1 + OPF)$ traffic. For more information, see [LCM Calculation Workflow, on page 76](#). The default value is 0.


Step 4 To save your configuration, click **Commit Changes**. If congestion occurs on any monitored interfaces, LCM will display *recommendations* (LCM will *not* automatically commit or deploy new TTE policies) on the **LCM Operational Dashboard**. You can then preview the recommended TTE policies and decide whether or not to commit and deploy them onto your network.

Add Individual Interface Thresholds



Networks have many different links (10G, 40G, 100G) that require different thresholds to be set. To assign specific threshold values for individual interfaces when using LCM or Bandwidth Optimization, do the following:


-
- Step 1** From the main menu, choose one of the following:
- **Local Congestion Mitigation > Link Management**
 - **Bandwidth Optimization > Link Management**
- Step 2** Click .
- Step 3** Click the **Download sample configuration file** link.
- Step 4** Click **Cancel**.
- Step 5** Open and edit the configuration file (sampleLcmLinkManagement.csv) you just downloaded. Replace the sample text with your specific node, interface, and threshold information.
- Step 6** Rename and save the file.
- Step 7** Navigate back to the **Link Management** window.
- Step 8** Click  and navigate to the CSV file you just edited.
- Step 9** Click **Import**.
- Step 10** Confirm that the information appears correctly in the **Link Management** window.
-

Monitor LCM Operations

The LCM Operational Dashboard (**Traffic Engineering > Local Congestion Mitigation > Domain-ID >  > Operational Dashboard**) shows congested interfaces as defined by the configured utilization threshold. For each interface, it lists details such as current utilization, recommended action, status, expected utilization after committing recommendations, and so on. Recommendations are listed as part of a set, and if deployed, all changes are committed. **Urgency** indicates the importance of recommendation deployment or action. Urgency values can be one of the following:

- **Low**—Indicates that LCM instantiated policies can be removed because they are no longer needed or that no changes are required.
- **Medium**—Indicates new or modified recommendations.
- **High**—Indicates network failures and recommendations should be deployed. This is a candidate that can be addressed automatically if the **Auto Repair Solution** advanced option was enabled. See [Configure LCM, on page 85](#).

Hover the mouse pointer over  to view a description of what type of information each column provides. From this dashboard, you can also preview ( > **Preview**) and deploy TTE policy recommendations.

In addition to the LCM Operational Dashboard, you can click  > **Events** tab. Note which LCM events are listed in the **Events** window.



CHAPTER 9

Use Bandwidth Optimization (BWOpt) to Optimize the Network



Note

- Functionality described within this section is only available as part of the Advanced RTM license package.
- Throughout this section, the navigation is documented as **Traffic Engineering > Traffic Engineering**. However, when using Crosswork Optimization Engine within the Crosswork Network Controller solution, the navigation is **Traffic Engineering & Services > Traffic Engineering**.

- [Bandwidth Optimization Overview, on page 89](#)
- [BWOpt Important Notes, on page 89](#)
- [Automated Network Congestion Mitigation Example, on page 91](#)
- [Configure Bandwidth Optimization, on page 94](#)
- [Add Individual Interface Thresholds, on page 95](#)
- [Troubleshoot Bandwidth Optimization, on page 95](#)

Bandwidth Optimization Overview

Bandwidth Optimization (BWOpt) provides closed-loop tactical traffic engineering (TTE) for segment routed policies by *automatically* detecting and mitigating congestion in your network. It achieves this through a real-time view of the network topology overlaid with a demand matrix built through telemetry-based Segment Routing Traffic Matrix (SRTM). The intent is to optimize bandwidth resource utilization by setting utilization thresholds on links. BWOpt uses the threshold interface utilization requested by the user and compares it to the actual utilization in the network. When interface congestion is detected by BWOpt, it attempts to reroute intent-based traffic from hot spots through the use of TTE SR policies which are deployed to the network via SR-PCE. As network conditions (topology and/or traffic) change over time, BWOpt continues to monitor interface utilization and manage any TTE SR policies deployed, including changing their paths and/or removing them from the network when deemed no longer necessary.

BWOpt Important Notes

Consider the following information when using BWOpt:

- You must have the Advanced RTM license package to use BWOpt.
- You cannot enable Bandwidth Optimization if LCM is enabled.
- BWOpt will not shift traffic in existing SR-TE policies that it did not create. This may prevent it from being able to mitigate congestion if most of the traffic on the congested link is in non-BWOpt SR-TE policies.
- BWOpt relies on the PCC's autoroute feature to steer traffic into the tactical SR-TE policies it creates. Autoroute is applied to these policies through the proper **Profile ID** option set in BWOpt (to align with configuration on the PCC associating that Profile ID with autoroute feature). This is critical to tactical SR policies shifting traffic away from congested links.
- Enable BWOpt on single-level IGP domains only.
- BWOpt leverages on the use of Segment Routing Traffic Matrix (SR-TM). SR-TM has the following limitations:
 - IPv6 is not supported.
 - Management, bundle, subinterfaces and tunnel interfaces are not supported as external interfaces.
 - Non-default Virtual, Routing, and Forwarding (VRF) is not supported as external interfaces.
 - SR-TM only takes SR labeled traffic into consideration. It will not account for Label Distribution Protocol (LDP) traffic.



Note For more information on SR-TM, see [Segment Routing Traffic Matrix](#).

- BWOpt uses simulated traffic based on measured SR-TM data to determine link utilizations and when to mitigate congestion. The simulated interface utilization that BWOpt monitors should closely align with the SNMP-based interface utilization that is displayed in the UI. However, due to various factors, including SNMP polling cadence and rate averaging techniques, they may differ at times. This can result in scenarios like a link appearing to be congested in the UI and BWOpt not reacting.
- BWOpt only creates tactical SR-TE policies on PCCs that are sources of SRTM telemetry data. Only these nodes (typically provider edge routers) provide the telemetry-based data needed to create simulated traffic demands in the internal model representing the traffic from that node to other PE nodes in the network.
- Only solutions that produce interface utilization below the threshold (set across all interfaces) will be deployed. If BWOpt is unable to mitigate congestion across the entire network, it will not deploy any tactical SR-TE policies and a “Network Congested. BWOpt unable to mitigate.” alarm is raised. This alarm goes away when congestion either subsides on its own or can be addressed successfully through BWOpt tactical SR-TE policy deployments.
- BWOpt temporarily pauses operation whenever the system is unavailable due to a restart or a rebuild of the topology from Topology Services. When this occurs, an alarm indicating this condition is set by BWOpt. During this time, BWOpt will not evaluate congestion in the network. All currently deployed tactical SR policies are maintained, but will not be modified or deleted. As soon as the model becomes available, the alarm is cleared and BWOpt will resume normal operation.

Automated Network Congestion Mitigation Example

This example demonstrates how Bandwidth Optimization (BWOpt) automatically mitigates network congestion by rerouting intent-based traffic without user intervention. In this example, the optimization intent is set to minimize the IGP metric.

The following BWOpt options are set (**Traffic Engineering > Bandwidth Optimization > Configuration**):

Figure 21: Bandwidth Optimization Configuration

The screenshot shows the configuration page for Bandwidth Optimization. The left sidebar has 'Bandwidth Optimization' selected, with sub-items 'Configuration' and 'Link Management'. The main area is titled 'Configuration' and has two tabs: 'Basic' (selected) and 'Advanced'. The configuration is organized into several sections:

- Enable:** A toggle switch is set to 'True'.
- Optimization Objective:** A dropdown menu is set to 'Minimize the IGP metric'.
- Color:** A text input field contains the value '1000'.
- Utilization Threshold:** A text input field contains the value '100'.
- Utilization Hold Margin:** A text input field contains the value '5'.
- Maximum Global Reoptimization Interval:** A text input field contains the value '0'.
- Profile ID:** A text input field contains the value '0'.
- Max Number of Parallel Tactical Policies:** A text input field contains the value '1'.

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

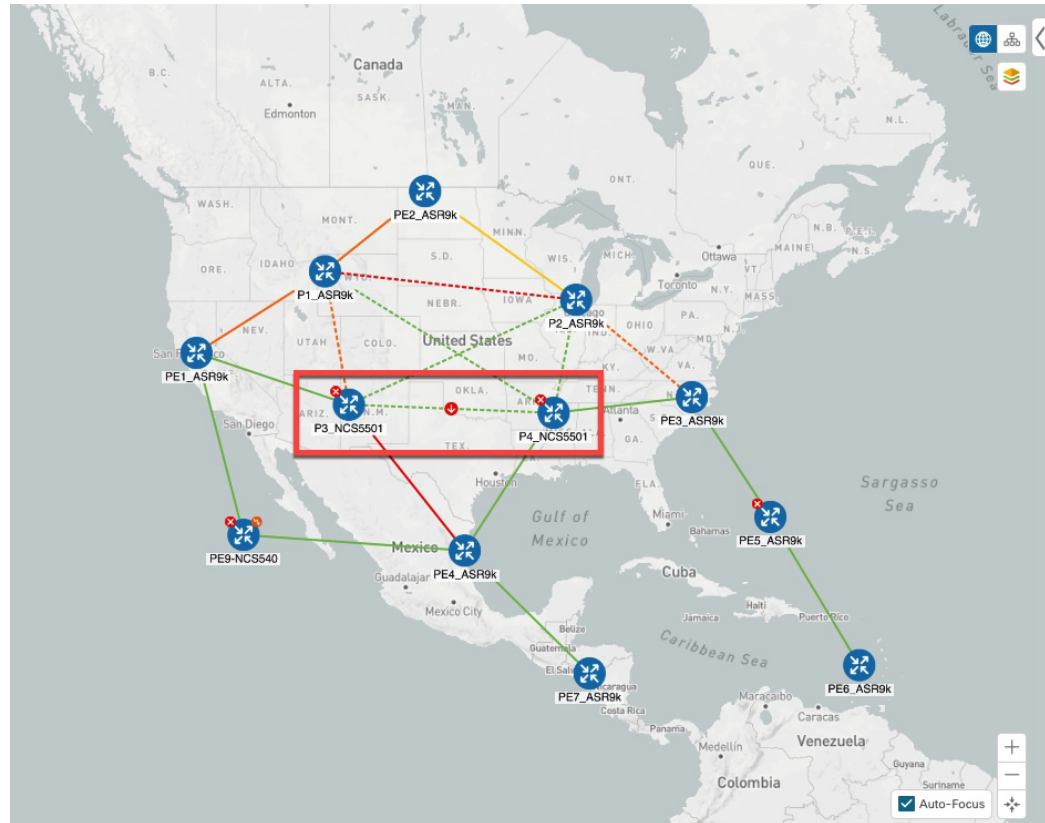
Below is a network with various devices and links that span the United States. Note that there are no SR-TE policies listed in the **SR Policies** table.

Figure 22: Example: Current Network



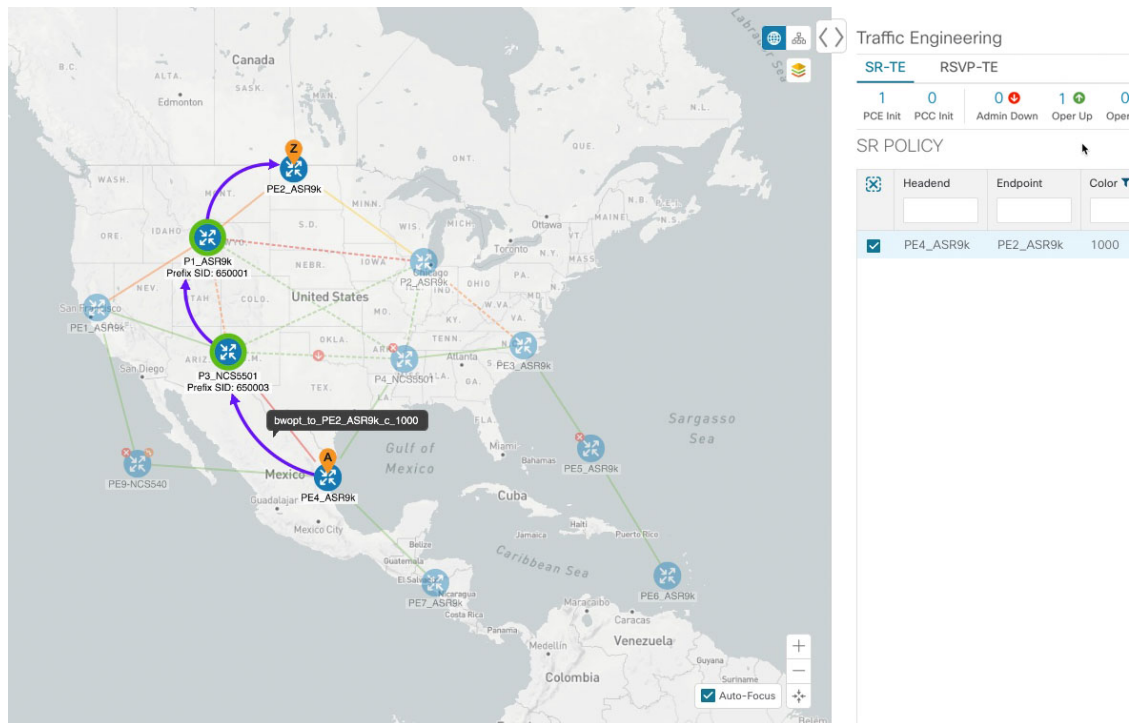
Suppose the link between P3_NCS5501 and P4_NCS5501 goes down. Traffic moves towards other links causing congestion and exceeds the configured utilization threshold.

Figure 23: Example: Link Down Between P3 and P4 Nodes




BWOpt recognizes the congestion and immediately calculates and deploys a tactical SR-TE policy. This new tactical SR-TE policy is listed in the **SR Policies** window.

Figure 24: Example: Tactical SR Policy Deployed



BWOpt continually monitors the network. When the links between P3_NCS5501 and P4_NCS5501 are back up, BWOpt will detect that the congestion (based on the defined criteria) has been mitigated. When the congestion falls under the set utilization threshold minus the utilization hold margin, the tactical SR-TE policy is automatically removed from the network.

You can also click  to view events relating to instantiation and removal of tactical SR-TE policies created by BWOpt.

Configure Bandwidth Optimization




Note Bandwidth Optimization (BWOpt) is only available as part of the Advance License package.

After BWOpt is enabled, it monitors all interfaces in the network for congestion based on the configured utilization threshold. When the utilization threshold is exceeded, it automatically deploys tactical policies and moves traffic away from the congested links. When congestion is alleviated, BWOpt automatically removes the tactical SR policy.

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



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

Note LCM and Bandwidth Optimization cannot be enabled at the same time.

- Step 3** Enter the required information. Hover the mouse pointer over  to view a description of each field.
- Step 4** Click **Commit Changes**. BWOpt begins to monitor network congestion based on the threshold and optimization intent that was configured.
-

Add Individual Interface Thresholds

Networks have many different links (10G, 40G, 100G) that require different thresholds to be set. To assign specific threshold values for individual interfaces when using LCM or Bandwidth Optimization, do the following:

- Step 1** From the main menu, choose one of the following:
- **Local Congestion Mitigation > Link Management**
 - **Bandwidth Optimization > Link Management**
- Step 2** Click .
- Step 3** Click the **Download sample configuration file** link.
- Step 4** Click **Cancel**.
- Step 5** Open and edit the configuration file (sampleLcmLinkManagement.csv) you just downloaded. Replace the sample text with your specific node, interface, and threshold information.
- Step 6** Rename and save the file.
- Step 7** Navigate back to the **Link Management** window.
- Step 8** Click  and navigate to the CSV file you just edited.
- Step 9** Click **Import**.
- Step 10** Confirm that the information appears correctly in the **Link Management** window.
-

Troubleshoot Bandwidth Optimization

BWOpt disables itself and issues an alarm when specific error conditions occur that hinder its ability to manage congestion properly and may lead to instability. The following table defines some of these conditions and possible causes to investigate. Additional details can be obtained for each error condition by referring to the BWOpt logs.



Note You can navigate to **Administration > Collection Jobs** and then filter the list of active collection jobs for Optim in the App ID column.

Table 5: Errors

Error Event Message	Possible Causes and Recommended Corrective Action
Optima Engine model error	<p>The network model used by BWOpt from the Optimization Engine is corrupt or is missing key data that is needed to properly support BWOpt. Possible causes include network discovery issues or synchronization problems between the Optimization Engine and Topology Services. Try restarting the Optimization Engine pod to rebuild the model.</p> <p>This error can also occur if the time required to deploy a tactical policy through SR-PCE, discover it, and add it to the model exceeds the Deployment Timeout option set for BWOpt. The default is 30 seconds which should suffice for small to medium sized networks. However, larger networks may require additional time.</p>
PCE Dispatch unreachable	<p>The deployment of a tactical policy to the network is not confirmed successful before the Deployment Timeout is exceeded. Increase the Deployment Timeout option to allow for additional time for deployments in larger networks.</p>
Unable to deploy a tactical SR policy	<p>A tactical SR policy deployment to SR-PCE was unsuccessful. There could be a variety of reasons for this. BWOpt and/or PCE Dispatch logs can provide some guidance as to the details of the failure. Confirm basic SR policy provisioning capability to the PCC via one of the SR-PCE providers is working.</p>



CHAPTER 10

Define and Maintain Intent-Based Bandwidth Requirements



Note Functionality described within this section is only available as part of the Advance RTM license package.

Bandwidth on Demand (BWoD) provides a bandwidth-aware Path Computation Element (PCE) to derive SR policy paths with requested bandwidth when available. Computed paths are deployed to the network through SR-PCE. BWoD continuously monitors link utilization to ensure no congestion occurs along the path. If conditions change in the network which causes link utilization to exceed the congestion threshold set by the user, BWoD automatically reoptimizes the policy path. BWoD supports bandwidth constraints for both PCE-initiated and PCC-initiated SR-TE policies.

BWoD utilizes a near real-time model of the network along with SNMP-based SR policy traffic measurements to ensure BWoD policies meet their bandwidth constraints. Users may fine tune the behavior of BWoD, affecting the path it computes, through the selection of application options including network utilization threshold (definition of congestion) and path optimization intent. BWoD works as a bandwidth-aware PCE for SR policies created through the UI and for SR policies created through CLI configuration on a headend with delegation to the SR-PCE. In the latter case, SR-PCE will subdelegate the SR policy with a bandwidth constraint to BWoD for path computation and relay the computed path returned by BWoD to the headend for instantiation.

- [BWoD Important Notes, on page 97](#)
- [Provision an SR-TE Policy to Maintain Intent-Based Bandwidth Requirements Example, on page 98](#)
- [Configure Bandwidth on Demand, on page 101](#)
- [Troubleshoot BWoD, on page 101](#)

BWoD Important Notes

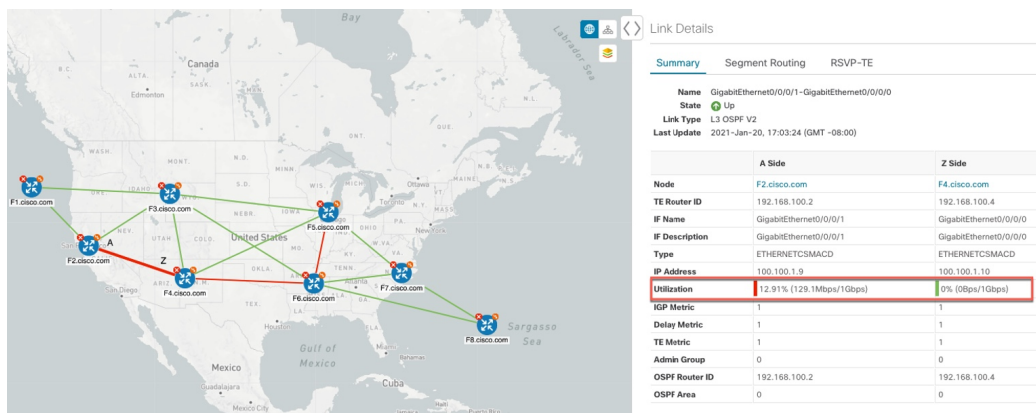
Consider the following information when using BWoD:

- You must have the Advanced RTM license package to use BWoD.
- If BWoD cannot find a path for a policy that guarantees its requested bandwidth, BWoD will attempt to find a *best effort* path if this option is enabled.

- BWoD temporarily pauses operation whenever the Optimization Engine model is unavailable due to an Optimization Engine restart or a rebuild of the topology from Topology Services. Any requests to BWoD during this time are rejected. When the model becomes available and BWoD receives 2 traffic updates from the Optimization Engine, BWoD will resume normal operation.

Provision an SR-TE Policy to Maintain Intent-Based Bandwidth Requirements Example

Figure 25: Initial BWoD Topology Example



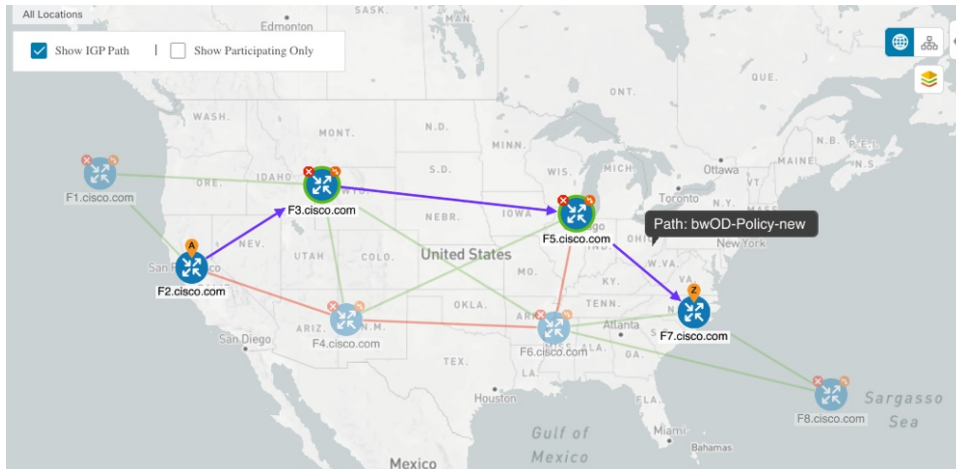
In this scenario we are using the above topology. The goal is to create a path from F2.cisco.com to F7.cisco.com that can accommodate 920 Mbps of traffic while keeping the utilization at 80%. The above example highlights the utilization on nodes F2.cisco.com and node F4.cisco.com to show that the link is being utilized and has a capacity of 1 Gbps. BWoD will initially try to find a single path that does not include this link since the addition of the requested bandwidth would exceed the utilization threshold. If a single path cannot be found, BWoD may recommend splitting the path.

Step 1 Enable and Configure BWoD.

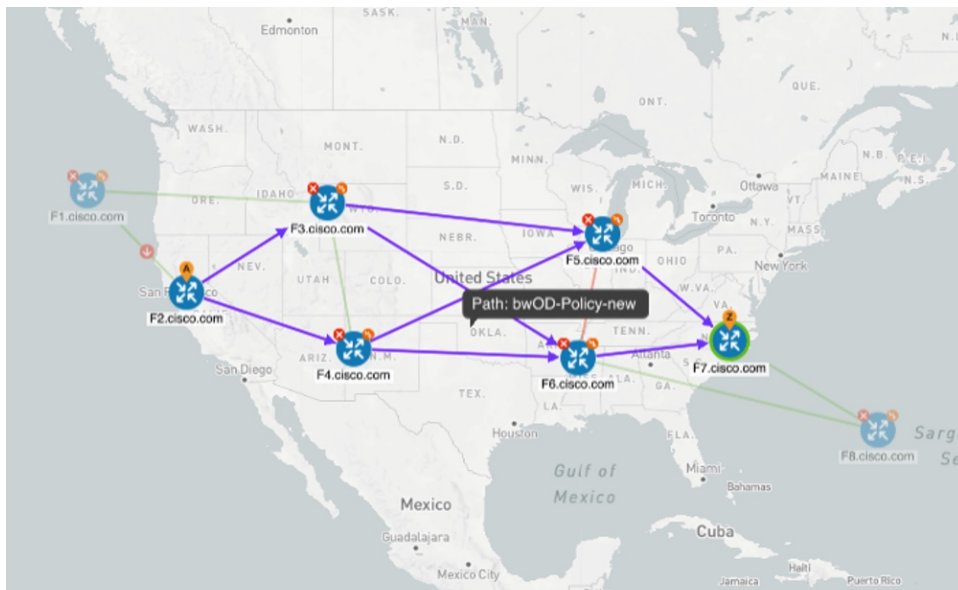
- From the main menu, choose **Traffic Engineering > Bandwidth on Demand > Configuration**.
- Toggle the Enable switch to **True** and enter **80** to set the utilization threshold percentage. To find descriptions of other options, simply hover the mouse over **?**.
- Click **Commit Changes**.

Step 2 Create a PCE-initiated BWoD SR-TE Policy.

- From the main menu, choose **Traffic Engineering > SR-TE** tab and click **+Create**.
- Enter the required SR-TE policy details.
- In the **Policy Path** field, click **Bandwidth on Demand** and enter a unique name for the BWoD path. In this case, **bwOD-Policy-new**.
- From the **Optimization Objective** drop-down list, select **Traffic Engineering (TE) Metric**.
- In the **Bandwidth** field enter the requested bandwidth. In this case, we are requesting **920 Mbps**.
- Click **Preview**.



In the above example, BWoD finds a single path that is under utilized and can still accommodate the requested bandwidth without going above the utilization threshold.



In the above example, BWoD cannot find a single path because of utilization and capacity limitations across several links. In this case, BWoD splits the path to obtain bandwidth and utilization requirements.

- g) If you are satisfied with the proposed SR-TE policy deployment, click **Provision**.

Step 3

Verify that the new BWoD SR-TE policy has been created.


- From the main menu, choose **Traffic Engineering** > **SR-TE**.
- Select the new BWoD SR-TE policy and view the SR policy details (click and choose **View**). Note that the Policy Type is **Bandwidth on Demand**.

Callout No.	Description
2	The bandwidth statement is added to a PCE delegated SR policy to create a BWoD policy. Once committed, the PCC delegates the path compute to SR-PCE.
3, 4	SR-PCE then sub-delegates the policy to BWoD which attempts to compute a path that meets the bandwidth constraint.
5, 6	If a bandwidth-compliant path is found, the segment list is returned to SR-PCE which forwards it over PCEP to the PCC and the PCC instantiates it. If BWoD is unable to compute a bw-compliant path for the policy or doing so will force an existing BWoD policy to not have a bw-compliant path, best effort paths may be computed by BWoD which attempt to minimize violations. This occurrence will also trigger BWoD to issue an event to the COE events UI indicating which BWoD policies are now on best effort paths.
7	A BWoD SR-TE policy is instantiated.

Configure Bandwidth on Demand

There are two parts to configure Bandwidth on Demand (BWoD):

1. Enable and configure BWoD options.
2. Create BWoD SR policies. As long as BWoD is enabled, you can create multiple BWoD SR policies.

-
- Step 1** From the main menu, choose **Traffic Engineering > Bandwidth on Demand > Configuration**.
- Step 2** Toggle the **Enable** switch to **True**.
- Step 3** Configure additional options. Hover the mouse pointer over  to view a description of each field.
- Step 4** Click **Commit Changes** to save the configuration.
- Step 5** To create BWoD SR policies, navigate to **Traffic Engineering > Traffic Engineering**.
- Step 6** From the SR Policy table, click **Create > PCE Init**.
- Step 7** In addition to entering the required SR policy details, click the **Bandwidth on Demand** option and enter the required bandwidth.
- Step 8** Click **Preview** to view the proposed SR policy.
- Step 9** Click **Provision** to commit the SR policy.
-

Troubleshoot BWoD

The following are some of the most common error conditions for BWoD and some possible corrective actions that may fix the issue.

Table 6: Errors

Error Event Message	Possible Causes and Recommended Corrective Action
OptimaModelError	<p>The network model used by BWoD from the Optimization Engine is corrupt or is missing key data that is needed to properly support BWoD. Possible causes include network discovery issues or synchronization problems between the Optimization Engine and Topology Services. Try restarting the Optimization Engine pod to rebuild the model.</p> <p>This error can also occur if the time required to discover a policy and add it to the model after it has been deployed exceeds the Deployment Timeout option set for BWoD. The default is 30 seconds which should suffice for small to medium sized networks. However, larger networks may require additional time.</p>
NATSTimedOutError	<p>The deployment of a bandwidth policy through SR-PCE exceeds the Deployment Timeout option set for BWoD. Increase the Deployment Timeout option to allow for additional time for deployments in larger networks.</p>
Traceback or other errors found in the log file	Please contact your Cisco service representative.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.

